ENSECUR

DATENSCHUTZ
BESSER
MACHEN

DATENSCHUTZ IN SOZIALEN EINRICHTUNGEN

WHITE PAPER

Version 1.0 - Stand: 23.12.2020

erstellt von der ENSECUR GmbH

ENSECUR GmbH

Standort Karlsruhe:
Kaiserstraße 86
76133 Karlsruhe
T: +49 (0) 721/180 356 70
F: +49 (0) 721/180 356 75

Standort Stuttgart:
Sophienstraße 25
70178 Stuttgart
T: +49 (0) 711/460 541 40
F: +49 (0) 711/460 541 45

Registergericht Mannheim
HRB 712239
USt-ID-Nr. DE277945684
Mail: info@ensecur.de
Web: www.ensecur.de

Geschäftsführer
Julian Häcker
Thorsten Jordan

ENSECUR DATENSCHUTZ BESSER MACHEN

INHALTSVERZEICHNIS

VORWORT **3**

1. DATENSCHUTZKONFORMER VERSAND VON E-MAILS **4**

1.1 Transportverschlüsselung reicht nicht aus 4

1.2 Geeignete Schutzmaßnahmen 4

1.3 Was ist mit Faxen? 5

1.4 Fazit 6

2. ERSTELLEN UND VERSAND VON E-RECHNUNGEN **7**

2.1 Anforderung zum E-Rechnungsversand in sozialen Einrichtungen und Umsetzungshinweise für eine datenschutzkonforme Ausgestaltung 7

2.2 Wie kann eine soziale Einrichtung den Anforderungen nachkommen? 8

2.3 Auftragsverarbeitung 8

2.4 Zusatzvereinbarung DSG-EKD 9

2.5 Prüfung der technischen und organisatorischen Maßnahmen 9

2.6 Durchführen einer Datenschutz-Folgenabschätzung 9

3. EINWILLIGUNGEN **11**

3.1 Worum geht es bei Einwilligungserklärungen? 11

3.2 Einwilligungsfähigkeit von Minderjährigen 12

3.3 Ist eine Einwilligung durch den gesetzlichen Betreuer möglich? 13

3.4 Schweigepflichtentbindung als besondere Ausgestaltung einer Einwilligung zur Datenweitergabe 14

4. HOME-OFFICE **16**

4.1 Was Sie beim Arbeiten zu Hause beachten sollten 16

4.2 Praktische Umsetzung der Datensicherheit im Home-Office 16

4.3 Besondere Vorsicht bei der Nutzung privater Endgeräte 18

4.4 Videokonferenzen im Home-Office 18

5. PRÄVENTION VON DATENPANNEN **20**

5.1 Was sind Datenpannen? 20

5.2 Was sind die Herausforderungen bei Datenpannen speziell für soziale Einrichtungen? 20

5.3 Häufige Datenschutzrisiken in sozialen Einrichtungen 21

ÜBER DIE AUTOREN **25**

ENSECUR DATENSCHUTZ BESSER MACHEN

VORWORT

Datenschutz in sozialen Einrichtungen ist spannend und herausfordernd zugleich. Die Beschäftigten verarbeiten höchst sensible personenbezogene Gesundheits- und Sozialdaten, tun dies häufig in offenen Häusern und müssen neben dem Datenschutz zahlreiche andere Regelungen in einem turbulenten Arbeitsalltag beachten. In vielen Fällen bleibt wenig Zeit für Sensibilisierung, so dass viele Beschäftigte sich alleine gelassen fühlen. Das ist schon herausfordernd genug.

Erhöhte Anforderungen entstehen dadurch, dass soziale Einrichtungen mit zahlreichen externen Stellen wie z.B. Landratsämtern, Krankenversicherungen, dem KVJS, Krankenhäusern, Arztpraxen etc. ihre besonders schützenswerten Daten austauschen müssen. Diese **besonders schützenswerten Gesundheitsdaten dürfen nur verschlüsselt übertragen werden**. Das ist keine neue Erkenntnis, doch die Verbreitung im Arbeitsalltag ist leider nach wie vor dürftig. Viele der externen Empfänger bieten immer noch keine einfache Möglichkeit, verschlüsselte Dokumente zu übermitteln. Dies erschwert den Arbeitsalltag zusätzlich. Mangels Alternativen bleibt häufig nur der Weg des postalischen Versands.

Die **E-Rechnungsverordnung** ändert dies in kleinen Schritten. Rechnungen an öffentliche Auftraggeber, wie z.B. Landratsämter als Kostenträger sind ab dem 27. November 2020 ab einem Betrag von 1.000 €, und sofern keine Ausnahmeregelungen greifen, digital und sicher (verschlüsselt) zu übermitteln. Daran arbeiten Stand Dezember 2020 noch viele soziale Einrichtungen und Kostenträger. Nach erfolgreicher und datenschutzkonformer Umsetzung wird dies zukünftig den Arbeitsalltag erheblich beschleunigen. Von dieser Änderung profitieren zukünftig auch Sonderzahler, die an dem Verfahren teilnehmen können, wenn sie ihre Einwilligung erteilen.

Einwilligungserklärungen sind eine weitere Herausforderung. Häufig ist eine Datenweitergabe oder -verarbeitung ohne Einwilligung rechtlich nicht möglich, z.B. Besuche durch Ehrenamtliche oder Seelsorger, Namen und Zimmernummern auf Informationstafeln, Veröffentlichung von Fotos in Medien der sozialen Einrichtungen. Dabei tritt auch die Frage nach der **Schweigepflichtentbindung** auf, da zahlreiche Beschäftigte einer beruflichen Schweigepflicht unterliegen. Nur wenn die Entbindung formal richtig erfolgt, dürfen Daten weitergegeben werden.

Corona bedingt bzw. weil soziale Einrichtungen flexible und attraktive Arbeitgeberinnen sind, arbeiten viele Beschäftigte aus dem **Home-Office.** Dabei gelten ebenfalls spezielle Datenschutzanforderungen gelten. Wenn die Beschäftigten die organisatorischen Vorgaben nicht einhalten, kann dies zu meldepflichtigen **Datenpannen** führen. Was Sie tun können, um diese zu **verhindern**, lesen Sie hier ebenfalls.

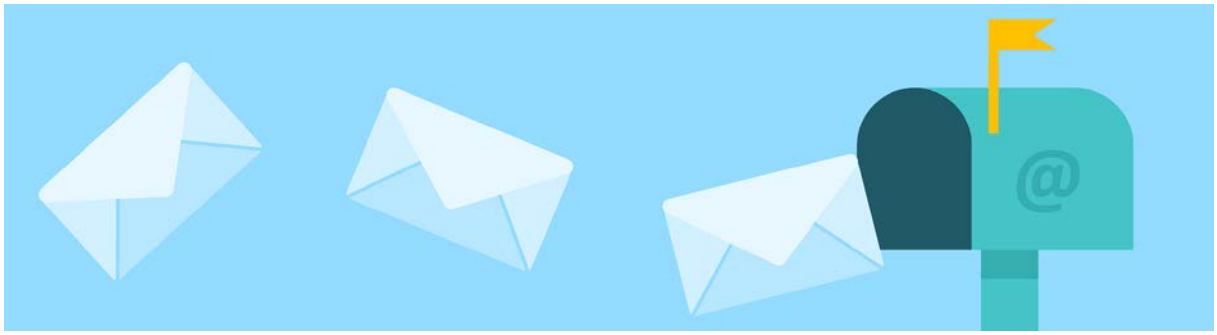
Dieses White Paper richtet sich an Beschäftigte in sozialen Einrichtungen, insbesondere Vorgesetzte im Bereich der sozialen Dienste, der IT, dem Rechnungswesen und auch allen anderen administrativen Bereichen. Wir wollen Ihnen **konkrete Lösungsempfehlungen** aufgrund unserer Praxiserfahrung an die Hand geben. Wenn uns das gelingt, sagen Sie uns das gerne. Wenn uns das nicht gelingt, sagen Sie uns das erst recht!

Noch ein Hinweis zum Gendern: Unser gemischtes Team an Autorinnen und Autoren wechselt im White Paper zwischen weiblichen und männlichen Formulierungen. Wir sind für Gleichberechtigung und gegen jegliche Art der Diskriminierung. Aus unserer Sicht erreichen wir das jedoch nicht durch ein Gendersternchen. Aus Gründen der Lesbarkeit haben wir uns für den genannten Weg entschieden.

Ihnen, liebe Leserinnen und Leser, wünschen wir beim Lesen viel Inspiration, wir freuen uns, wenn wir einen kleinen Beitrag für einen besseren Datenschutz in sozialen Einrichtungen leisten können.

Karlsruhe, im vorweihnachtlichen Dezember 2020,
die Autorinnen und Autoren

DATENSCHUTZKONFORMER VERSAND VON E-MAILS



Der Versand von E-Mails – ein Dauerbrenner in der Beratungspraxis bei sozialen Einrichtungen. Immer wieder schicken Mitarbeitende Gesundheitsdaten und Dokumente mit sensiblen Inhalten wie Beobachtungs- und Entwicklungsberichte über Klienten unverschlüsselt durch die Gegend. Versendet werden diese E-Mails sowohl intern als auch insbesondere an Leistungsträger, Krankenkassen, Landratsämter, Jugendämter oder sonstige behördliche Einrichtungen. Das ist datenschutzrechtlich sehr problematisch, da Gesundheitsdaten zu den besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO gehören. Diese Daten sind sehr sensibel und besonders gut zu schützen. *„Aber Herr Datenschutzbeauftragter, das machen doch alle so und die Behörden wollen das auch nicht anders!“* Gegenfrage: *„Müssen wir es falsch machen, nur weil es alle anderen auch falsch machen? – Bitte nicht!“*

1.1 Transportverschlüsselung reicht nicht aus

E-Mails sind in der Regel durchaus verschlüsselt, allerdings nur transportkanalverschlüsselt. Was heißt das? Wenn Sie eine E-Mail versenden, durchläuft diese bis zum Eingang beim Empfänger zwei Stationen, bis sie letztlich bei Station 3 ankommt.

1. Beim Versand verschicken Sie die E-Mail aus Ihrem Postausgang Ihres E-Mail-Server (Station 1).
2. Ihr E-Mail-Server schickt die E-Mail an den E-Mail-Server des Empfängers weiter (Station 2)
3. Von dort wird die E-Mail dann in das E-Mail-Postfach des Empfängers übermittelt, sodass der Empfänger die E-Mail lesen kann (Station 3).

Der Weg der E-Mail ist transportkanalverschlüsselt. Die E-Mail fliegt also wie durch einen geschützten Tunnel. Aber sobald die E-Mail den Tunnel verlässt, um den Weg zur nächsten Station einzuschlagen, ist sie ungeschützt. Das heißt bei Station 1 und Station 2 liegt die E-Mail unverschlüsselt auf dem jeweiligen Server, sodass Dritte oder auch der Serverbetreiber theoretisch Zugang zu den Daten bekommen können. Die Transportkanalverschlüsselung bietet also kein geeignetes Schutzniveau für den Versand von besonders sensiblen Daten.

1.2 Geeignete Schutzmaßnahmen

Der Königsweg ist die Ende-zu-Ende-Verschlüsselung. Hier wird die E-Mail beim Versand bereits so verschlüsselt, dass diese nur vom Empfänger mit einem privaten und geheimen Schlüssel geöffnet werden kann. Die E-Mails sind sowohl auf dem Transportweg als auch auf den E-Mail-Servern (Station 1 und 2) geschützt. Ohne Schlüssel sind die Daten nicht einsehbar. Eine Kenntnisnahme durch Dritte oder die Serverbetreiber ist ausgeschlossen. Aber Achtung! Bei einer Ende-zu-Ende-Verschlüsselung sind nur

der Inhalt der E-Mail und die Anhänge geschützt, nicht aber der Betreff und die E-Mail-Adresse (sogenannte Meta-Daten). Im Betreff sollten also keine personenbezogenen Daten auftauchen, da Dritte sonst zumindest im Groben über den Inhalt der E-Mail Kenntnis erlangen können. Die Ende-zu-Ende-Verschlüsselung ist nicht schwierig umzusetzen (gängige Systeme sind z.B. PGP und S/MIME), jedoch noch nicht weit verbreitet. Die Verschlüsselung funktioniert nur, wenn der Empfänger diese ebenfalls eingerichtet hat. Insofern ist es oftmals gar nicht möglich, Ende-zu-Ende-verschlüsselt zu kommunizieren. Folgende weitere Maßnahmen sollten Sie ergreifen, wenn eine Ende-zu-Ende-Verschlüsselung nicht möglich ist:

- Den Betreff der E-Mail ohne Personenbezug formulieren.
- Den Inhalt der E-Mail vorsichtig formulieren.
- Möglichst keine personenbezogenen Daten in die E-Mail schreiben. Oftmals reicht es aus, ein Kürzel des Klienten oder ein Aktenzeichen zu verwenden.
- Anhänge mit besonders sensiblen Inhalten über Klienten sind unbedingt mit einem sicheren Passwort zu versehen (mindestens 12 Zeichen, 3 aus 4 Kriterien aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen)!
- Übermitteln Sie das Passwort an Ihren Empfänger unbedingt über einen anderen Kanal (z.B. Telefon) und niemals in derselben E-Mail.
- Überprüfen Sie genau, ob die E-Mail-Adresse des Empfängers stimmt. Vorsicht mit der Autofill-Funktion!
- Sprechen Sie mit Ihren Vorgesetzten über eine zentrale und einrichtungsübergreifende Vorgabe, an die sich alle halten müssen.
- Setzen Sie eine Ende-zu-Ende-Verschlüsselung in Ihrer Einrichtung um, sodass zumindest intern Ende-zu-Ende-verschlüsselt kommuniziert werden kann.
- Klären Sie mit Ihren Empfängern, welche Möglichkeiten diese zum Empfang verschlüsselter E-Mails anbieten.

1.3 Was ist mit Faxen?

„Aber Herr Datenschutzbeauftragter, das ist doch alles viel zu kompliziert. Wir können doch auch einfach faxen. Das ist doch sicher, oder?“- Nein! Faxe sollten bei der Übermittlung besonders sensibler Daten nicht verwendet werden. Zwar ist beim Faxen über das Internet eine Transportkanalverschlüsselung möglich, aber damit sind die Verschlüsselungsmöglichkeiten auch schon erschöpft. Zudem werden Faxe auch heute noch oft über Telefonleitungen übertragen. Das kommt dem Versand einer offenen Postkarte gleich, denn diese Leitungen lassen sich nicht verschlüsseln. Rein technisch haben Faxe also kein angemessenes Datenschutzniveau für den Versand von Gesundheitsdaten. Vom technischen Aspekt abgesehen, bestehen beim Faxversand noch weitere Probleme:

- Die Faxe werden oftmals an zentralen Faxgeräten in einem Büro „ausgespuckt“ und liegen dann offen für jeden zugänglich im Posteingang des Gerätes. Es kann also nicht gewährleistet werden, dass nur der berechtigte Empfänger die Unterlagen erhält.
- Wenn die Zielnummer falsch eingegeben wird, können die Dokumente fehlgeleitet werden und landen an der falschen Adresse. Vertippt hat man sich leider schnell.

Faxe sind also für die Übermittlung von sensiblen Dokumenten nicht geeignet und sollten nicht genutzt werden. Für den Fall, dass es ohne Fax wirklich nicht geht, weil z.B. eine Arztpraxis keine Alternative anbietet, so beachten Sie unbedingt unsere Hinweise unter 5.3!

1.4 Fazit

Wir machen regelmäßig die Erfahrung, dass E-Mails mit besonders sensiblen Daten nicht datenschutzkonform versendet werden. Dies liegt nicht nur an den sozialen Einrichtungen, die durch die Beratung durchaus die Notwendigkeit erkennen, Maßnahmen zu ergreifen und Bereitschaft zeigen, Prozesse zu ändern. Oft sind es auch die externen Empfänger (Leistungsträger, Krankenkassen, Behörden), die sich weigern, an einer datenschutzkonformen Versendung von E-Mails durch Verschlüsselung mitzuwirken. Hier besteht aber definitiv Handlungsbedarf und wir plädieren dafür, dass Sie sich in Ihrer Einrichtung dieses Themas annehmen.

ERSTELLEN UND VERSAND VON E-RECHNUNGEN

2.1 Anforderung zum E-Rechnungsversand in sozialen Einrichtungen und Umsetzungshinweise für eine datenschutzkonforme Ausgestaltung

Im Rahmen der europäischen Digitalisierungsstrategie wurde im April 2014 die EU Richtlinie 2014/55/EU erlassen. Im Gegensatz zu einer Verordnung (wie z.B. der Datenschutz-Grundverordnung) sind Richtlinien durch die jeweiligen Gesetzgeber in nationales Recht umzusetzen. Diesem Auftrag kam die Bundesregierung mit der E-Rechnungsverordnung (E-Rech-VO) nach.

Was ist der Zweck der E-Rechnungsverordnung?
Die E-Rech-VO verfolgt zwei grundlegende Ziele. Zum einen liegt der Fokus auf einem einheitlichen Format, welches die automatisierte Weiterverarbeitung vereinfachen soll. Zum anderen soll neben der Standardisierung auch ein schneller, reibungsloser und sicherer Daten- bzw. Rechnungsaustausch mit den öffentlichen Einrichtungen gewährleistet werden.

Zu diesem Zweck sollen Rechnungen grundsätzlich in einem vordefinierten Format (XRechnung oder ZUGFeRD) erstellt werden. Neben der Anforderung zu einem einheitlichen Rechnungsstandard, der die automatische Datenverarbeitung vereinfachen soll, sind die so erstellten Rechnungen auch elektronisch an die jeweiligen öffentlichen Stellen zu übermitteln. Im Kern geht es demnach um eine elektronische Rechnungsstellung und -übermittlung. Herkömmliche Formate wie z.B. eine PDF-Datei sind demnach nicht länger zu verwenden.

Wer ist von der E-Rech-VO betroffen und wann ist diese umzusetzen?
Betroffen sind alle Unternehmen, Betriebe und soziale Einrichtungen, die mit öffentlichen Stellen Rechnungen austauschen. Soziale Einrichtungen haben in aller Regel viele Kontaktpunkte zu öffentlichen Stellen und Kostenträgern und unterliegen somit den Anforderungen der E-Rech-VO, welche ab dem 27.11.2020 verpflichtend umzusetzen sind.

2.2 Wie kann eine soziale Einrichtung den Anforderungen nachkommen?

Für die Umsetzung der Anforderungen kommen grundsätzlich zwei Optionen in Frage:

1. **Implementierung eigener Mechanismen zur Umsetzung der Anforderungen**
   Insbesondere das von der E-Rech-VO bevorzugte Format XRechnung, welches ein auf XML basiertes Datenmodell aufbaut, ist aufgrund der Open Source Implementierung inkl. frei zur Verfügung stehender Referenzimplementierungen gut zur eigenen Umsetzung geeignet – entsprechende Kapazitäten und IT-Know-How vorausgesetzt. Der aktuelle Stand der XRechnung Implementierung, welche durch das Bundesministerium des Innern, für Bau und Heimat (BMI) in Kooperation mit der Koordinierungsstelle für IT-Standards (KoSIT) entwickelt wurde, entspricht noch nicht vollumfänglich den Anforderungen aller Branchen und Länder. Daher wird in absehbarer Zeit das Format durch Erweiterungen vervollständigt. Sofern eine eigene Implementierung angestrebt wird, ist in Zukunft mit Anpassungsbedarf zu rechnen.

   Neben den Anforderungen an die XRechnung sind außerdem weitreichende technische und organisatorische Maßnahmen zur Sicherstellung der IT-Sicherheit zu treffen, deren Erläuterungen den Rahmen dieses White Papers deutlich sprengen würden. Sollten Sie eine eigene Implementierung erwägen, beziehen Sie sowohl Ihre Datenschutzbeauftragte als auch Ihre IT-Sicherheitsbeauftragte frühzeitig in die Thematik mit ein.

   Aufgrund der knappen IT-Ressourcen und ggf. aus Mangel an entsprechendem Fachpersonal für die eigene Implementierung der X-Rechnung und deren sichere Übermittlung an die öffentlichen Stellen, dürfte für viele soziale Einrichtungen der einzige Weg für eine Umsetzung der Anforderungen die Kooperation mit einem Dienstleister sein, der die Anforderungen erfüllen kann.

2. **Heranziehen von Dienstleistern zur Erfüllung der Anforderung**
   Sofern entsprechende Ressourcen und/oder schlichtweg das Know-How der eigenen Einrichtung nicht ausreichend ist, um eine Implementierung vorzunehmen, bleibt nur die Inanspruchnahme einer Dienstleistung. Im Vorfeld sind aus Datenschutzsicht folgende Aspekte zu berücksichtigen:

   1. Auftragsverarbeitung
   2. Zusatzvereinbarung auf Einhaltung des DSG-EKD (sofern der Verantwortliche eine evangelische kirchliche Stelle ist)
   3. Prüfung der technischen und organisatorischen Maßnahmen
   4. Durchführung einer Datenschutz-Folgenabschätzung

2.3 Auftragsverarbeitung

Bei Rechnungserstellung und -versand fallen in aller Regel personenbezogene Daten an. Gerade im Kontext von sozialen Einrichtungen werden häufig auch Rechnungen über erbrachte Leistungen gestellt, die Rückschlüsse auf Gesundheitsdaten zulassen. Daher werden in vielen Fällen besondere personenbezogene Daten gemäß § 4 Nr. 2 DSG-EKD verarbeitet, die aufgrund der Sensibilität auch mit technischen und organisatorischen Maßnahmen geschützt werden müssen, die über das übliche Maß hinausgehen. Aus diesem Grund kann grundsätzlich davon ausgegangen werden, dass bei einer Beauftragung eines Dienstleisters für die Erfüllung dieser Aufgaben ein Auftragsverarbeitungsverhältnis vorliegt und zwingend ein Auftragsverarbeitungsvertrag samt geeigneter technischer und organisatorischer Maßnahmen abgeschlossen werden muss.

2.4 Zusatzvereinbarung DSG-EKD

Sofern Ihre Einrichtung dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) unterliegt, ist neben dem Auftragsverarbeitungsvertrag auch zwingend noch eine Zusatzvereinbarung notwendig, in der sich die Auftragsnehmerin der kirchlichen Datenschutzaufsicht unterwirft.

2.5 Prüfung der technischen und organisatorischen Maßnahmen

Neben dem Abschluss eines Auftragsverarbeitungsvertrages, welcher die Rechtsgrundlage für die angestrebte Datenübermittlung sicherstellt, sind die Anlagen des Vertrages detailliert zu überprüfen. Insbesondere die vom Dienstleister getroffenen und gemäß Vertrag zugesicherten technischen und organisatorischen Maßnahmen (toMs) müssen für den Kontext der Verarbeitung angemessen sein. Folgende Aspekte (Auszug) sind zwingend zu berücksichtigen bzw. zu erfüllen:

- Ausgereiftes Berechtigungskonzept (sowohl in der Anwendung, als auch beim Dienstleister selbst), welches ausgewählten Personen Zugriff auf die notwendigen Informationen gewährt.
- Sichere und ggf. verschlüsselte Speicherung der Rechnungen (sowohl lokal in der Einrichtung, als auch bei dem Dienstleister).
- Überprüfung und Einsatz sicherer Protokolle für die Datenübermittlung zwischen Einrichtung, Dienstleister und Rechnungsempfängern.
- Überprüfung der Subdienstleister, insbesondere mit Hinblick auf Verarbeitungen in Drittländern.

2.6 Durchführen einer Datenschutz-Folgenabschätzung

Das DSG-EKD fordert eine Datenschutz-Folgenabschätzung, sofern die Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen zur Folge hat. In Anbetracht der erfassten Daten, die unter Umständen Rückschlüsse auf den Gesundheitszustand der Rechnungsempfängerin zulassen und eventuell aufgeführten Bank- und Kreditkartendaten, sowie der Hinzuziehung weiterer Parteien (Auftragsverarbeiter samt Subdienstleister) ist in aller Regel eine Datenschutz-Folgenabschätzung unabdingbar. Die im Vorfeld sauber dokumentierten und auf Eignung geprüften toMs des Dienstleisters dienen als Grundlage, um eine Risikoanalyse durchzuführen.

Neben diesen Aspekten sollten Sie bei der Umsetzung auch daran denken, das Verfahrensverzeichnis und die Informationspflichten zu aktualisieren. Die Einbindung Ihrer Datenschutzbeauftragten ist daher obligatorisch.

Hinweis zum Versand von Rechnungen an Endkunden, Klienten & Betreuer
Die Anforderungen aus der E-Rechnungsverordnung beziehen sich ausschließlich auf öffentliche Stellen. Ein Versand in den Formaten XRechnung oder ZUGFeRD an Endverbraucher ist kein Bestandteil der Verordnung. Im Alltag dürfte ein Versand dieser Formate an Endverbraucherinnen auch an deren technischen Mitteln zur Weiterverarbeitung scheitern. Aus diesem Grund dürfte bis auf absehbare Zeit nach wie vor das PDF-Format Verwendung finden. Beim Rechnungsversand als PDF-Datei ist unbedingt zu berücksichtigen, dass es sich bei den Inhalten, die bei der Rechnungsstellung durch soziale Einrichtungen regelmäßig um besonders sensible personenbezogene Daten handeln, die entsprechend zu

schützten sind. Eine Übermittlung solcher Rechnungen mit einer lediglich auf dem Transportkanal verschlüsselten E-Mail ist in aller Regel nicht ausreichend. In diesem Kontext ist unbedingt zu berücksichtigen, dass das Unterlassen von geeigneten toMs auch nicht durch das Einholen einer Einwilligung durch die Rechnungsempfängerinnen (z.B. Klientinnen oder deren Betreuerinnen) zu legitimieren ist.

Hilfreiche Links:

- https://www.gesetze-im-internet.de/erechv/BJNR355500017.html
- https://www.bmi.bund.de/DE/startseite/startseite-node.html
- https://de.wikipedia.org/wiki/Koordinierungsstelle_f%C3%BCr_IT-Standards
- https://github.com/itplr-kosit

EINWILLIGUNGEN

3.1 Worum geht es bei Einwilligungserklärungen?

Das Recht auf informationelle Selbstbestimmung verbietet grundsätzlich das Verarbeiten von personenbezogenen Daten (pb Daten) und erlaubt dies lediglich unter bestimmten Voraussetzungen. Daher kommt der Einwilligungserklärung im Datenschutz eine besondere Bedeutung zu, da sich die Rechtmäßigkeit der Verarbeitung von pb Daten aus der Zustimmung des Betroffenen ergibt. Das ist das sogenannte "*Verbot mit Erlaubnisvorbehalt*". Eine Zustimmung des Betroffenen ist nur in Ausnahmefällen zu empfehlen und kein allgemeiner Lösungsansatz. Eine Rechtsgrundlage für die Verarbeitung pb Daten zu finden, die keine Einwilligung des Betroffenen erfordert, ist für soziale Einrichtungen die bevorzugte Lösung, da in diesem Fall kraft Gesetzes eine Verarbeitung möglich ist. Beispiele hierfür sind:
Daten, die im Beschäftigungsverhältnis notwendigerweise erhoben und gespeichert werden müssen, oder (sensible) pb Daten, die zur Erfüllung des Betreuungsvertrages mit den Klienten notwendig sind. Wann eine Datenverarbeitung rechtmäßig ist, richtet sich dabei insbesondere nach den Rechtsgrundlagen des Artikel 6 Absatz 1 der DS-GVO oder den vergleichbaren Vorschriften des DSG-EKD.

Bestimmte Verarbeitungen können nur mit einer Einwilligung durchgeführt werden und auch nur, wenn sämtliche rechtlichen Anforderungen erfüllt sind:

Anforderungen an eine wirksame Einwilligung:

1. **Freiwilligkeit:**
   Sie muss auf einer freiwilligen Entscheidung beruhen. Das heißt, der Betroffene muss eine echte Wahl haben, ohne durch die Entscheidung Nachteile zu erleiden (Erwägungsgrund 42 DS-GVO, sog. Kopplungsverbot). Zum Beispiel darf die Nutzung einer Webseite nicht davon abhängig gemacht werden, ob der Betroffene in das Setzen von Tracking Cookies einwilligt oder nicht.

2. **Für den bestimmten Fall:**
   Der Betroffene muss eindeutig erkennen können, für welchen Zweck die Einwilligung eingeholt werden soll. Es ist daher die Aufgabe des Verantwortlichen, eindeutig festzulegen, für welche Datenverarbeitungen sie genutzt wird. Pauschale Einwilligungen, bei denen der Betroffene den Zweck der Datenverarbeitung nicht klar erkennen kann, sind ungültig.

Anforderungen an eine wirksame Einwilligung (Fortsetzung):

3. **In informierter Weise:**
   Der Betroffene muss vor der Einwilligung in die Lage versetzt werden zu wissen, für was er sie erteilt, welche seiner Daten durch wen verarbeitet werden und welche Tragweite seine Entscheidung hat. Nur wenn der Betroffene dies weiß, kann er eine informierte Entscheidung treffen. Zudem ist der Betroffene über sein Widerrufsrecht zu informieren.
4. **Unmissverständlichkeit**:
   Die Einwilligung in die Datenverarbeitung muss durch eine ausdrückliche und eindeutige Willensbekundung erfolgen.

Formerfordernis
Eine festgeschriebene Form für eine Einwilligung gibt es nicht. Sie kann schriftlich, elektronisch oder mündlich erteilt werden. Jedoch ist der Verantwortliche für die Einhaltung der Grundsätze der Datenverarbeitung rechenschaftspflichtig und muss diese nachweisen können. Arbeiten Sie deshalb mit schriftlichen oder elektronischen Einwilligungen! Dies erfolgt für den Fall einer elektronischen Einwilligung oftmals durch das Double Opt-in Verfahren, das eine zweistufige Bestätigung vorsieht, um die Einwilligung zweifach zu verifizieren. Der Anfragende wird durch die Zusendung eines Links gebeten die Anfrage (zum Beispiel für den Erhalt eines Newsletters) zu bestätigen.

Betroffenenrechte im Zusammenhang mit einer Einwilligung
Wie oben erwähnt, muss die Betroffene bei der Einholung ihrer Einwilligung darauf aufmerksam gemacht werden, dass sie die Einwilligung jederzeit widerrufen kann. Die Verarbeitung der pb Daten ist dann für eine zukünftige Verwendung untersagt. Zum Beispiel sind dann Fotos auf einer Webseite zu entfernen, wenn der Betroffene seine ursprünglich erteilte Einwilligung widerruft. Die Transparenz über die konkrete Zweckbestimmung der Verarbeitung pb Daten macht es zudem erforderlich, dass die soziale Einrichtung ihrer Informationspflicht nach Art. 13 DS-GVO nachkommt.

Typische Beispiele für die Notwendigkeit einer Einwilligung

- Verwendung von Foto- oder Videoaufnahmen für einen bestimmten Zweck (Veröffentlichung auf der Webseite der sozialen Einrichtung, in Printmedien etc.)
- Namen und Zimmernummern auf Informationstafeln
- Zusendung von Informationen als Newsletter oder durch Anfragende bei der Suche nach einer geeigneten Einrichtung für ihre Angehörigen
- Tracking des Verhaltens von Webseitenbesuchern durch den Einsatz von sog. Cookies
- Teilnahme an bestimmten Programmen, die die soziale Einrichtung den Beschäftigten zugutekommen lassen möchte.

3.2 Einwilligungsfähigkeit von Minderjährigen

Ab welchem Alter Kinder selbst wirksam die Einwilligung in die Verarbeitung der sie betreffenden Daten durch Dritte erteilen können, hat die DS-GVO nicht eindeutig geregelt. Nach der Definition in Art. 4 Nr. 11 DS-GVO muss die betroffene Person freiwillig und in informierter Weise zu verstehen geben, dass

sie mit der Verarbeitung ihrer Daten einverstanden ist. Daraus lässt sich ableiten, dass die betroffene Person fähig sein muss, Bedeutung und Tragweite ihrer Erklärung zu erfassen. So regelt etwa Artikel 8 DS-GVO, dass bei einem direkt an ein Kind gerichteten Angebot von Diensten der Informationsgesellschaft das Kind selbst wirksam in die Datenverarbeitung einwilligen kann, wenn es 16 Jahre alt ist. Ist es jünger, bedarf es (auch oder stattdessen) der Zustimmung der Erziehungsberechtigten. Inwieweit diese Regelung der DS-GVO auf andere Einwilligungserklärungen durch Minderjährige verallgemeinerungsfähig ist, ist allerdings umstritten. Für die Praxis empfiehlt es sich, sowohl vom Kind als auch von dessen gesetzlichen Vertretern eine Einwilligung einzuholen, sobald in Betracht kommt, dass das Kind die nötige Verstandesreife haben könnte, um Bedeutung und Tragweite der Einwilligung in die konkrete Datenverarbeitung zu erkennen.
(Quelle: https://www.baden-wuerttemberg.datenschutz.de/fotografierverbot-an-schulen/)

3.3 Ist eine Einwilligung durch den gesetzlichen Betreuer möglich?

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht. Ein solches Recht ist nicht ohne Weiteres übertragbar. In der Praxis erleben wir oftmals die Annahme, dass Einwilligungserklärungen selbstverständlich durch die gesetzlichen Betreuer unterschrieben werden könnten. Damit machen es sich die sozialen Einrichtungen zu einfach.

Durch die Erstellung und Erläuterung einer Einwilligungserklärung in einfacher Sprache ist oftmals die Grundlage geschaffen, dass Menschen mit Behinderung den zur Erlaubnis angefragten Verarbeitungszweck verstehen und durchaus selbst entscheiden können, ob sie dem zustimmen möchten oder nicht. Ein gesetzlicher Betreuer kann dabei eine wertvolle beratende Rolle einnehmen, die er als Vertrauensperson ohnehin haben sollte. Unterschreibt der gesetzliche Betreuer zusätzlich die Einwilligungserklärung, so "schadet" das sicherlich nicht. Erster Adressat sollte aber immer die betroffene Person sein.

Einen guten Überblick über die Erteilung von Einwilligungen durch die betroffene Person selbst oder die gesetzliche Betreuerin bietet die nachfolgende Übersicht:

Personen	Rechtsstatus	Erteilung der Einwilligung
Kinder unter 7 Jahren	geschäftsunfähig § 104 Ziff. 1 BGB	Gesetzliche Vertreter; bei gemeinsamem Sorgerecht können Eltern nur gemeinsam einwilligen (Einwilligung ist die vorher erteilte Zustimmung, § 183 BGB). **Ausnahmen**: Siehe bei Erwachsenen.
Minderjährige	Beschränkt geschäftsfähig § 106 BGB	Fotos von der eigenen Person dürfen nur mit Einwilligung der betroffenen Person verbreitet oder öffentlich zur Schau gestellt werden (§ 22 KunstUrG). Bei Minderjährigen bedarf es der Zustimmung des gesetzlichen Vertreters, wobei ein Foto nicht gegen den Willen des Kindes veröffentlicht werden darf. **Ausnahmen**: Siehe bei Erwachsenen.

Personen	Rechtsstatus	Erteilung der Einwilligung
Erwachsene	geschäftsfähig	Das Recht am eigenen Bild ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts, Art. 2 i. V. m. Art. 1 GG. Daraus folgt, dass grundsätzlich allein dem Abgebildeten die Befugnis zusteht darüber zu befinden, ob und in welcher Weise er der Öffentlichkeit vorgestellt wird. **Ausnahmen:** Keine Einwilligung ist nötig, wenn abgebildete Person nicht den Motivschwerpunkt bildet oder Teil einer Versammlung ist, § 23 KunstUrG.
Erwachsene mit Behinderung und gesetzlicher Betreuung	geschäftsfähig	Grundsätzlich wie Erwachsene (unter Berücksichtigung der Einwilligungsfähigkeit)
Erwachsene mit Behinderung und Einwilligungsvorbehalt	beschränkt geschäftsfähig	Ein Betreuter mit Einwilligungsvorbehalt steht weitgehend einem beschränkt Geschäftsfähigen gleich, § 1903 Abs. 1 S. 2 und Abs. 3 BGB. Das allgemeine Persönlichkeitsrecht des Betreuten kann jedoch nur zu dessen erforderlichen Schutz eingeschränkt werden, so dass es hier maßgeblich auf seine Einwilligung ankommt.
Geschäftsunfähige Erwachsene	geschäftsunfähig § 104 Ziff. 2 BGB	Einwilligung des Betreuers als gesetzlicher Vertreter ist erforderlich

3.4 Schweigepflichtentbindung als besondere Ausgestaltung einer Einwilligung zur Datenweitergabe

Im Kontext von Einwilligungserklärungen ist die Schweigepflichtentbindung relevant, da diese letztendlich die Zustimmung (Erlaubnis) dokumentiert, besonders sensible pb Daten eines Betroffenen (Gesundheitsdaten) an Dritte weitergeben zu dürfen. Die konkrete Pflicht einer Schweigepflichtentbindung ergibt sich aus der Zugehörigkeit zu den Berufsgruppen von Geheimnisträgern, die in § 203 Abs. 1 Nr. 1 6 StGB aufgezählt sind, und aus der sich das besondere Vertrauensverhältnis zwischen Klienten und Sozialarbeitern/Sozialpädagogen etc. ergibt.

In der Aufzählung des § 203 Abs. 1 StGB finden sich

- Ärzte, Krankenschwestern, Hebammen, Arzthelfer, Masseure, Altenpfleger und Angehörige eines anderen Heilberufs mit staatlich geregelter Ausbildung,
- Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

- Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer öffentlich anerkannten Beratungsstelle,
- Mitglieder oder Beauftragte einer anerkannten Beratungsstelle nach den §§ 3 und 8 Schwangerschaftskonfliktgesetz,
- staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen,
- berufsmäßig tätige Gehilfen, die in die Vorbereitung, Durchführung, Auswertung der beruflichen Tätigkeit des Berufsgeheimnisträgers einbezogen sind,
- Personen, die in Vorbereitung auf einen der vorgenannten Berufe tätig sind (§ 203 Abs. 3 StGB) z.B. Berufspraktikanten, im Rahmen einer Schul- oder Hochschulausbildung tätige Studenten im Vor-, Zwischenpraktikum und im Praxissemester.
- sonstige mitwirkende Personen: Annahme von Telefonanrufen, Schreibarbeiten, Tätigkeiten im Rechnungswesen, Aktenarchivierung, Einrichtung/Wartung/Änderung informationstechnischer Anlagen.

Entsprechend den oben genannten Anforderungen an eine rechtswirksame Einwilligung erfordert eine Schweigepflichtentbindung eine hinreichende Beschreibung darüber, welche Daten eines Betroffenen für welchen Zweck an welche Personen/Institutionen weitergegeben werden sollen. Die Betroffenenrechte sind analog zu den Einwilligungserklärungen auch hier zu beachten!

Praktische Bedeutung erlangt die Schweigepflichtentbindung bei sozialen Einrichtungen bei der Weitergabe von Informationen eines Klienten durch die gewünschte Zusammenarbeit/Abstimmung mit weiteren Personen außerhalb der Einrichtung. Ein Beispiel hierfür ist die Hilfeplanung nach § 36 SGB VIII, an dem sich mehrere Personen aus verschiedenen Fachbereichen unterschiedlicher Einrichtungen/Institutionen über die Betreuung einer Klientin austauschen.

Hilfreiche Links:

- DSK Kurzpapier: Einwilligung nach der DS-GVO
- GDD Praxishilfe XIII
- Datenschutz und Schweigepflicht
- Fotografieren und Datenschutz (Infobroschüre des LfDI BW)
- Schweigepflicht der Mitarbeiter (Info der Caritas)
- Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis
- Datenschutz in Paritätischen Mitgliedsorganisationen

HOME-OFFICE

4.1 Was Sie beim Arbeiten zu Hause beachten sollten

Ihre Privatwohnung erfüllt in der Regel nicht die gleichen Sicherheitsstandards, wie Ihr Arbeitsplatz in Ihrer sozialen Einrichtung. Daher besteht ein erhöhtes Missbrauchsrisiko von Daten durch Dritte, welches Sie durch die folgenden Praxishinweise reduzieren können. Sie als Mitarbeitende stehen im Home-Office umso mehr in der Verantwortung, die Daten angemessen vor Verlust, Zugriff oder Einsichtnahme durch Unbefugte zu schützen.

4.2 Praktische Umsetzung der Datensicherheit im Home-Office

Anforderung	Erläuterung	Erfüllt	
1. Unbefugte Einsichtnahme verhindern	Achten Sie darauf, dass keine Unbefugten Einsicht in personenbezogene Daten nehmen. *„Unbefugte“* sind in diesem Kontext auch Kinder, Ehepartnerinnen oder sonstige im Haushalt lebende Personen. Es bietet sich also an, in einem geschlossenen separaten Zimmer zu arbeiten.	☐ **Ja**	☐ **Nein**
2. Offizielle Ausrüstung verwenden	Grundsätzlich sollten Sie im Home-Office nur mit den von Ihrer Einrichtung bereitgestellten betrieblichen Geräten und Softwareanwendungen arbeiten. Nutzen Sie die betrieblichen Geräte nur für dienstliche Zwecke.	☐ **Ja**	☐ **Nein**
3. Sichere Einwahl auf das Einrichtungsnetzwerk	Greifen Sie auf das Netzwerk der Einrichtung am besten nur über eine gesicherte Verbindung (VPN) zu.	☐ **Ja**	☐ **Nein**
4. Eigenes Netzwerk absichern	Stellen Sie sicher, dass der häusliche WLAN-Router mit der aktuell höchsten Sicherheitsstufe konfiguriert (WPA2 Sicherheitsstandard) und der WLAN-Zugang durch ein komplexes Passwort geschützt ist (Anmerkung: Tipps zu sicheren Passwörtern am Ende dieses Artikels) → Dies können Sie i.d.R. in den Einstellungen Ihres Routers unter *Sicherheit* konfigurieren. Denken Sie daran, das vorgegebene Passwort, welches auf der Unterseite des Routers steht, unbedingt zu ändern.	☐ **Ja**	☐ **Nein**

Anforderung	Erläuterung	Erfüllt	
5. Zugriff auf Computer schützen	Schützen Sie den Zugang zum Computer mit einem komplexen Passwort. Sperren Sie beim Verlassen des Arbeitsplatzes das Gerät, so dass bei der Rückkehr zum Arbeitsplatz die erneute Eingabe des Passwortes erforderlich ist. → Tastenkombination *„Strg“+“Alt“+“Entf“* oder *„Windows-Taste“+ „L“* gleichzeitig drücken! Stellen Sie das Gerät so ein, dass die automatische Sperrung nach 5 Minuten erfolgt, falls Sie die manuelle Sperrung einmal vergessen sollten. → Über Energieoptionen ist einstellbar, ab wann eine Sperrung erfolgt. Fahren Sie das Gerät am Ende des Arbeitstages herunter, da eine Angreiferin auch bei aktivierter Verschlüsselung im Ruhemodus das Gerät angreifen kann. Bewahren Sie den Computer sowie sonstige Unterlagen in einem abschließbaren Schrank auf. Entfernen Sie im privaten Gebrauch befindliche und genutzte Sprachassistenzsysteme (z.B. ALEXA etc.) aus dem Home-Office, denn ALEXA hört mit!	☐ **Ja**	☐ **Nein**
6. Private Geräte schützen	Sofern Sie doch auf einem privaten Gerät arbeiten, so beachten Sie bitte die Sicherheitshinweise Ihrer Einrichtung. Für die Nutzung von privaten Geräten ist vorab unbedingt die Erlaubnis der Vorgesetzten einzuholen! Verschlüsseln Sie die Festplatte Ihres PC/Laptops (z.B. mit VeraCrypt oder Bitlocker) →Anleitung zum Verschlüsseln mit VeraCrypt z.B. über dieses Video	☐ **Ja**	☐ **Nein**

4.3 Besondere Vorsicht bei der Nutzung privater Endgeräte

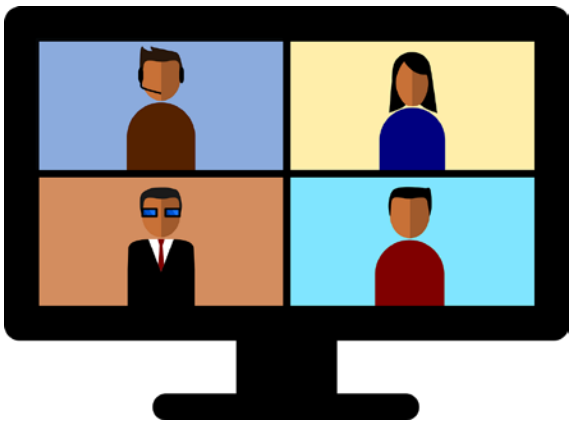
Wie oben erläutert, sollten Sie ausschließlich betriebliche Geräte nutzen. Sollte für Sie dennoch die Nutzung von privaten Laptops, Rechnern oder Smartphones relevant werden, so berücksichtigen Sie bitte zusätzlich die folgenden spezifischeren Maßnahmen zur Datensicherheit:

- Holen Sie sich vorher die Genehmigung Ihrer Vorgesetzten ein und beachten Sie zwingend die internen Vorgaben.
- Stellen Sie sicher, dass auf Ihrem privaten Computer bzw. Ihrem privaten Smartphone stets die aktuellste Version des Betriebssystems installiert ist.
- Alle vom Hersteller verfügbaren Sicherheitspatches, Updates und Upgrades sollten Sie unverzüglich installieren.
- Verwenden Sie ausschließlich aktuelle Browser mit den neusten Aktualisierungen.
- Stellen Sie sicher, dass stets ein aktueller Virenschutz aktiv ist.
- Von einer lokalen Speicherung personenbezogener Daten sollten Sie möglichst absehen. Eine Speicherung in einer privaten Cloud ist nicht zulässig.
- Wenn ein Datentransfer vom privaten Endgerät auf das dienstliche Endgerät per mobilem Datenträger erfolgt (USB-Sticks, externe Festplatten), sollten Sie die Datenträger (wenn möglich) zuvor durch die IT auf Viren untersuchen lassen.
- Grundsätzlich sollten Sie nur mobile Datenträger verwenden, die durch die IT ausgegeben werden.
- Vermeiden Sie eine Vermischung von betrieblichen und privaten Daten.
- Schließen Sie private Anwendungen während Sie dienstliche Anwendungen verwenden.
- Nutzen Sie möglichst keine „*Familien-PCs*“ bzw. keine Familienkonten. Es bietet sich also an, ein separates Gerät oder ein extra passwortgeschütztes Konto für den dienstlichen Kontext auf dem „*Familien-PC*“ zu verwenden. Familienmitglieder dürfen keinen Zugang zu personenbezogenen Daten erhalten, insbesondere auch nicht auf gespeicherte Daten. Ein passwortgeschütztes Konto auf einem gemeinschaftlich genutzten Computer können Sie so einrichten:

  Für Windows 10 klicken Sie hierzu auf „Start“ -> „Einstellungen“ -> „Konten“ -> „Familie und andere Benutzer“ (je nach Betriebssystem). Ein Erklärvideo findet sich auch bei Microsoft direkt (z.B. für Windows 10)

4.4 Videokonferenzen im Home-Office

Im Home-Office wird natürlich nicht nur am Rechner gearbeitet, mit dem Risiko, dass Unbefugte womöglich Daten auf dem Bildschirm einsehen können. Es werden auch Meetings per Videokonferenz abgehalten. Durch den akustischen Informationsaustausch sowie den Einsatz der Kamerafunktion kann ebenso eine unbefugte Offenlegung von personenbezogenen Daten stattfinden. Dabei können nicht nur Daten von Ihren beruflichen Kontakten betroffen sein. Auch Ihre eigenen Familienmitglieder, Freundinnen Ihrer Kinder etc. können beim falschen Umgang mit Videokonferenzen von einer unrechtmäßigen Datenerfassung betroffen sein, wenn diese von der Kamera erfasst werden. Setzen Sie daher bitte folgende Tipps um:



- Stellen Sie Vertraulichkeit sicher, indem Sie Videokonferenzen in räumlich getrennten Bereichen durchführen. Dadurch kann verhindert werden, dass Unbefugte den Inhalt der Konferenzen mithören können. Am besten verwenden Sie Kopfhörer.
- Schaffen Sie einen neutralen Hintergrund (z.B. eine weiße Wand). Damit verhindern Sie, dass versehentlich Familienangehörige im Hintergrund durch das Bild laufen und damit in ihrem Persönlichkeitsrecht auf informationelle Selbstbestimmung eingeschränkt werden. Außerdem verhindern Sie dadurch, dass Ihr privater Wohnraum vom Bild Ihrer Kamera erfasst wird. Dieser sollte stets privat bleiben! Manche Tools wie Microsoft Teams bieten auch die Möglichkeit, dass Sie einen virtuellen Hintergrund einstellen. Auch der Einsatz solcher Features ist empfehlenswert. Im Zweifel können Sie die Bildübertragung auch einfach ausschalten.

Tipps für sichere Passwörter

- Ihr Passwort sollte komplex sein: Mindestlänge 12 Zeichen; Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (4 aus 4 Kriterien).
- Halten Sie so wenige Passwörter wie möglich schriftlich fest und bewahren Sie sämtliche Passwörter an einem sicheren Ort auf, z.B. in einem abgeschlossenen und sicheren Schrank oder in einem entsprechenden Programm auf dem Computer wie dem Passwortsafe „KeePass“ (https://keepass.info/). Das Zugangspasswort zum Passwortsafe sollten Sie sich nicht aufschreiben, sondern merken!
- Damit Sie sich komplexe Passwörter leichter merken können, bilden Sie einen Merksatz und übernehmen Sie die Anfangsbuchstaben. Beispiel: Karla isst um 13 Uhr eine Pizza mit 4 Zutaten. -> Passwort: Kiu13UePm4Z.
- Nutzen Sie jedes Passwort nur einmal und nutzen Sie insbesondere keine Passwörter, die Sie auch im privaten Gebrauch verwenden.

PRÄVENTION VON DATENPANNEN

5.1 Was sind Datenpannen?

Datenpannen sind Datenschutzverletzungen im Umgang mit personenbezogenen Daten. Diese liegen vor, wenn Risiken aus einem fehlerhaften Umgang mit Daten von Betroffenen wie Klienten, Beschäftigten, Mitarbeiterinnen oder Angehörigen drohen. Die möglichen Vorfälle lassen sich z.B. in folgende Kategorien unterteilen:

- Unbewusste/unbeabsichtigte Veröffentlichung von personenbezogenen Daten im Internet
- Hackerangriff, Schadsoftware, Phishing
- Unbefugten werden in einem geschlossenen System Daten zugänglich gemacht
- Missbrauch von Zugriffsrechten
- Verlust von Speichermedien
- E-Mail-Fehlleitungen / unverschlüsselter E-Mail-Versand
- Unterlagen verloren, falsch versendet oder an einem unsicheren Platz gelagert
- Nicht datenschutzgerechte Entsorgung

5.2 Was sind die Herausforderungen bei Datenpannen speziell für soziale Einrichtungen?

Soziale Einrichtungen stehen bei der Verarbeitung von personenbezogenen Daten gleich vor mehreren Herausforderungen. Viele ihrer Angebote bestehen in persönlichen Hilfeleistungen von Menschen für Menschen, wie z.B. der Pflege, Unterstützung von Menschen mit Behinderungen oder psychischen Erkrankungen, Bildungs- oder Betreuungsleistungen für junge Menschen, Wohnangebote, ambulante Hilfsmaßnahme oder integrative Maßnahmen für Menschen mit Migrationshintergrund. All diese Hilfeleistungen haben eines gemeinsam: Sie sind nur möglich, wenn bestimmte personenbezogene Daten

der Klienten bekannt sind. Die Qualität der Betreuung kann je nach Sachverhalt sogar noch höher sein, wenn weitere hilfreiche Daten den sozialen Einrichtungen bekannt sind. So können biographische Daten dabei helfen die Erinnerungsfähigkeit von dementen Personen gezielt anzusprechen. Soziale Einrichtungen stehen damit vor der Herausforderung sensible personenbezogene Daten wie Gesundheitsdaten bzw. Sozialdaten zu verarbeiten. Bei einer Datenpanne drohen besonders hohe Risiken für die Klientinnen.

In den meisten Fällen liegen den Einrichtungen somit **zahlreiche höchstsensible personenbezogene Daten vor, die besonders zu schützen sind**.

Die zweite Herausforderung ergibt sich aus dem Charakter der sozialen Einrichtungen. Häufig sind soziale Einrichtungen offene Häuser. Sie richten sich mit ihren Angeboten an hilfsbedürftige Menschen, d.h. sie wollen offen und erreichbar für diese sein. Sie wollen sich gerade nicht vor der Öffentlichkeit verschließen. Denn das würde dazu führen, dass ein gesellschaftliches Miteinander von Menschen mit und ohne Behinderungen oder zwischen Jung und Alt zusätzlich erschwert werden würde. Aus Sicht des Datenschutzes folgt daraus ein gemindertes Datenschutzniveau. Es gibt offene Häuser statt Pförtner und Werkstore zur Kontrolle des Zutritts. Besucher und Angehörige bewegen sich in den Gängen statt abgesicherten Büroräumlichkeiten, die nur interne Mitarbeiterinnen nutzen.

Häufig sind soziale Einrichtungen offene Häuser – daraus ergeben sich zusätzliche Herausforderungen, den Umgang mit Daten sicherzustellen.

Die dritte Herausforderung besteht in den Mitarbeiterinnen und Mitarbeitern der sozialen Einrichtungen selbst. Ihre Tätigkeit ist für unsere Gesellschaft sehr wichtig, ist für sie jedoch mit hohem Zeitdruck, physischen und psychischen Belastungen und zahlreichen zu beachtenden Regelungen verbunden. In der Praxis bedeutet das, zahlreiche Schulungen zu Pflegestandards, Hygiene, ggf. Gebärdensprache, korrekter Umlagerung von Klienten, Brandschutz etc. – und dann kommt auch noch der Datenschutz.
Da bleibt nur wenig Zeit für Hinweise zum Umgang mit Daten oder zum sicheren und angemessenen Umgang mit E-Mail, PC, Apps auf Smartphones - denn auch die Abläufe von sozialen Einrichtungen werden zunehmend digital unterstützt.

Mitarbeiter in sozialen Einrichtungen sind hohen Arbeitsbelastungen ausgesetzt und es bleibt wenig Zeit, sie für den sicheren Umgang mit Daten und der IT zu schulen.

5.3 Häufige Datenschutzrisiken in sozialen Einrichtungen

Als Datenschutzberater begegnen uns in der täglichen Praxis unterschiedlichste Sachverhalte, die zu Datenpannen führen können oder bereits zu konkreten Datenschutzverletzungen geführt haben. Daher hoffen wir, dass diese Beispiele zur Sensibilisierung beitragen und helfen, ähnliche Vorfälle zu vermeiden.

E-Mail-Fehlleitungen / unverschlüsselter E-Mail-Versand / Fax-Versand

Soziale Einrichtungen kommunizieren mit zahlreichen externen Kommunikationspartnern. Dies sind z.B. Arztpraxen, Kostenträger wie Ämter und Behörden, Agentur für Arbeit, Krankenkassen etc. Glücklicherweise beobachten wir, dass viele der genannten externen Stellen zunehmend Möglichkeiten eines sicheren Datenaustausches anbieten. Beispielsweise bietet die Agentur für Arbeit in der Zusammenarbeit eine Plattform für den verschlüsselten Datenaustausch an. Auch einzelne Landratsämter nutzen Plattformen, die ihnen die jeweiligen Bundesländer zur Verfügung stellen.

Leider erlebten wir das im ersten und zweiten Quartal 2020 jedoch auch anders und durften mit zahlreichen Landratsämtern lebhaft diskutieren, warum Excel-Listen mit Daten von Pflegeheimbewohnern und einzelnen Gesundheitsdiagnosen vielleicht nicht einfach unverschlüsselt per E-Mail versendet werden sollten. Die Beratungsresistenz einzelner Ansprechpartner auf Behördenseite ist nicht nachvollziehbar - dass Datenschutz nicht über allem steht, ist uns auch klar. Leider sind diese Mängel jedoch nicht nur in Zeiten von Corona, sondern auch zu normalen Zeiten ein übliches Ärgernis. Auch der Datenaustausch via Fax an Arztpraxen ist ein häufiges Problem in der Praxis.

→ Unsere Praxisempfehlungen zur Prävention einer Datenpanne

Klären Sie mit externen Adressaten, wie Sie besonders schützenswerte Inhalte sicher übermitteln können.

- **Offizielle Plattform:** Gibt es die Möglichkeit eine offizielle Plattform zu verwenden, bei der Sie sich anmelden müssen und dann ein Dokument sicher hochladen können?
- **Datenaustausch per Plattform der IT:** Falls die Empfängerin dies nicht kann, gibt es eine offizielle Lösung aus Ihrem Haus? Fragen Sie bei Ihrer IT nach. Mittlerweile bieten die IT-Abteilungen immer häufiger solche Lösungen an.
- **Verschlüsselte Zip-Datei/PDF:** Wenn es keine Möglichkeit per Plattform gibt, so können Sie einen verschlüsselten Anhang erzeugen und diesen einer E-Mail anhängen, die Sie an Ihren Ansprechpartner schicken. Dann müssen Sie noch das Passwort zum Entschlüsseln der Datei Ihrer Ansprechpartnerin über einen separaten Kanal zukommen lassen (z.B. per Telefon, per SMS, per Messenger, persönlich oder postalisch). Bitte achten Sie darauf, dass im Mailbetreff keine personenbezogenen Daten genannt sind. Eine genaue Anleitung finden Sie hier.
- **Fax-Versand:** Sensible Gesundheitsdaten sollten Sie nicht mehr per Fax übermitteln. Die Übermittlung erfolgt wie bei einer E-Mail und ist somit nicht als ausreichend sicher zu bewerten. Wenn es keine sicheren Alternativen gibt, dann sollten Sie zumindest die folgenden Hinweise berücksichtigen. Was sind mögliche Fehlerquellen?
    - Fehlversand an einen falschen Empfänger – Sorgfältige Nummerneingabe oder Hinterlegung der Nummer im Speicher, um Fehleingaben zu vermeiden.
    - Prüfung von Sendeprotokollen, ob das Fax tatsächlich an die gewünschte Rufnummer übermittelt wurde. Laut (kirchlichen) Aufsichtsbehörden sind die Protokolle für 3 Monate aufzubewahren und anschließend datenschutzkonform per Entsorgungsbehälter oder Aktenvernichter zu entsorgen.
    - Gelegentliche Kontrolle der gespeicherten Rufnummern – Prüfung, ob die hinterlegten Rufnummern noch korrekt sind oder auch gelöscht werden können, wenn diese nicht mehr erforderlich sind.

Bei wichtigen / vertraulichen Faxsendungen

- Telefonische Ankündigung. Dadurch stellen Sie sicher, dass Ihr Empfänger die Faxsendung unmittelbar entgegennehmen kann.
- Telefonische Rückversicherung. Dadurch stellen Sie sicher, dass die Empfängerin die Faxsendung wirklich erhalten hat. Eine Bitte zur telefonischen Bestätigung kann auch auf dem Fax-Vordruck erbeten werden. Berücksichtigen Sie dies insbesondere, wenn Sie wissen, dass das Faxgerät beim Empfänger in einem *„Taubenschlag“* steht.

Beim Aufstellen von Faxgeräten zu beachten

- Bitte stellen Sie das Faxgerät nur an Orten auf, an denen keine unbefugten Personen Zugriff auf eingegangene Faxsendungen haben.
- Bitte stellen Sie sicher, dass durch regelmäßige Kontrollgänge keine Faxsendungen *„herrenlos“* liegen bleiben.

Bei der Entsorgung von Faxgeräten zu beachten

- Bitte löschen Sie die eingegebenen Rufnummern aus den lokalen Speichern.
- Bitte übergeben Sie das Gerät an die IT, damit diese eine abschließende datenschutzkonforme Löschung anstoßen kann

Unbewusste/unbeabsichtigte Veröffentlichung von personenbezogenen Daten

Immer wieder kommt es zu unbeabsichtigten Veröffentlichungen personenbezogener Daten in sozialen Einrichtungen. Diese können sowohl nach innen als auch nach außen erfolgen. In einem leicht veränderten realen Fall legte ein Betriebsratsmitglied Unterlagen eines Kündigungsverfahrens aus Versehen in einem für alle Mitarbeiterinnen zugänglichen Netzlaufwerk ab. Bei einem solchen Vorfall kann nicht ausgeschlossen werden, dass mehrere Mitarbeiter auf dieses Dokument aus Versehen oder aus Neugier zugreifen.

→ Unsere Praxisempfehlung zur Prävention dieser Datenpanne

Rein technisch lässt sich dieser Sachverhalt so gut wie nicht verhindern. Natürlich könnte man nicht erforderliche Berechtigungen dieses Benutzers entfernen lassen. Das geht jedoch nur, wenn alle Aufgaben ohne diese Berechtigung noch durchgeführt werden können. Ansonsten hilft hier nur Sensibilisierung, Sensibilisierung und nochmals Sensibilisierung. Gerade im Umgang mit höchstsensiblen Unterlagen zählt jeder Handgriff bzw. jeder Klick.

In einem anderen skurrilen Fall leitete sich ein Mitarbeiter betriebliche E-Mails mit Personalsachverhalten an eine private E-Mail-Adresse und verarbeitete diese auf seinem privaten Endgerät. Was anfangs vielleicht noch unter die Kategorie *„besonders fleißiger Mitarbeiter“* gefallen wäre, entpuppte sich im weiteren Verlauf als renitentes und fundamental falsches Verständnis des Umgangs mit Daten. Trotz Ermahnungen und Hinweisen, wie diese Daten zu verarbeiten sind, zeigte dieser Mitarbeiter keine Einsicht eines Fehlverhaltens.

→ Unsere Praxisempfehlung zur Prävention dieser Datenpanne

Dieses Beispiel zeigt leider, dass Sensibilisierung und Schulung nicht in jedem Fall zum gewünschten Erfolg führen. Aus unserer Erfahrung ist das jedoch die absolute Ausnahme. In den meisten Fällen erleben wir viele Mitarbeiterinnen sehr einsichtig und interessiert, wie sie mit Daten umgehen dürfen. Insbesondere die Hinweise zum Eigenschutz vor gut gemeintem, jedoch schadhaftem Verhalten, stoßen in der Regel auf großes Interesse. Wenn eine Einsicht nicht vorhanden ist, dann geht es ausnahmsweise nur mit arbeitsrechtlichen oder strafrechtlichen Mitteln, das ist jedoch die absolute Ausnahme.

ÜBER DIE AUTOREN

Erstellt von der ENSECUR GmbH in gemeinsamer Ausarbeitung von Steven Bösel, Mareike Fischer, Julian Häcker, Thorsten Jordan und Bastian Maute (in alphabetischer Reihenfolge).

ENSECUR ist ein Beratungsunternehmen für Datenschutz und Datensicherheit. Wir unterstützen als Datenschutzbeauftragte kleine und mittelständische Unternehmen im Südwesten (Baden-Württemberg, Rheinland-Pfalz, Hessen), insbesondere:

- Softwareunternehmen mit Datenschutzanforderungen von Auftraggebern
- Soziale Einrichtungen mit gesetzlichen und kirchlichen Datenschutzanforderungen
- Industrieunternehmen mit gesetzlichen Datenschutzanforderungen
- Organisationen mit der Motivation, Datenschutz besser machen zu wollen

Mission
Wir brennen für Datenschutz und wollen diese Begeisterung an Sie und Ihre Organisation weitergeben, um gemeinsam mit Ihnen Ihre Datenschutzziele zu erreichen.

Bildquellen
Titel: Bild von Anemone123 auf Pixabay
S. 5: Bild von Tumisu auf Pixabay
S. 7: Bild von Kevin Phillips auf Pixabay
S. 12: Bild von Catkin auf Pixabay
S. 17: Bild von everesd_design auf Pixabay
S. 20: Bild von talha khalil auf Pixabay
Grafik auf den S. 18,19,20: Bild von IO-Images auf Pixabay

Bitte beachten Sie, dass dieses White Paper trotz großer Sorgfalt keinen Anspruch auf Vollständigkeit hat und natürlich auch keine rechtliche Empfehlung bedeuten soll. Aufgrund der hohen Dynamik sind alle Angaben ohne Gewähr.