ARBEITSSCHUTZ UND HYGIENE IM GESUNDHEITSWESEN

RECHTSSICHERHEIT SCHAFFEN • FACHWISSEN ERHALTEN • ARBEITSALLTAG ERLEICHTERN

DSGVO PRAXISNAH GESTALTEN



DATENSCHUTZ: WENN DOCH ETWAS SCHIEFGEHT

So erkennen und bewältigen Sie Datenschutzvorfälle sicher – mit Abläufen für den Ernstfall. **S. 3**

DATENSCHUTZ-VORFÄLLE SOUVERÄN MEISTERN

Wie Sie Datenschutzvorfälle Schritt für Schritt bewerten, bearbeiten und abschließen. **S. 5**

UMGANG MIT PERSONENBEZOGENEN DATEN

Lesen Sie, welche DSGVO-Grundsätze Sie bei jeder Datenverarbeitung beachten müssen. **S. 10**

SAFETYXPERTS
Ihre Spezialisten für Arbeitssicherheit

DAS EXPERTENTEAM



Ricarda Waldon

Ihre Expertin für Qualitätsmanagement im Gesundheitswesen: Ricarda Waldon leitete über 15 Jahre das Qualitätsmanagement eines Gesundheitsdienstleisters mit 90 Standorten und 1.200 Mitarbeitern. Dabei war sie auch als Expertin für die Themengebiete Arbeitssicherheit, Hygiene, Medizinprodukte, Datenschutz und Informationssicherheit verantwortlich. In diesen Themen absolvierte sie auch diverse Weiterbildungen. Derzeit ist sie als Expertin für Datenschutz in der IT tätig.

Datenschutz beginnt im Alltag

Liebe Leserin, lieber Leser,

Patientendaten gehören zu den sensibelsten Informationen überhaupt – und deren Schutz ist weit mehr als eine gesetzliche Pflicht. Schon kleine Unachtsamkeiten können Datenschutzverstöße nach sich ziehen. In dieser Ausgabe erfahren Sie, welche Grundlagen der Datenschutz-Grundverordnung (DSGVO) Sie kennen sollten und wie Sie diese praxisnah umsetzen. Darüber hinaus begleiten wir Sie in weiteren Beiträgen durch den gesamten Prozess eines Datenschutzvorfalls – von der Erkennung und Risikobewertung über die Meldung bis hin zur Information Betroffener und der anschließenden Nachbereitung. So erhalten Sie einen umfassenden Leitfaden für den sicheren Umgang mit personenbezogenen Daten im Gesundheitswesen.

Viel Spaß beim Lesen!

Ihre

Ricarda Waldon

ALLES INKLUSIVE

Onlinebereich

Nutzen Sie über 500 Checklisten, Muster und Vorlagen unter: **safetyxperts.de/login**

Spezialreports & Facharchiv

Möchten Sie in ein Thema tiefer eintauchen, finden Sie praktische E-Books und Arbeitshilfen.

Fragen an die Xperten

Stellen Sie Ihre individuellen Fragen zum Thema Arbeitsschutz gerne über das Kontaktformular auf **safetyxperts.de/login**

Videos & Webinare

Im Onlinebereich finden Sie unter „Videos" und „Veranstaltungen" praktische Inhalte für Ihre Unterweisung.

Wenn etwas schiefgeht: So beherrschen Sie Datenschutzvorfälle sicher

Ein unaufmerksamer Moment, ein falscher Klick und es ist passiert: Die E-Mail mit einem medizinischen Befund ging unverschlüsselt an den falschen Thomas Schneider. Oder: Ihr neuer Mitarbeiter hat es gut gemeint und die alten Patientenakten im Altpapiercontainer entsorgt, weil er Platz schaffen wollte. Beide Situationen sind Datenschutzvorfälle – auch wenn weder Hacker noch Schadsoftware beteiligt waren. Tatsächlich entstehen viele Datenschutzverletzungen im Alltag durch kleine menschliche Fehler. Umso wichtiger ist es, dass Ihre Gesundheitseinrichtung weiß, wie im Ernstfall richtig gehandelt wird.

Das ist ein Datenschutzvorfall

Häufig wird mit einem Datenschutzvorfall verbunden, dass Unbefugte Zugriff auf personenbezogene Daten erhalten. Das ist allerdings nur ein Aspekt. Die DSGVO definiert einen Datenschutzvorfall als „….jede Verletzung der Sicherheit personenbezogener Daten, durch die Daten unbeabsichtigt oder unrechtmäßig vernichtet, verändert, verloren, offengelegt oder unbefugt zugänglich werden." Dies bedeutet:

- Unbeabsichtigte Zerstörung / Verlust von personenbezogenen Daten (z. B. Patientenakten verbrennen, Daten werden gelöscht, unzugänglich verschlüsselt)
- Unbeabsichtigte Veränderung der gespeicherten Daten (z. B. bei einer Datenmigration werden die Kontonummern Ihrer Mitarbeiter vertauscht)
- Unberechtigtes Bekanntwerden von personenbezogenen Daten (Berechtigungen wurden aus Versehen falsch gesetzt und unberechtigte Personen haben Zugriff auf die Adressdaten von Mitarbeitern, Verlust eines unverschlüsselten USB-Sticks mit personenbezogenen Daten, Cyberangriff mit Datenklau)

Weitere Beispiele für potenzielle Datenschutzvorfälle sind:

- Medikamentenplan wird an den falschen Patienten geschickt.
- Arztbrief landet im falschen Briefumschlag.
- Ausdruck mit Laborwerten bleibt im Wartezimmer liegen.
- Mitarbeiter fotografiert Patientenakte mit privatem Smartphone.
- Patienten werden im offenen Wartebereich mit vollständigem Namen und Diagnose aufgerufen.

Wichtig

Die Regelungen gelten ausschließlich für personenbezogene Daten. Versenden Sie z. B. versehentlich Geschäftszahlen an Ihren Newsletter-Verteiler, ist dies zwar ein unerwünschter Vorfall, aber kein Datenschutzvorfall.

Besonderheiten bei der Auftragsverarbeitung

Damit es sich um „Ihren" Datenschutzvorfall handelt, müssen Sie außerdem Verantwortlicher für die Datenverarbeitung sein. Als Verantwortlicher entscheiden Sie über Zwecke und Mittel der Verarbeitung personenbezogener Daten. Anders verhält es sich bei Auftragsverarbeitern: Wenn Sie Daten im Auftrag eines anderen Verantwortlichen verarbeiten – beispielsweise als IT-Dienstleister oder Callcenter – und dabei einen Datenschutzvorfall feststellen oder verursachen, müssen Sie den Verantwortlichen unverzüglich darüber informieren. Dieser übernimmt die weiteren Schritte und prüft insbesondere die erforderlichen Maßnahmen. Dafür ist er auf Ihre Unterstützung und die Bereitstellung aller relevanten Informationen angewiesen. Als Gesundheitseinrichtung treten Sie jedoch in der Regel als Verantwortlicher und nicht als Auftragsverarbeiter auf.

Wichtig

Verursacht Ihr IT-Dienstleister einen Datenschutzvorfall, bleiben Sie als Verantwortlicher erst einmal gegenüber der Aufsichtsbehörde verantwortlich.

Verursacht ein Auftragsverarbeiter (z. B. IT-Dienstleister oder Abrechnungsdienstleister) einen Datenschutzvorfall mit Ihren personenbezogenen Daten, bleiben Sie als Verantwortlicher in der Pflicht. Regeln Sie deshalb bereits im Vertrag, wer wann, wie und mit welchen Informationen informiert.

Achten Sie hierbei insbesondere auf den Zeitraum, in dem Ihr Dienstleister Sie informieren muss. Da Sie einen Vorfall gegebenenfalls innerhalb von 72 Stunden melden müssen, sollten Sie Ihren Dienstleister dahingehend verpflichten, Sie innerhalb von 24 Stunden zu informieren.

Prüfen Sie genau bei der für Sie zuständigen Aufsicht, wann die Frist zur Meldung eines Datenschutzvorfalls zu laufen beginnt. Bei der bayerischen Datenschutzaufsicht z. B. zählen die 72 Stunden ab 0:00 Uhr des Folgetages, an dem die Datenschutzverletzung in Ihrer Einrichtung festgestellt wurde. Dies bedeutet, dass bei einer Verletzung, die am Donnerstag um 16:00 Uhr festgestellt wird, die 72-Stunden-Frist am Sonntag um 23:59 Uhr abläuft. Bei der Festlegung der 72 Stunden werden Wochenenden und Feiertage mitgerechnet.

Die bayerische Datenschutzaufsicht geht davon aus, dass die 72-Stunden-Frist bereits mit einem hinreichenden Verdacht auf eine Datenschutzverletzung beginnt. So soll verhindert werden, dass Meldefristen durch lange Prüfungen verzögert werden. Da andere Aufsichtsbehörden dies teilweise anders auslegen, sollten Sie die für Sie geltende Regelung prüfen.

Fazit

Datenschutzvorfälle lassen sich nicht immer verhindern – entscheidend ist jedoch, wie Ihre Gesundheitseinrichtung darauf reagiert. Im nächsten Artikel lesen Sie, wie Sie einen Prozess etablieren können, damit Ihnen alle potenziellen Datenschutzvorfälle zeitnah gemeldet werden.

So etablieren Sie einen Meldeprozess für Datenschutzvorfälle

In Arztpraxen und Pflegeeinrichtungen werden täglich besonders schützenswerte Gesundheitsdaten verarbeitet. Kommt es zu einer Verletzung des Datenschutzes, verlangt die Datenschutz-Grundverordnung (DSGVO) ein schnelles Handeln. Besteht ein Risiko für die Rechte und Freiheiten der betroffenen Personen, muss der Vorfall innerhalb von 72 Stunden nach Kenntniserlangung an die zuständige Datenschutzaufsichtsbehörde gemeldet werden.

In der Praxis scheitert dies jedoch häufig nicht an der fehlenden Bereitschaft, sondern daran, dass Mitarbeitende nicht wissen:

- Was ist überhaupt ein Datenschutzvorfall?
- An wen muss der Datenschutzvorfall gemeldet werden?
- Welche Informationen werden benötigt?
- Wer entscheidet über das weitere Vorgehen?

Ein klar definierter Meldeprozess beantwortet diese Fragen bereits, bevor ein Vorfall eintritt.

Schritt 1: Datenschutzvorfälle eindeutig definieren

Nicht jeder Mitarbeitende verfügt über datenschutzrechtliche Kenntnisse. Deshalb sollten Sie Ihre internen Richtlinien möglichst verständlich formulieren.

Eine einfache Definition lautet:

Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten versehentlich oder unrechtmäßig verloren gehen, verändert, gelöscht oder unbefugten Personen offengelegt oder zugänglich gemacht werden. Ergänzen Sie diese Definition am besten durch praxisnahe Beispiele.

Schritt 2: Eine niedrige Meldehürde schaffen

Der häufigste Fehler besteht darin, dass Mitarbeitende zunächst selbst beurteilen möchten, ob tatsächlich ein Datenschutzvorfall vorliegt. Das sollten sie ausdrücklich nicht tun. Die interne Regel muss stattdessen lauten:

Jeder Verdacht wird gemeldet. Die Bewertung übernimmt die verantwortliche Stelle.

Dadurch gehen keine wertvollen Stunden verloren und Unsicherheiten führen nicht dazu, dass Vorfälle verschwiegen werden.

Schritt 3: Klare Verantwortlichkeiten festlegen

Jeder Mitarbeitende muss wissen, an wen ein Vorfall gemeldet wird. Regeln Sie das am besten über ein digitales Formular, das automatisch an den korrekten Empfänger geschickt wird. Die Meldung sollte direkt an die verantwortliche Datenschutzabteilung gehen, ohne dass diese vorher durch den Vorgesetzten des Absenders geprüft wird.

Für die Datenschutzbeauftragten Ihrer Einrichtung ist es wichtig, dass Vertretungsregelungen definiert werden. Datenschutzvorfälle halten sich nicht an Öffnungszeiten oder Urlaubspläne. Eine Meldung ist nur wirksam, wenn sie die zuständige Stelle erreicht und bearbeitet werden kann.

Schritt 4: Ein standardisiertes Meldeformular verwenden

Ein Meldeformular für alle Ihre Mitarbeitenden verhindert, dass wichtige Informationen fehlen. Ein digitales Meldeformular erleichtert die Erfassung von Datenschutzvorfällen. So können Vorfälle schnell und einheitlich dokumentiert werden. Ermöglichen Sie auch anonyme Meldungen, um Hemmschwellen zu senken. Je einfacher das Formular aufgebaut ist, desto vollständiger sind die Angaben.

MELDEFORMULAR „DATENSCHUTZVORFALL“

Bitte vollständig ausfüllen und umgehend an die zuständige Stelle weiterleiten.

1. Angaben zur meldenden Person (auch anonyme Meldung möglich)

Name, Vorname: _____

Funktion / Abteilung: _____

Telefon / E-Mail: _____

Datum und Uhrzeit der Meldung: _____

2. Angaben zum Vorfall

Datum und Uhrzeit des Vorfalls (falls bekannt): _____

Ort des Vorfalls: _____

Wie wurde der Vorfall festgestellt?

❑ selbst bemerkt ❑ von Dritten mitgeteilt ❑ durch System / IT erkannt ❑ Sonstiges: _____

Das Meldeformular Datenschutzvorfall können Sie unter **safetyxperts.de/login** downloaden.

Vom Eingang der Meldung bis zur Lösung: Datenschutzvorfälle sicher bearbeiten

Sie haben einen Meldeprozess für Datenschutzvorfälle etabliert und nun passiert es – die erste Meldung trifft ein. Wie gehen Sie jetzt am besten damit um?

Prüfen Sie zunächst, ob die Meldung tatsächlich einen potenziellen Datenschutzvorfall betrifft. Wenn Sie ein Meldewesen etabliert haben, werden darüber erfahrungsgemäß auch andere Anliegen oder Hinweise eingehen, die keinen Datenschutzverstoß darstellen. Ergibt die Prüfung jedoch einen möglichen Datenschutzvorfall, gehen Sie wie folgt vor:

1. Evaluieren Sie den Sachverhalt

Prüfen Sie, was genau passiert ist und ob Informationen für Ihre vollständige Bearbeitung fehlen (in den meisten Fällen wird dies so sein). Suchen Sie einen Ansprechpartner, den Sie zu dem Vorfall befragen können, z. B. die meldende Person, Applikationsverantwortliche oder Verantwortliche für den Bereich, in dem die Verarbeitung stattfindet. Gegebenenfalls fragen Sie auch Ihre Cybersecurity-Abteilung für weitere Analysen. Zuerst müssen Sie aber prüfen, ob sofortiger Handlungsbedarf besteht.

2. Sofort handeln – bevor Sie melden

Unmittelbar nach Bekanntwerden sollten Sie zunächst den Schaden begrenzen.

Beispiele:

- falsche E-Mail möglichst zurückrufen
- Empfänger kontaktieren
- Benutzerkonto sperren
- Passwort ändern
- verlorenes Gerät aus der Ferne löschen
- IT-Dienstleister informieren
- Backups prüfen
- Beweise sichern
- Cybersecurity-Versicherung informieren.

Erst danach erfolgen die Dokumentation und Bewertung.

3. Dokumentieren Sie Ihre Ergebnisse

Für jede Meldung, die ein potenzieller Datenschutzvorfall sein könnte, dokumentieren Sie sorgfältig und nachvollziehbar Ihre vollständige standardisierte Analyse – auch, wenn Sie nicht an die Behörde melden müssen.

Ihre Dokumentation zur Evaluation der Meldung könnte so aussehen:

EVALUIERUNGSBOGEN „DATENSCHUTZVORFALL“

Bitte vollständig ausfüllen und umgehend an die zuständige Stelle weiterleiten.

1 Angaben zur meldenden Person

Name, Vorname:	Funktion / Abteilung:
Telefon / E-Mail:	Datum und Uhrzeit der Meldung:
Fristbeginn (Kenntnisnahme):	Meldefrist läuft ab am:

2 Angaben zum Vorfall

Beginn der Datenschutzverletzung:	Ende der Datenschutzverletzung:
Ort des Vorfalls:	
Wie wurde der Vorfall festgestellt?	
Beschreibung des Vorfalls (Was ist passiert? Wie ist es passiert?):	

Den Evaluierungsbogen „Datenschutzvorfall“ können Sie unter **safetyxperts.de/login** downloaden.

Fortsetzung auf Seite **6**

FORTSETZUNG VON SEITE 5 **Vom Eingang der Meldung bis zur Lösung: Datenschutzvorfälle sicher bearbeiten**

4. Melden Sie den Verstoß Ihrer Datenschutzaufsichtsbehörde

Ein Datenschutzvorfall ist grundsätzlich unverzüglich und innerhalb von 72 Stunden zu melden, es sei denn, die Verletzung führt voraussichtlich zu keinem Risiko für die Rechte und Freiheiten der betroffenen Personen.

Für die Meldung stellen die Datenschutzbehörden in der Regel Online-Formulare bereit, die Sie auf der Webseite Ihrer zuständigen Aufsichtsbehörde finden. Die 72-Stunden-Frist beginnt, sobald Ihnen der Datenschutzvorfall bekannt wird.

Stellen Sie beispielsweise heute fest, dass vor drei Monaten aufgrund falscher Berechtigungen ein unbefugter Zugriff auf Mitarbeiterbeurteilungen möglich war, beginnt die Meldefrist erst mit dieser Kenntnisnahme.

Das bedeutet für Sie: Sie sollten bereits im Vorfeld festlegen, wie Sie bei einem gemeldeten Datenschutzvorfall vorgehen, und diese Abläufe im Team bekannt machen. Nur so können Sie die Meldefrist zuverlässig einhalten.

Was tun, wenn die 72-Stunden-Frist nicht eingehalten werden kann?

Was aber, wenn Sie die Frist nicht einhalten können? In diesem Fall können Sie zunächst die Informationen melden, die Ihnen bereits vorliegen, und fehlende Angaben später nachreichen. Die Verzögerung müssen Sie jedoch begründen (Folgemeldung). Besser ist es, den Vorfall von Anfang an möglichst vollständig zu melden.

Welche Informationen werden im Meldeformular der Datenschutzaufsicht abgefragt? Im Wesentlichen handelt es sich um ähnliche Angaben wie im Evaluierungsbogen für den Datenschutzbeauftragten. Bei Datenschutzvorfällen durch Malware, Cyberangriffe oder Ransomware werden zusätzlich technische Details zum Vorfall benötigt.

Das Meldeformular finden Sie auf der Webseite der für Sie zuständigen Datenschutzbehörde. Benutzen Sie am besten die folgende Checkliste, um zu prüfen, ob Sie an alles gedacht haben.

Datenschutzvorfall – was zu tun ist

Nutzen Sie diese Checkliste, um im Ernstfall strukturiert und rechtssicher zu handeln.

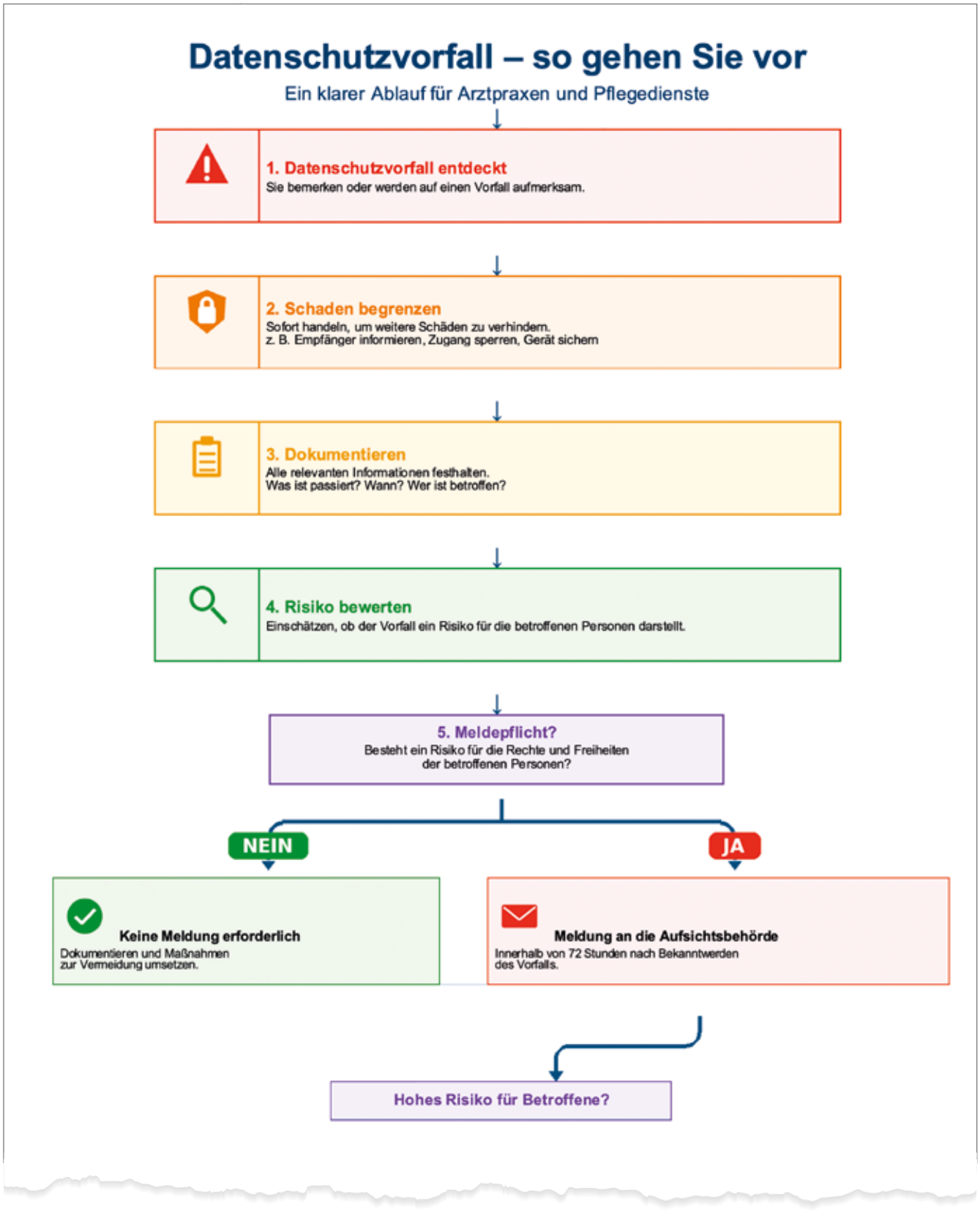
	1	**Vorfall entdeckt / gemeldet** Meldung ernst nehmen und sofort reagieren.	☐
	2	**Schaden begrenzen** Weitere Datenverluste verhindern und sofort Maßnahmen ergreifen (z. B. Systeme sperren, Zugriff entziehen).	☐
	3	**Datenschutzbeauftragten informieren** Den Datenschutzbeauftragten unverzüglich einbeziehen.	☐
	4	**Dokumentation beginnen** Den Vorfall vollständig und nachvollziehbar dokumentieren (alle relevanten Informationen sichern).	☐
	5	**Risiko bewerten** Bewerten, ob der Vorfall ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.	☐
	6	**Meldung an Aufsichtsbehörde prüfen** Wenn erforderlich, Meldung innerhalb von 72 Stunden vorbereiten und übermitteln.	☐
	7	**Betroffene informieren** Bei hohem Risiko Betroffene so schnell wie möglich informieren (klar, verständlich und transparent).	☐
	8	**Ursachenanalyse durchführen** Ursachen des Vorfalls analysieren und Schwachstellen identifizieren.	☐
	9	**Maßnahmen umsetzen** Technische und organisatorische Maßnahmen ergreifen, um den Vorfall zu beheben und Wiederholungen zu verhindern.	☐
	10	**Mitarbeitende sensibilisieren** Mitarbeitende informieren und ggf. schulen, um das Bewusstsein für Datenschutz und Informationssicherheit zu stärken.	☐

Die Checkliste zum Datenschutzvorfall können Sie unter **safetyxperts.de/login** downloaden.

Mein Tipp

Testen Sie Ihren Prozess regelmäßig und passen Sie ihn bei Bedarf an. So sind Sie im Ernstfall gut vorbereitet.

Das folgende Prozessdiagramm führt Sie Schritt für Schritt durch den Ablauf – von den ersten Sofortmaßnahmen über Dokumentation und Risikobewertung bis hin zu möglichen Melde- und Informationspflichten. So behalten Sie auch unter Zeitdruck den Überblick und stellen sicher, dass notwendige Maßnahmen rechtzeitig eingeleitet werden.



Das Ablaufdiagramm für den Datenschutzvorfall können Sie unter **safetyxperts.de/login** downloaden.

Fazit

Datenschutzvorfälle lassen sich trotz aller Vorsichtsmaßnahmen nicht vollständig vermeiden. Entscheidend ist daher nicht nur, wie gut Ihre technischen und organisatorischen Maßnahmen sind, sondern auch, wie professionell Sie im Ernstfall reagieren. Ein klar definierter Meldeprozess, geschulte Mitarbeitende und eine vollständige Dokumentation helfen, Schäden für Betroffene zu begrenzen und die gesetzlichen Anforderungen der Datenschutz-Grundverordnung einzuhalten. Wer vorbereitet ist, schützt nicht nur personenbezogene Daten, sondern auch das Vertrauen von Patienten, Angehörigen und Mitarbeitenden.

So informieren Sie die Betroffenen eines Datenschutzvorfalls

Bei einem hohen Risiko für die Betroffenen eines Datenschutzvorfalls müssen Sie diese über den Datenschutzvorfall informieren. In anderen Fällen möchten Sie die Betroffenen vielleicht freiwillig informieren, um sie vor potenziellen Auswirkungen zu schützen (z. B. Phishing-Versuche). Erfahren Sie in diesem Artikel, worauf Sie bei der Information betroffener Personen achten müssen und wie Sie dies praxisgerecht gestalten.

Informieren Sie so bald wie möglich, soweit der Vorfall ein hohes Risiko für die Betroffenen mit sich bringt. Ob es ein hohes Risiko ist, kommt auf die genaue Situation an. Lassen Sie sich auf jeden Fall von Ihrem Datenschutzbeauftragten oder der Aufsichtsbehörde beraten.

Download-Tipp

Eine genauere Betrachtung dieses Themas bietet auch das Kurzpapier der Deutschen Datenschutzkonferenz, das Sie unter: **kurzlinks.de/snlu** lesen können.

Vergessen Sie nicht, dass die Betroffenen auch Ihre Mitarbeitenden sein können.

Datenschutzvorfall: So informieren Sie betroffene Personen

Nachfolgend finden Sie ein Muster für die Information betroffener Personen über einen Datenschutzvorfall.

Information über einen Datenschutzvorfall

Sehr geehrte/r Frau/Herr [Name],
der Schutz Ihrer personenbezogenen Daten hat für unsere Einrichtung höchste Priorität. Leider müssen wir Sie darüber informieren, dass es am [Datum] zu einem Datenschutzvorfall gekommen ist, von dem auch Ihre personenbezogenen Daten betroffen sein können.

Was ist passiert?
Am [Datum] wurde festgestellt, dass [kurze Beschreibung des Vorfalls, z. B. ein Arztbrief versehentlich an einen falschen Empfänger versendet wurde / ein mobiles Endgerät mit Patientendaten verloren gegangen ist / Unbefugte zeitweise Zugriff auf bestimmte Daten hatten].

Welche Daten sind betroffen?
Nach unserem derzeitigen Kenntnisstand betrifft dies folgende Daten:
- Name
- Anschrift
- Kontaktdaten
- Gesundheitsdaten / Behandlungsdaten (soweit zutreffend)
- weitere betroffene Daten: _____

Welche Folgen sind möglich?
Je nach Art der betroffenen Daten besteht das Risiko, dass personenbezogene Informationen unbefugt bekannt oder missbräuchlich verwendet werden. Nach derzeitigem Stand liegen uns [keine Hinweise / Hinweise] auf einen Missbrauch Ihrer Daten vor.

Welche Maßnahmen haben wir bereits ergriffen?
Wir haben den Vorfall unverzüglich untersucht und geeignete Maßnahmen eingeleitet. Dazu gehören insbesondere:
- Behebung der Ursache des Vorfalls,
- Sicherung der betroffenen Systeme,
- Überprüfung unserer technischen und organisatorischen Maßnahmen,
- ggf. Information der zuständigen Datenschutzaufsichtsbehörde.

Was können Sie selbst tun?
Sollten ungewöhnliche Kontaktaufnahmen, verdächtige E-Mails oder andere Auffälligkeiten auftreten, empfehlen wir Ihnen, diese sorgfältig zu prüfen und sich bei Fragen oder Unsicherheiten unmittelbar an uns zu wenden.

Fragen?
Wenn Sie Fragen zum Vorfall oder zur Verarbeitung Ihrer personenbezogenen Daten haben, erreichen Sie uns unter:
[Name der Einrichtung]
[Ansprechpartner]
Telefon: _____
E-Mail: _____
Sofern ein Datenschutzbeauftragter benannt wurde:
Datenschutzbeauftragte/r_____
Telefon: _____
E-Mail: _____
Wir bedauern diesen Vorfall sehr und entschuldigen uns für die entstandenen Unannehmlichkeiten. Gleichzeitig versichern wir Ihnen, dass wir alles daransetzen, vergleichbare Vorfälle künftig zu vermeiden.
Mit freundlichen Grüßen
[Name der Einrichtung]

Die Information an Betroffene sollte klar und einfach formuliert sein. Beschreiben Sie den Vorfall ehrlich, erläutern Sie mögliche Folgen und nennen Sie konkrete Ansprechpartner. Vermeiden Sie Fachbegriffe und Spekulationen. Informieren Sie erst, wenn feststeht, dass voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht und die Fakten zum Vorfall geklärt sind.

Fazit

Auch wenn ein Datenschutzvorfall für Ihre Einrichtung unangenehm ist und negative Medienberichte nach sich ziehen kann, können Sie durch offene, transparente und professionelle Kommunikation das Vertrauen der Betroffenen bewahren oder zurückgewinnen.

„Muss ich von jedem Patienten eine Einwilligung zur Datenverarbeitung einholen?“

Frage: *„In unserer Arztpraxis unterschreibt jeder neue Patient eine Einwilligung zur Verarbeitung seiner personenbezogenen Daten. Nun habe ich gehört, dass dies gar nicht erforderlich sein soll. Stimmt das?“*

Antwort: Das kommt darauf an. Eine Einwilligung zur Verarbeitung personenbezogener Daten ist in einer Arztpraxis nicht zwingend erforderlich. Tatsächlich gehört sie zu den häufigsten Missverständnissen im Datenschutz. Die Verarbeitung von Patientendaten erfolgt in erster Linie, um den Behandlungsvertrag zu erfüllen. Darüber hinaus bestehen zahlreiche gesetzliche Verpflichtungen, beispielsweise zur Dokumentation und Aufbewahrung von Patientenakten. Für diese Verarbeitungen bildet die Datenschutz-Grundverordnung (DSGVO) bereits eine ausreichende Rechtsgrundlage. Eine zusätzliche Einwilligung wäre daher nicht nur überflüssig, sondern kann sogar Nachteile mit sich bringen.

Der Grund: Eine Einwilligung kann grundsätzlich jederzeit widerrufen werden. Stützt sich eine Praxis ausschließlich darauf, könnte der Eindruck entstehen, die Verarbeitung müsse nach einem Widerruf eingestellt werden. Behandlungsunterlagen müssen jedoch aufgrund gesetzlicher Aufbewahrungspflichten weiterhin gespeichert werden. Eine Einwilligung ist daher vor allem erforderlich, wenn die Verarbeitung über die Erfüllung des Behandlungsvertrags hinausgeht, etwa beim Versand eines Newsletters, bei Fotos auf der Praxis-Webseite oder bei der Weitergabe von Daten an Dritte, sofern keine andere Rechtsgrundlage besteht.

Eine Einwilligung ist nur dann wirksam, wenn sie freiwillig, informiert und für einen konkreten Zweck erteilt wird. Formulierungen wie „Ich stimme der Verarbeitung meiner personenbezogenen Daten zu“ genügen den Anforderungen der DSGVO nicht. Stattdessen muss klar beschrieben werden, für welchen Zweck die Einwilligung gegeben wird (z. B. zum Erhalt des Praxis-Newsletters oder zum Erstellen der Arztbriefe mit Künstlicher Intelligenz). Ebenso muss die betroffene Person darüber informiert werden, dass und wie sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Unabhängig davon, ob Sie personenbezogene Daten auf Grundlage eines Vertrags, einer gesetzlichen Verpflichtung oder einer Einwilligung verarbeiten, sollten Sie die jeweilige Rechtsgrundlage stets sorgfältig dokumentieren. So können Sie im Fall einer Prüfung durch die Datenschutzaufsichtsbehörde oder bei Rückfragen von Patienten nachvollziehbar darlegen, warum die Verarbeitung zulässig ist. Gleichzeitig vermeiden Sie, dass vorsorglich Einwilligungen eingeholt werden, obwohl hierfür keine Notwendigkeit besteht.

Prüfen Sie daher immer zuerst, auf welcher Rechtsgrundlage Sie welche personenbezogenen Daten Ihrer Patienten verarbeiten, und verwenden Sie die Einwilligung nur für die Zwecke, für die sie notwendig ist.

„Wie können wir den Datenschutz im hektischen Praxis- oder Pflegealltag verbessern?“

Frage: *„Datenschutz klingt oft nach viel Bürokratie. Welche Maßnahmen bringen im Alltag einer Arztpraxis oder Pflegeeinrichtung tatsächlich den größten Nutzen?“*

Antwort: Ein wirksamer Datenschutz muss nicht kompliziert sein. Oft sind es kleine organisatorische Maßnahmen, die das Risiko von Datenschutzverstößen erheblich reduzieren. Ein wichtiger Punkt sind dabei persönliche Benutzerkonten. Jeder Mitarbeitende sollte ausschließlich mit seinem eigenen Zugang arbeiten. Nur so lassen sich Zugriffe auf Patienten- oder Bewohnerdaten nachvollziehen und unberechtigte Einsichten erkennen. Verwenden Sie keine Gemeinschaftskonten, und gehen Sie mit Arbeitsplätzen sorgfältig um. Computer sollten beim Verlassen des Arbeitsplatzes sofort gesperrt werden – mit der Tastenkombination „Windows + L“ gelingt das innerhalb weniger Sekunden.

Auch Patientenakten, Pflegeunterlagen oder Medikamentenlisten sollten niemals unbeaufsichtigt offen zugänglich sein. Der Klassiker ist hier, dass die Patientenakten im Behandlungszimmer liegen, in dem die Patienten allein warten und so jederzeit Zugriff auf die Akten hätten. Oder der PC im Behandlungszimmer wird bereits entsperrt, und das gesamte Praxisverwaltungssystem ist für die Patienten offen zugänglich. Überprüfen Sie außerdem regelmäßig, welche personenbezogenen Daten tatsächlich benötigt werden. Werden Informationen ohne konkreten Zweck erhoben oder länger gespeichert als erforderlich, steigt das Datenschutzrisiko unnötig. Ein Löschkonzept mit klaren Aufbewahrungsfristen für alle personenbezogenen Daten, die Sie speichern, ist nicht nur eine gesetzliche Anforderung, sondern gibt auch Ihnen Sicherheit. Nicht zuletzt spielt die Sensibilisierung Ihrer Mitarbeitenden eine entscheidende Rolle.

Viele Datenschutzvorfälle entstehen nicht durch technische Fehler, sondern durch menschliche Unachtsamkeit – etwa durch das Abschicken einer E-Mail an den falschen Empfänger oder ein Telefonat mit vertraulichen Informationen in einem öffentlich zugänglichen Bereich. Regelmäßige Schulungen und klare Arbeitsanweisungen helfen, solche Fehler zu vermeiden.

Haben auch Sie eine Frage an unsere Fachexperten? Dann schreiben Sie gerne direkt an redaktion@safetyxperts.de

Der Datenschutz-Guide für Ihre Gesundheitseinrichtung

Ob neue Software, digitale Anwendungen oder veränderte Prozesse: Die Frage nach den richtigen Datenschutzmaßnahmen stellt sich regelmäßig. Auch wenn die Details komplex sein können, beruhen viele Anforderungen auf denselben Grundprinzipien. In diesem Artikel erfahren Sie, worauf Sie beim Datenschutz immer achten sollten.

Die wichtigste Referenz bezüglich des Datenschutzes in Deutschland ist die Datenschutz-Grundverordnung. Die DSGVO nennt in Art. 5 Grundsätze zur Verarbeitung personenbezogener Daten, die Sie immer berücksichtigen müssen.

Damit legen Sie die Grundlage für eine rechtmäßige Datenverarbeitung in Ihrer Einrichtung.

1. Jede Verarbeitung personenbezogener Daten muss rechtmäßig, fair und transparent erfolgen

Ihre Organisation kann die personenbezogenen Daten einer Person nur verarbeiten, wenn die geplante Verarbeitung rechtmäßig ist. Folgende Gründe machen Ihre Datenverarbeitung rechtmäßig (es gibt noch weitere als die hier aufgeführten, aber sie sind für eine Gesundheitseinrichtung kaum relevant):

- **Einwilligung der betroffenen Person:** Ausführliche Informationen dazu finden Sie bereits in der Leserfrage auf Seite 9: „Muss ich von jedem Patienten eine Einwilligung zur Datenverarbeitung einholen?"
- **Notwendig für die Erfüllung eines Vertrags:** Dies bedeutet, wenn Sie einen Arbeitsvertrag mit Ihren Mitarbeitenden abschließen, ist dieser Arbeitsvertrag die Grundlage dafür, dass Sie deren Daten verarbeiten dürfen, um den Arbeitsvertrag zu erfüllen, z. B. um Accounts in Ihren Applikationen anzulegen oder die Daten für die Gehaltsabrechnung in der Personalakte abzulegen. Dazu benötigen Sie keine Einwilligung. Anders wäre es, wenn Sie ein Bild von Ihrem Mitarbeitenden machen möchten, um dieses in Ihrer Mitarbeiterzeitung zu veröffentlichen. Der Arbeitsvertrag kann auch ohne ein Bild in der Mitarbeiterzeitung erfüllt werden, deshalb ist der Arbeitsvertrag keine Rechtsgrundlage dafür und Sie benötigen eine Einwilligung.
- **Gesetzliche Vorgabe zur Datenverarbeitung, die Sie erfüllen müssen:** Ein Beispiel hierfür ist die Weiterleitung personenbezogener Daten bei bestimmten meldepflichtigen Krankheiten an das Gesundheitsamt nach § 6 Infektionsschutzgesetz.
- **Berechtigtes Interesse Ihrer Einrichtung:** Dieses wird oft benutzt, wenn keine andere Rechtsgrundlage gefunden wird. Dabei müssen Sie aber vorsichtig sein, denn sollte es zu einem Streit kommen, müssen Sie gut begründen können, warum Ihr Interesse jenes des Betroffenen überwiegt. Sie haben bei Verwendung dieser Rechtsgrundlage keine Rechtssicherheit. In jedem Fall müssen Sie die Interessenabwägung schriftlich dokumentieren. Wichtige Kriterien sind hierbei, dass Sie darlegen, was Ihr berechtigtes Interesse ist, dass die Art der Datenverarbeitung die „mildeste" Variante ist (z. B. Zutrittsprotokoll anstelle von Videoüberwachung) und was die Interessen der Betroffenen sind. Manche Aufsichtsbehörden stellen Hilfestellungen zur Interessenabwägung zur Verfügung oder lassen Sie sich dazu von Ihrem Datenschutzbeauftragten beraten.

2. Zweckbindung: Daten nur für den vorgesehenen Zweck nutzen

Ihre Organisation darf personenbezogene Daten nur für bestimmte, eindeutige und legitime Zwecke erheben. Die Verarbeitung der Daten einer Person muss streng auf die anfänglich festgelegten Zwecke beschränkt sein. Sie dürfen diese nicht für andere Zwecke verwenden. Erfassen Sie beispielsweise die Telefonnummer Ihres Patienten, um Ihrem Behandlungsvertrag nachzukommen und ihn über seine Blutwerte zu informieren, dürfen Sie diese Telefonnummer nicht verwenden, um ihn anzurufen und Ihre neue IGeL-Leistung zu bewerben.

3. Datenminimierung: Nur notwendige Daten erheben

Ihre Gesundheitseinrichtung darf nur personenbezogene Daten verarbeiten, die für den vorgesehenen Zweck notwendig und angemessen sind. Der Klassiker ist das Geburtsdatum. Wie viele Formulare haben Sie schon ausgefüllt, bei denen Sie Ihr Geburtsdatum angeben mussten? In Einkaufszentren, Autohäusern etc. Wenn Sie dabei hinterfragen, wozu das Geburtsdatum benötigt wird, gibt es keinen wirklichen Grund dafür. Dies ist ein klassisches Beispiel, bei dem keine Datenminimierung erfolgte. Für Sie bedeutet das: Wenn Sie personenbezogene Daten erfassen, müssen Sie immer begründen können, wofür Sie dieses eine personenbezogene Datum benötigen.

4. Richtigkeit: Daten aktuell und korrekt halten

Die personenbezogenen Daten von Personen, die Sie verarbeiten, müssen korrekt und aktuell gehalten werden. Falsche personenbezogene Daten müssen berichtigt oder gelöscht werden.

5. Begrenzung der Speicherung

Die Speicherung personenbezogener Daten muss zeitlich begrenzt sein, entsprechend dem Zweck, für den diese Daten erhoben und verarbeitet wurden. Die personenbezogenen Daten müssen gelöscht oder anonymisiert werden, sobald sie nicht mehr benötigt werden. Das bedeutet, dass Sie vor Beginn der Datenverarbeitung dokumentieren müssen, wie lange Sie welche Daten aufheben. Klären Sie, wie die Daten gelöscht werden können. Achten Sie beim Softwarekauf darauf, dass eine automatisierte Löschung nach den Aufbewahrungsfristen möglich ist oder Zusatztools verfügbar sind. Sind z. B. die Fristen für Patienten- oder Personalakten abgelaufen, müssen diese gelöscht werden.

6. Datensicherheit: Personenbezogene Daten schützen

Die Verarbeitung personenbezogener Daten muss jederzeit ausreichend sicher erfolgen. Dazu müssen Sie technische und organisatorische Maßnahmen treffen, sodass die Daten vor unbeabsichtigter, unbefugter oder rechtswidriger Offenlegung, Verlust, Zerstörung oder Beschädigung geschützt sind. Hierzu gibt die IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung detaillierte Anforderungen vor.

NUTZEN SIE IHREN EXKLUSIVEN ONLINEBEREICH



JEDERZEIT VON ALLEN GERÄTEN AUF IHRE **ARBEITSHILFEN** ZUGREIFEN. GLEICH REINSCHAUEN!

Nutzen Sie den Onlinebereich auch mobil und stöbern Sie durch die Updates:
safetyxperts.de/login

Arbeitshilfen: Muster, Vorlagen, Checklisten

Bequemer als Google und verlässlicher als KI: Sie finden über die Schlagwortsuche alle Arbeitshilfen zum Herunterladen und Bearbeiten.

Archiv: Ihre Ausgaben

Digital und auf allen Geräten können Sie auf die bisher erschienenen Ausgaben bequem zugreifen – nichts geht verloren!

Newsfeed: Aktuelle Beiträge

Bleiben Sie stets über aktuelle Themen und wichtige Änderungen im Arbeitsschutz informiert.

Impressum

SafetyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG • Theodor-Heuss-Str. 2–4, 53095 Bonn • Telefon: 02 28 / 95 50 120 • Fax: 02 28 / 36 96 486 • Internet: www.safetyxperts.de • E-Mail: kundendienst@safetyxperts.de • E-Mail für Leserfragen: gesundheitswesen@safetyxperts.de • Vorstand: Richard Rentrop, Michael Schrader, Bonn • ISSN: 2365-7723 • Erscheinungsweise: 26-mal pro Jahr • Redaktionell Verantwortlicher: Martin Grashoff, VNR Verlag für die Deutsche Wirtschaft AG; Adresse s. o. • Redaktion: Ricarda Waldon, Bayreuth (RW) • Produktmanagement: Chanaya Schönborn, Bonn • Satz: Schmelzer Medien GmbH, Siegen • Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim • Titelbild: © HNFOTO – stock.adobe.com • Alle Angaben in „Arbeitsschutz und Hygiene im Gesundheitswesen" wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden. Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

© 2026 by SafetyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

Dieser Fachnewsletter richtet sich gleichermaßen an weibliche und männliche Leser. Aus Gründen der Lesbarkeit wird die männliche Schreibweise (z. B. Unternehmer, Mitarbeiter) gewählt. Diese schließt stets alle Geschlechterformen mit ein.

Wie viel Spam steckt in unseren E-Mails?

Was denken Sie, wie viel Prozent der weltweit versandten E-Mails sind unerwünscht?

- 10 %
- 40 %
- 70 %

Korrekt ist: 70 %. Diese E-Mails enthalten unerwünschte Werbung oder Schadcodes. Dies zeigt deutlich, wie wichtig gute üFiltermechanismen sind.
Quelle: **kurzlinks.de/0zm4**