Agenda

1. Datenschutz Ursprung und Sinn

Die Europäische Menschenrechtscharta bekräftigt das Recht auf Achtung des Privat- und Familienlebens sowie den Schutz personenbezogener Daten. Diese Rechte sind auch in der Europäischen Datenschutz-Grundverordnung (DSGVO) verankert, die im Mai 2018 in Kraft getreten ist und für alle EU-Mitgliedsstaaten verbindlich ist. Die DSGVO stellt sicher, dass personenbezogene Daten nur für legitime Zwecke gesammelt und verarbeitet werden, und dass die Betroffenen ein Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung ihrer Daten haben. Darüber hinaus müssen Unternehmen und Organisationen, die personenbezogene Daten verarbeiten, angemessene Sicherheitsmaßnahmen ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten zu gewährleisten. Insgesamt sind die Datenschutzbestimmungen in der Europäischen Union darauf ausgerichtet, die Würde, Freiheit und Gleichheit der Bürgerinnen und Bürger zu schützen, und geben eine praktische Umsetzung der Grundsätze der Europäischen Menschenrechtscharta dar.

Die DSGVO

Grob gesagt formuliert die DSGVO einzelne Anforderungen über den gesamten Lebenszyklus der Verarbeitung. Von der Zulässigkeitsprüfung vor der Verarbeitung über die Risikobeherrschung während der Verarbeitung bis hin zur Reaktion auf Sicherheitsverletzungen reihen sich die Regelungen wie Perlen an einer Schnur aneinander und haben gemeinsam, dass sie den Verantwortlichen verpflichten, technische und organisatorische Maßnahmen zu ergreifen, um das in der jeweiligen Norm adressierte Risiko normgerecht zu beherrschen. Als zentrale Regelung bringt dies Art. 24 DSGVO zum Ausdruck in den 5 Grundsätzen des Datenschutzes, die der Verarbeiter einhalten muss:

1) Die **Rechtmäßigkeit** der Verarbeitung muss nachgewiesen werden, andernfalls ist die Datenverarbeitung unzulässig (Einwilligung, Vertrag, Gesetz, Notfall, Eigeninteresse, öffentl. Interesse)
2) **Datenminimierung:** Es dürfen nur so viele Daten erhoben werden, wie für die Erledigung des Behandlungsvertrages erforderlich sind .
3) Die Daten dürfen nur für den Zweck verwenden, für den die Erlaubnis gegeben wurde, d.h. die **Zweckbindung** (Jeder Zweck hat seine eigene Rechtsgrundlage)
4) Die Datenverarbeitung muss gegenüber dem Bürger **transparent** sein (Rechenschaftspflicht, Dokumentationspflicht)
5) Die **Sicherheit und Integrität** der Daten muss gewährleistet sein (Stand der Technik).

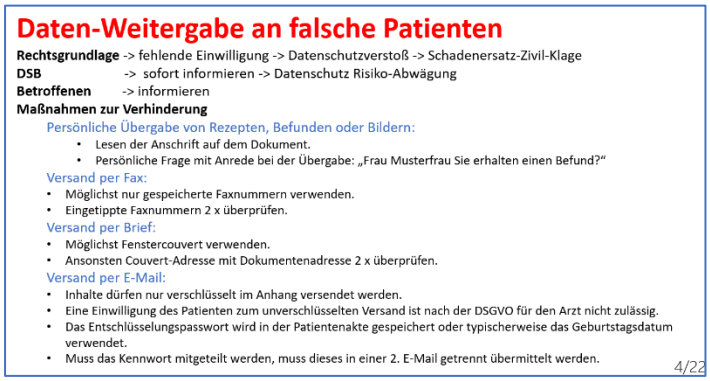
2. Häufige Datenschutzverletzungen

2.1. Daten-Weitergabe an falsche Patienten

Weitergabe von Rezepten, Befunden, Bildern an falsche Patienten.

1. Rechtlicher Hintergrund:

Die Weitergabe personenbezogener Daten an Dritte ohne Einwilligung des Betroffenen stellt einen Verstoß gegen Artikel 6 der Datenschutz-Grundverordnung (DSGVO) dar.
Artikel 6 legt fest, dass die Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn eine der folgenden Bedingungen erfüllt ist: Einwilligung, Vertrag, Gesetz, Notfall, eigenes Interesse, öffentliches Interesse.



2. Datenschutzbeauftragte:

Der Datenschutzbeauftragte ist unverzüglich zu informieren. Dieser beurteilt in einer Datenschutz-Folgenabschätzung (DSFA), welcher Schaden und welches Risiko für den Patienten eingetreten ist und ob die Datenschutzverletzung innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden muss. Auf der Grundlage seiner Bewertung empfiehlt er das weitere Vorgehen.

3. Information der betroffenen Personen:

Es ist wichtig, dass die betroffenen Personen so schnell wie möglich über die Situation informiert werden. Dies ist ein Anliegen von Artikel 34 der Datenschutz-Grundverordnung (DSGVO), der besagt, dass der Verantwortliche die betroffene Person unverzüglich über die Verletzung des Schutzes personenbezogener Daten benachrichtigen muss.

Die Benachrichtigung sollte so erfolgen, dass die betroffene Person klar und präzise über die Art der Verletzung, die möglichen Folgen und die getroffenen Abhilfemaßnahmen informiert wird.

Es gibt jedoch einige Ausnahmen, in denen eine Benachrichtigung der betroffenen Person nicht erforderlich ist. Dazu gehören beispielsweise Fälle, in denen die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

4. Maßnahmen zur Verhinderung von Fehlübergaben:

<u>Persönliche Übergabe von Rezepten, Befunden oder Bildern:</u>

- Lesen der Anschrift auf dem Dokument.
- Persönliche Frage mit Anrede bei der Übergabe: „Frau Musterfrau Sie erhalten ein Rezept?“

<u>Versand per Fax:</u>

- Möglichst nur gespeicherte Faxnummern verwenden.
- Eingetippte Nummern 2 x überprüfen.
- Versand per Brief:
- Möglichst Fenstercouvert verwenden.
- Ansonsten Couvert Adresse mit Dokumentenadresse 2 x überprüfen.

<u>Versand per E-Mail:</u>

- Inhalte dürfen nur verschlüsselt im Anhang versendet werden.
- Eine Einwilligung des Patienten zum unverschlüsselten Versand ist nach der DSGVO für den Arzt nicht zulässig.
- Das Entschlüsselungspasswort wird in der Patientenakte gespeichert oder typischerweise das Geburtstagsdatum verwendet.
- Muss das Kennwort mitgeteilt werden, muss dieses in einer 2. E-Mail getrennt übermittelt werden.

2.2. Auskünfte am Telefon in der Arztpraxis

Nach der DSGVO, aber auch nach dem strafrechtlich geschützten Arztgeheimnis (§ 203 StGB), dürfen Patientendaten nicht unberechtigten Personen bekanntgegeben werden. Dies gilt auch bei telefonischen Anfragen.

Wird einer unberechtigten Person eine Auskunft gegeben, so kann dies eine meldepflichtige Datenpanne sein, die an die Datenschutzaufsicht und aufgrund der Infopflicht auch an

betroffene Patienten zu melden ist. Dies kann in der Folge, insbesondere wenn die Melde und Informationspflichten verletzt werden, zu hohen Bußgeldern führen und strafrechtliche oder arbeitsrechtliche Konsequenzen haben (siehe Verpflichtungserklärung).

Am Telefon ist es besonders schwierig, eine Person eindeutig zu identifizieren. Die Frage nach Namen und Geburtsdatum (evtl. noch der Anschrift) ist untauglich zur Identifikation, ob wirklich der Patient selbst anruft, da diese Daten zahlreichen anderen Personen zugänglich sind. Man stelle sich den Arbeitgeber vor, der über diese Daten verfügt und sich nach dem Corona-Testergebnis, oder einen (Ex-)Partner, der sich nach einem Schwangerschaftstest erkundigt. Aus diesen Gründen ist generell höchste Vorsicht bei telefonischen Auskünften angebracht. Daher ist es empfehlenswert, im Regelfall keine telefonischen Auskünfte zu erteilen.

Wenn dennoch ausnahmsweise auf Wunsch und in Verantwortung der Praxisleitung Auskünfte am Telefon erteilt werden sollen, sollten Sie eindeutige Kriterien zur Identifikation mit dem betroffenen Patienten vereinbaren. Das sollten Dinge sein, die im Normalfall nur der betroffene Patient selbst wissen kann, die zumindest aber nicht zahlreiche andere Personen in seinem sozialen und beruflichen Umfeld kennen.

Wenn z. B. für den Patienten ein Labortest beauftragt wurde, könnte man die Laborauftragsnummer als Identifikationskennzeichen vereinbaren. Dann kann sich der Patient mit dieser Auftragsnummer als berechtigter Empfänger der Information über das Testergebnis identifizieren. Als Alternative könnte der Patient darum gebeten werden, das Ergebnis des Labortests mit der Ärztin in der Praxis zu besprechen.

Als weitere Möglichkeit, den Patienten zu identifizieren, könnte z. B. nach Dingen aus der Behandlung gefragt werden, wie z. B. nach den letzten 1-2 Behandlungsterminen, und worum es dabei ging. Möglich wären zur Identifikation des Patienten auch „Fangfragen“, wie: „Hatten Sie sich im letzten Jahr den Fuß gebrochen?“, wenn die Person wegen einer Steißbeinprellung in Behandlung war.

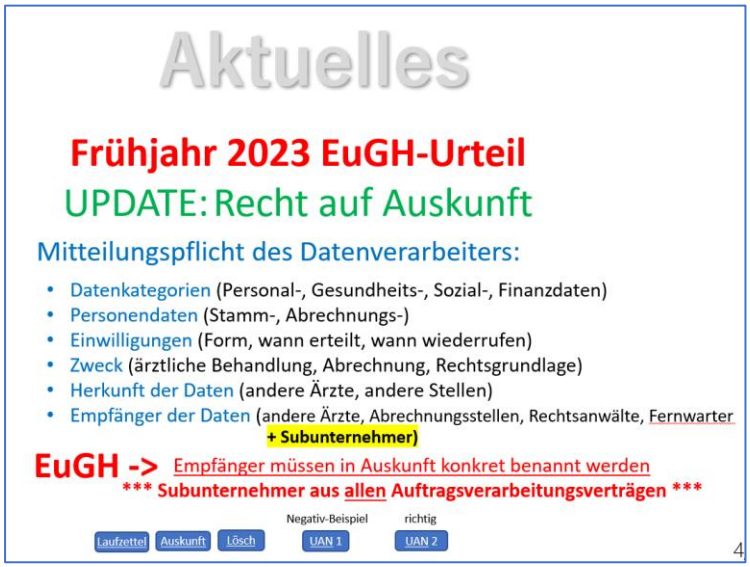
Wenn einem Patienten telefonisch eine Auskunft über seine Patientendaten erteilt wurde, sollte darüber auf jeden Fall in seiner Patientenakte eine Notiz aufgenommen werden, und zwar mit den Angaben, wer welche Information wollte und welche Information bekommen hat und wie sich diese Person autorisiert hat.

Der Prozess der Auskunftserteilung, speziell auch am Telefon, sollte in einer Arbeitsanweisung dokumentiert sein.

3. Recht auf Auskunft – Update

3.1. Die Auskunft als Ausgangspunkt für die Betroffenenrechte

Die Bedeutung des Auskunftsrechts für betroffene Personen ergibt sich vor allem daraus, dass die Informationen, die man als Betroffener hierzu erhält, die Basis bilden, um möglicherweise weitere Betroffenenrechte wie das Recht auf Berichtigung nach Art. 16 DSGVO oder das Recht auf Löschung nach Art. 17 DSGVO geltend zu machen. Nur wenn man als Betroffener vollständige Informationen erhält, welche Daten das verantwortliche Unternehmen zu welchen Zwecken eigentlich verarbeitet, ist es überhaupt möglich zu prüfen, ob die Daten auch korrekt verarbeitet werden oder ob Daten beispielsweise längst hätten gelöscht werden müssen.
Daraus lässt sich ableiten, dass dies auch für Informationen bezüglich der Datenempfänger gelten muss. Denn wie soll man erkennen oder prüfen, ob irgendein Vertragspartner des Unternehmens die eigenen Daten rechtmäßig verarbeitet oder nicht?

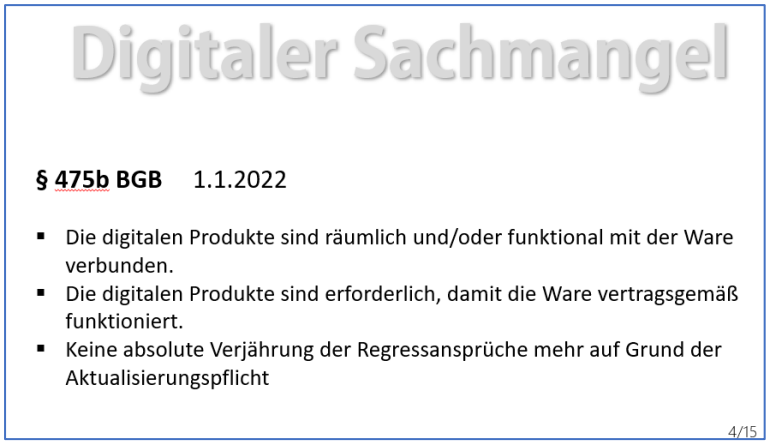


Die oben genannten Argumente werden von der Mitteilungspflicht (Art. 19 DSGVO) flankiert. Danach ist der Verantwortliche verpflichtet, sämtliche Datenempfänger zu informieren, wenn der Verantwortliche selbst Begehren von Betroffenen nach Recht auf Berichtigung (Art. 16), Recht auf Löschen (Art. 17) und Recht auf Einschränkung der Verarbeitung/Sperrung (Art 18 DSGVO) umsetzen muss.

3.2. Auswirkung auf die Umsetzung

Dies wirkt sich insbesondere bei der Erfüllung des Auskunfts- und Löschungsanspruchs aus. Um für den Patienten die notwendige Transparenz zu schaffen, wer alles mit seinen Daten in Berührung gekommen sein könnte, müssen auch gemäß dem neuen EuGH-Urteil alle **Unterauftragnehmer** des Auftragsverarbeiters, z.B. des Praxissoftwarelieferanten, genannt werden, um dem Patienten die Möglichkeit zu geben, auch dort seine Rechte auf Auskunft, Löschung, Berichtigung und Sperrung geltend zu machen.

4. Neue Regelung zu Sachmängeln in digitalen Produkten bei fehlendem Datenschutz (§ 475b BGB)



Bei digitalen Produkten ist es durchaus üblich, dass personenbezogene Daten verarbeitet werden. Mit der DSGVO sind Hersteller bzw. Verkäufer auch zu einer datenschutzkonformen Produktgestaltung und Entwicklung angehalten. Was aber wenn der Hersteller oder Verkäufer sich bei den Waren nicht an die DSGVO hält oder DSGVO-Konformität angibt, obwohl Mängel bestehen?

4.1. Das neue Kaufrecht zu Waren mit digitalen Elementen:

Die Regeln des Verbrauchsgüterkaufes werden grundlegend zugunsten des Verbrauchers ausgelegt.

Ein Sachmangel liegt vor:

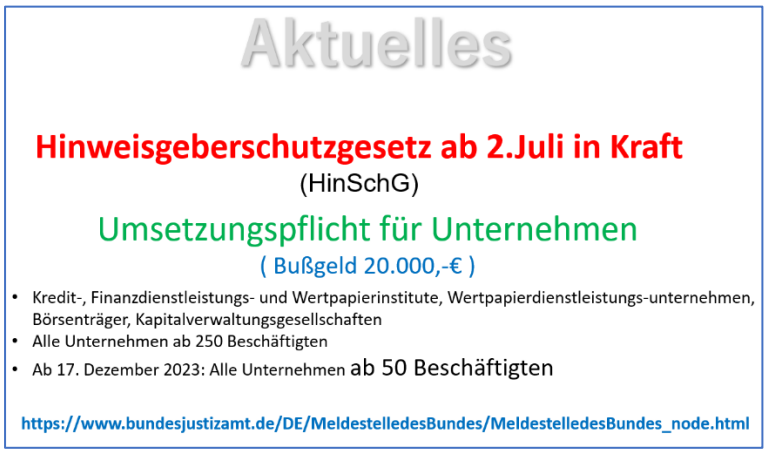
- wenn die Funktion durch einen Datenschutzmangel beeinträchtigt wird und für den Verbraucher spürbar ist,
- Voreinstellungen zur Erledigung von Betroffen-Rechten Art.25 DSGVO fehlen,
- die Sicherheit der Verarbeitung Art 32 DSGVO nicht gewährleistet ist.
- Aktualisierungspflicht

Sowohl für Waren mit digitalen Bestandteilen als auch für digitale Produkte gilt insbesondere ein erweiterter Sachmangelbegriff. Den Verkäufer trifft zudem eine Aktualisierungspflicht. Anders als sonst im deutschen Recht können Gewährleistungsrechte künftig auch dann entstehen, wenn die Ware bei Gefahrübergang mangelfrei war. Die objektiven Anforderungen an die Mangelfreiheit sind nur dann erfüllt, wenn der Verbraucher über Updates informiert wird und diese für den Zeitraum der gewöhnlichen Nutzung des Produkts zur Verfügung gestellt werden.

Eine absolute Verjährung von Rückgriffsansprüchen gibt es nicht mehr.

Nach der gesetzlichen Regelung tritt die Verjährung der Rückgriffsansprüche des Verkäufers gegen den Lieferanten frühestens zwei Monate nach dem Zeitpunkt ein, in dem der Verkäufer die Gewährleistungsansprüche seines Käufers erfüllt hat. Die derzeit noch geltende Höchstgrenze von fünf Jahren nach Ablieferung der Sache durch den Lieferanten an den Verkäufer (§ 445 b II 2 BGB) entfällt künftig. Grund hierfür ist die Aktualisierungspflicht, da eine diesbezügliche Haftung des Verkäufers gegenüber seinem Käufer auch nach mehr als fünf Jahren möglich ist.
Die Neuregelung gilt für Kaufverträge, die ab dem 01.01.2022 geschlossen werden.

5. Hinweisgeberschutzgesetz



Das Hinweisgeberschutzgesetz zielt darauf ab, einen umfassenden Schutz für Whistleblower sicherzustellen.

Inhalt des Gesetzes:
Unternehmen und Organisationen mit 50 oder mehr Beschäftigten müssen sichere interne Hinweisgebersysteme einrichten und betreiben.
Kleine Unternehmen mit 50 bis 249 Beschäftigten haben bis zum 17. Dezember 2023 Zeit, um diese Systeme einzuführen. Whistleblower haben das Recht, Hinweise mündlich, schriftlich oder persönlich abzugeben. Nachdem ein Hinweis abgegeben wurde, muss die interne Meldestelle dem Whistleblower innerhalb von sieben Tagen eine Bestätigung geben. Die Meldestelle muss den Whistleblower innerhalb von drei Monaten über die ergriffenen Maßnahmen informieren, wie z.B. interne Compliance-Untersuchungen oder die Weiterleitung der Meldung an eine zuständige Behörde.
Zusätzlich zur internen Meldestelle wird beim Bundesamt für Justiz eine externe Meldestelle eingerichtet. Die Bundesländer können auch eigene Meldestellen einrichten.
Es ist wichtig zu beachten, dass in Unternehmen mit Betriebsrat ein längerer Vorlauf einzuplanen ist, da dem Betriebsrat bei der Ausgestaltung des Hinweisgebersystems Mitbestimmungsrechte zustehen und eine Betriebsvereinbarung abgeschlossen werden muss. Zudem kann eine Nichtberücksichtigung des Whistleblowers bei einer Beförderung, Versetzung oder Nicht-Verlängerung seines Arbeitsvertrags als "Repressalie" gewertet werden. In diesem Fall muss der Arbeitgeber beweisen, dass dies keine Benachteiligung aufgrund der Meldung des Whistleblowers war. Andernfalls drohen Schadensersatzansprüche und Bußgelder. https://www.bundesjustizamt.de/DE/MeldestelledesBundes/MeldestelledesBundes_node.html

6. Datenschutzverstöße Webseite

Dass Daten einen extrem hohen Wert haben, zeigt das Geschäft von Google, das allein mit dem Sammeln von Daten und der Erstellung von Marktanalysen einen Jahresumsatz von 100 Milliarden Dollar erzielt.

Der Trick:

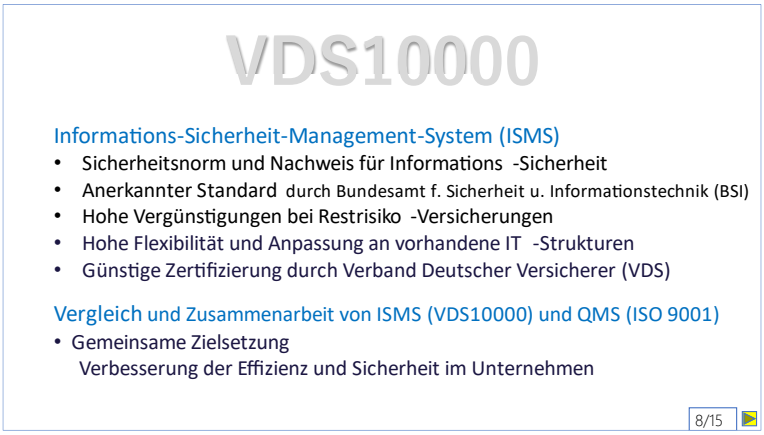
- Den Webseitenprogrammierern werden kostenlose Programmiertools angeboten, bei deren Nutzung aber die Kontakt- und Besucherdaten an Google fließen, um dort zu Marketingzwecken ausgewertet und verkauft zu werden.
- Analyseprogramme werden kostenlos angeboten, um die Effizienz der Seiten zu messen.
- Mächtige Navigationsdienste können kostenlos genutzt werden, um das Reiseverhalten und geographische Hotspots auszuwerten.

Was viele Programmierer und Webseitenbetreiber jedoch nicht bedenken ist, dass bei der Nutzung dieser Dienste auf der eigenen Webseite und der Weitergabe der Daten an Google eine Einwilligung des Webseitenbesuchers notwendig ist, da es sonst verboten ist, TTDSG §25.

Dies macht sich nun eine andere Gruppe zunutze und baut darauf ein lukratives Geschäftsmodell auf, indem sie Webseitenbetreiber wegen solcher Datenschutzverstöße massenhaft abmahnt und mit einer Klage oder einer Abmahngebühr droht.
Im Herbst letzten Jahres wurden die von Google kostenlos angebotenen Schriften für Webseiten damit bekannt und lösten eine riesige Abmahnwelle aus.
In einigen Fällen wurden Kanzleien, die solche Abmahnungen verschickten, zur Beendigung des Vorgehens gezwungen. In einem Fall wurde ein Anwalt und seine Mandantin, die vermeintliche Datenschützer, wegen Abmahnbetrugs und Erpressungsversuchs in mindestens 2418 Fällen durchsucht und mit einer Gesamtsumme von 346.000 Euro bestraft.
Insgesamt zeigt die rechtliche Konsequenz der Abmahnwelle, dass die massenhafte Abmahnung wegen angeblicher Datenschutzverstöße durch die Einbindung von Google Fonts als rechtsmissbräuchlich eingestuft werden kann. Es bleibt jedoch abzuwarten, ob diese Entscheidung auch in anderen Fällen und Gerichten Bestand haben wird.

Hinweis: In jedem Dienstleistung-Vertrag mit digitalen Produkten sollte daher der Zusatz aufgenommen werden: „...das Produkt...die Dienstleistung ist datenschutzkonform...“.

7. Sicherheitsnorm für Klein-Unternehmen



Die VDS10000 ist ein vom BSI anerkannter Sicherheitsstandard, der aufwärtskompatibel zu ISO 27001 ist und vom Gesamtverband der Deutschen Versicherungswirtschaft entwickelt wurde, um kleinen Unternehmen die Möglichkeit zu geben, bei einer Restrisikoversicherung eine günstige Versicherungsprämie zu erhalten. Mit der Einführung dieser Norm werden wie beim QM, aber im Bereich der Informationssicherheit, Sicherheit, Effizienz und Datensicherheit verbessert.
Sie unterscheidet sich wesentlich von anderen Normen, indem sie Hilfestellungen und Lösungen aufzeigt. Die Kosten einer Zertifizierung liegen wesentlich unter einer QM-Zertifizierung, von einer ISO 27001 ganz zu schweigen.

8. Die elektronische Patientenakte (ePa)

Vor knapp einem Jahr kündigte Bundesgesundheitsminister Karl Lauterbach auf der DMEA eine Digitalisierungsstrategie für das Gesundheitswesen und die Pflege an. Nun wurde diese veröffentlicht. Im Fokus: Die digitale Patientenakte und die Nutzung der Gesundheitsdaten für Forschungszwecke.

„Deutschlands Gesundheitswesen hängt in der Digitalisierung um Jahrzehnte zurück“, beginnt Bundesgesundheitsminister Karl Lauterbach die Pressekonferenz, bei der die Weichen für die Digitalisierung des Gesundheitswesens gestellt werden sollen:

Die elektronische Patientenakte – deren Grundlage vorsage und schreibe 20 Jahren gelegt wurde – wird nicht mal von einem Prozent der Versicherten genutzt, Forschung anhand von Gesundheitsdaten ist auch nicht möglich. Bei den elektronischen Daten, die genutzt werden könnten, um Forschung zu betreiben, haben wir die Lage, dass die Daten, die es gibt, nicht miteinander verknüpft werden können und weil sie nicht miteinander verknüpft werden können, sind Langzeitbeobachtungen nicht möglich, so Lauterbach.

Das soll sich nun mit der Digitalisierungsstrategie ändern. Man habe dafür drei Ziele definiert, die kurzfristig erreicht werden sollen, um zu zeigen, dass auch in Deutschland Digitalisierung möglich ist, erklärt der Minister. Diese sind:

- bis 2025 sollen 80 Prozent der gesetzlich Versicherten über eine **ePA** verfügen,
- bis Ende 2025 sollen 80 Prozent der ePA-Nutzer, die in medizinischer Behandlung sind, zudem eine digitale **Medikationsübersicht** haben
- und bis Ende 2026 sollen darüber hinaus mindestens **300 Forschungsvorhaben** mit Gesundheitsdaten durch das neue Forschungsdatenzentrum Gesundheit realisiert werden.

Diese Ziele sollen durch zwei Gesetze erreicht werden. Einerseits das **Digitalgesetz**. Dieses beschäftigt sich Lauterbach zufolge damit, wie die ePA als **Opt-out**-Variante eingeführt werden kann. „Das zweite Gesetz ist das **GesundheitsDatenNutzungsGesetz**. Dieses soll dafür sorgen, dass man die Daten, die es im System gibt, so zusammenführen kann, dass tatsächlich auch longitudinale Auswertungen möglich sind“, so Lauterbach.

8.1. Frage: Ist die Opt-out-Regelung nicht in der DSGVO oder TTDSG verboten?

Der englische Begriff "Opt-out" wird in der deutschen Sprache oft mit "Austritt" oder "Widerspruch" übersetzt. Dieser Begriff bezieht sich auf ein Verfahren, bei dem die Zustimmung zur Verarbeitung personenbezogener Daten implizit gegeben wird, es sei denn, der Betroffene widerspricht explizit. Das bedeutet, dass die Datenverarbeitung so lange erlaubt ist, bis der Betroffene gegen sie auftritt.

Zwar ist das Opt-Out weder in der Datenschutz-Grundverordnung (DSGVO) noch im Telekommunikations- und Telemedien-Datenschutzgesetz (TTDSG) explizit verboten. Beide Gesetze stellen jedoch strenge Anforderungen an die Einwilligung der Nutzer in die Verarbeitung ihrer personenbezogenen Daten:

- Die DSGVO fordert eine ausdrückliche, informierte und unmissverständliche Einwilligung der betroffenen Person. Das bedeutet, dass Nutzer aktiv zustimmen müssen und dass die Einwilligung nicht durch Voreinstellungen oder Opt-out-Optionen gegeben werden darf.
- Die TTDSG ergänzt diese Anforderungen um die Regel, dass die Einwilligung freiwillig sein muss und dass der Nutzer über die Zwecke und Folgen der Verarbeitung seiner personenbezogenen Daten informiert werden muss.

In beiden Gesetzen wird also deutlich, dass die Einwilligung von Nutzern in die Verarbeitung ihrer personenbezogenen Daten sehr strengen Anforderungen unterliegt und dass eine einfache Opt-out-Regelung nicht ausreicht, um eine rechtlich gültige Einwilligung zu erhalten.

8.2. Frage: Was ist die elektronische Patientenakte?

Die elektronische Patientenakte (ePA) ist ein digitales System zur Speicherung und Verwaltung von Gesundheitsdaten einer Person. Sie soll dazu beitragen, die medizinische Versorgung zu verbessern, indem sie Ärzten und anderen medizinischen Fachkräften einen schnellen und sicheren Zugriff auf wichtige Gesundheitsdaten des Patienten ermöglicht.
In der ePA werden zum Beispiel Diagnosen, Untersuchungsergebnisse, Impfungen, Medikamente, Arztbriefe und andere Gesundheitsdaten gespeichert. Der Patient hat dabei die Kontrolle über seine Daten und kann entscheiden, welche Daten gespeichert werden und wer darauf zugreifen darf. Die Daten werden durch moderne Sicherheitstechnologien und Verschlüsselungsverfahren geschützt, um eine hohe Datensicherheit und Vertraulichkeit zu gewährleisten.
Die ePA ist in Deutschland seit dem 1. Januar 2021 gesetzlich vorgeschrieben und wird schrittweise eingeführt. Versicherte hatten das Recht, eine ePA bei ihrer Krankenkasse zu beantragen und können selbst entscheiden, welche Daten sie in der ePA speichern lassen möchten. Ziel der ePA ist es, die Zusammenarbeit zwischen verschiedenen Ärzten und Gesundheitseinrichtungen zu verbessern und somit eine effizientere und bessere Versorgung zu gewährleisten.

8.3. Frage: Was ist das GesundheitsDatenNutzungsGesetz ?

Das **G**esundheits**D**aten**N**utzungs**G**esetz (GDNG) ist ein im Jahr 2021 in Kraft getretenes deutsches Gesetz zur Verbesserung der Nutzung von Gesundheitsdaten für Forschungs- und Versorgungszwecke. Das Gesetz regelt den Umgang mit Gesundheitsdaten und erlaubt deren Verwendung für wissenschaftliche Zwecke sowie für die Verbesserung der medizinischen Versorgung.

Das GDNG setzt dabei hohe Anforderungen an den Datenschutz und die Datensicherheit. So dürfen die Gesundheitsdaten nur unter strengen Voraussetzungen und nur pseudonymisiert verwendet werden, um die Identität der Patienten zu schützen. Zudem müssen die Daten in einer sicheren IT-Infrastruktur gespeichert und übertragen werden.

Das GDNG sieht vor, dass Daten aus verschiedenen Quellen wie Arztpraxen, Krankenhäusern, Krankenkassen und anderen Einrichtungen zusammengeführt werden können, um einen besseren Überblick über den Gesundheitszustand der Bevölkerung und die Qualität der medizinischen Versorgung zu erhalten. Ziel ist es, auf Basis dieser Daten fundierte Entscheidungen in der Gesundheitspolitik zu treffen und die medizinische Versorgung zu verbessern.

Das GDNG hat im Vorfeld der Verabschiedung kontrovers diskutiert und steht auch weiterhin in der Kritik von Datenschutz- und Patientenschutzverbänden. Kritiker befürchten eine unzureichende Kontrolle und Transparenz bei der Verwendung von Gesundheitsdaten sowie eine Einschränkung der informationellen Selbstbestimmung der Patienten.

9. Das eRezept

9.1. Timeline

Das eRezept ist eine elektronische Version eines ärztlichen Rezepts, das in Deutschland seit Januar 2022 verwendet wird. Es ersetzt das bisherige Papierrezept und wird direkt vom Arzt an die Apotheke übermittelt. Das eRezept soll den Prozess des Einlösens von Rezepten vereinfachen und beschleunigen, da es nicht mehr notwendig ist, das Papierrezept physisch zur Apotheke zu bringen. Stattdessen kann der Patient das eRezept direkt auf seinem Smartphone oder einem anderen mobilen Gerät speichern und es bei der Apotheke vorzeigen oder per QR-Code scannen lassen.

9.2. Das eRezept funktioniert folgendermaßen:

- Der Arzt erstellt das eRezept in seiner zertifizierten Software und speichert es digital.
- Der Patient erhält das eRezept entweder per E-Mail oder es wird ihm in der Praxis direkt auf sein Smartphone geladen, oder nach Gematik-Beschluss vom 22.06.23 ab 01.01.2024 auf die elektronische Gesundheitskarte. Der Patient kann das eRezept nun in seiner Apotheke einlösen.
- Die Apotheke überprüft die Gültigkeit des eRezept und gibt das Medikament aus.
- Die Abrechnung des eRezept erfolgt über die Kassenärztlichen Vereinigungen. Die Apotheke reicht das eRezept zusammen mit den Abrechnungsdaten bei der zuständigen Kassenärztlichen Vereinigung ein.

Es ist zu beachten, dass das eRezept nur für verschreibungspflichtige Medikamente verwendet werden kann und dass es in Deutschland derzeit noch nicht flächendeckend eingeführt ist.

Hier sind einige der wichtigsten datenschutzrechtlichen Dinge, die beim eRezept beachtet umgesetzt werden müssen.

<u>Gematik:</u>

- Datensicherheit: eRezepte enthalten personenbezogene Daten, einschließlich Namens, Adresse, Geburtsdatum, Krankenversicherungsnummer, medizinische Diagnosen und verschriebene Medikamente. Es ist wichtig, dass diese Daten sicher aufbewahrt und vor unbefugtem Zugriff geschützt werden.

- Zugriffskontrolle: Der Zugriff auf eRezepte sollte auf autorisierte Personen beschränkt sein, die einen legitimen Grund haben, auf diese Daten zuzugreifen. Es sollten klare Verfahren zur Überprüfung von Zugriffsrechten und zur Überwachung von Datenzugriffen vorhanden sein.
- Datenübertragung: Die Übertragung von eRezept-Daten zwischen Ärzten, Apotheken und anderen Beteiligten sollte verschlüsselt erfolgen, um die Sicherheit und Integrität der Daten zu gewährleisten.
- Zweckbindung: Die Verwendung von eRezept-Daten sollte auf den vorgesehenen Zweck beschränkt sein, wie z.B. die Verschreibung von Medikamenten. Eine Verwendung für andere Zwecke, wie z.B. Marketing, ist nicht zulässig.

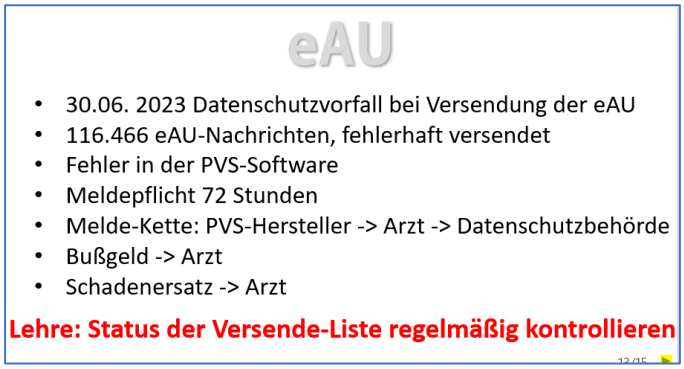
<u>Arztpraxis</u>:

- Datenschutzerklärung: Patienten sollten über den Umgang mit ihren persönlichen Daten im Zusammenhang mit eRezepten informiert werden. Die Datenschutzerklärung sollte klar und verständlich sein und den Patienten die Möglichkeit geben, der Verwendung ihrer Daten zu widersprechen.
- Aufbewahrungsdauer: Im Fall von eRezepten bedeutet dies, dass sie gelöscht werden müssen, sobald das Rezept abgelaufen ist und das Medikament abgegeben wurde. Konkret bedeutet dies, dass der QR-Code des eRezeptes nach Ablauf der Gültigkeitsdauer, die auf dem Rezept vermerkt ist, gelöscht werden muss. In Deutschland beträgt die Gültigkeitsdauer für ein eRezept derzeit 28 Tage nach Ausstellung des Rezepts.

Es ist wichtig, dass alle Beteiligten im Gesundheitswesen, einschließlich Ärzte, Apotheken und IT-Dienstleister, die datenschutzrechtlichen Anforderungen beim eRezept beachten und sicherstellen, dass die Daten ihrer Patienten sicher und geschützt sind.

Aktuelles Problem: Der Apotheker kann durch Kenntnis der Krankassen-ID auf alle früheren Medikamente zugreifen, ohne Einwilligung des Patienten.

10. eAU Datenschutzvorfall



10.1. Informationen zum Vorfall fehlgeleiteter KIM-Nachrichten

Die Gematik wurde am 30.06.2023 von einem KIM-Anbieter darüber informiert, dass es innerhalb der „Kommunikation im Gesundheitswesen“ (KIM) zu einer Fehlleitung von Nachrichten gekommen ist. Betroffene KIM-Nachrichten wurden nicht wie vorgesehen an die AOK Niedersachsen, sondern an eine einzelne Arztpraxis weitergeleitet. Nach derzeitigem Kenntnisstand enthielten die Nachrichten überwiegend elektronische Arbeitsunfähigkeitsbescheinigungen (eAU). Ursache für die Fehlleitung war vermutlich eine fehlerhafte Implementierung in den Praxisverwaltungssystemen des Herstellers. Um weitere Fehlleitungen von KIM-Nachrichten an die betroffenen Praxen zu verhindern, wurde die KIM-Adresse unmittelbar nach Bekanntwerden des Problems aus dem Verzeichnisdienst entfernt. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wurde über den Vorfall informiert und wird im Rahmen weiterer Analysen durch die Gematik unterrichtet.
Nach aktuellen Angaben der Fachabteilung der betroffenen Arztpraxis handelt es sich um ein Mengengerüst von 116.466 eAU-Nachrichten, die seit September 2022 fehlerhaft an diese einzelne Arztpraxis versendet wurden. Ein Großteil dieser Nachrichten wurde aus technischen Gründen erst in den letzten zwei Monaten fehlerhaft versendet. Die betroffene Arztpraxis bemerkte das hohe Nachrichtenaufkommen erst, als sich das Systemverhalten änderte und die Praxis bei ihrem Systemanbieter nachfragte. Das Problem blieb somit über einen längeren Zeitraum unbemerkt. Nach derzeitigem Kenntnisstand ist es wahrscheinlich, dass die Praxis aus technischen Gründen nicht zum Öffnen der fehlgeleiteten E-Mails in der Lage war. Da die Übermittlung an einen Berufsgeheimnisträger erfolgte, unterliegt der Vorgang zudem besonderen berufs- und strafrechtlichen Anforderungen. Der Übermittlungsvorgang über KIM ermöglichte trotz der Fehlleitung keinen Zugriff Unbefugter außerhalb der Telematikinfrastruktur.

10.2. Wie kam es zu dem Vorfall?

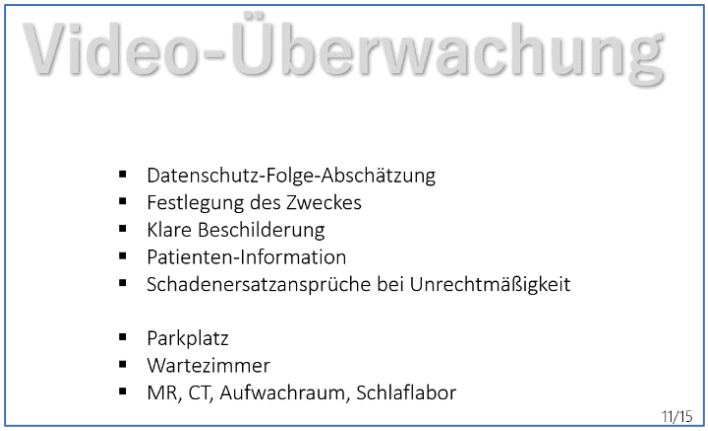
Sowohl Krankenkassen als auch Arztpraxen werden durch Identifikationsnummern im Verzeichnisdienst (VZD) identifiziert bzw. gekennzeichnet. Aufgrund einer unvollständigen Prüfung durch einige Primärsysteme konnte im beschriebenen Fall keine eindeutige Zuordnung bei der Identifikation der betroffenen Krankenkasse und der Arztpraxis gewährleistet werden. Diese unvollständige Prüfung ist auf eine fehlende technische Umsetzung seitens des Primärsystemherstellers zurückzuführen. Dadurch wurden die versendeten Nachrichten nicht wie beabsichtigt an die AOK Niedersachsen, sondern fälschlicherweise an eine einzelne Arztpraxis zugestellt. Der betroffene Primärsystemhersteller wird nochmals aufgefordert, die ab 2022 geltende Prüfpflicht unverzüglich umzusetzen.

11. Video-Überwachung

11.1. Grundsätze

Videoüberwachung im Gesundheitsbereich erfordert ein hohes Maß an Patientenschutz

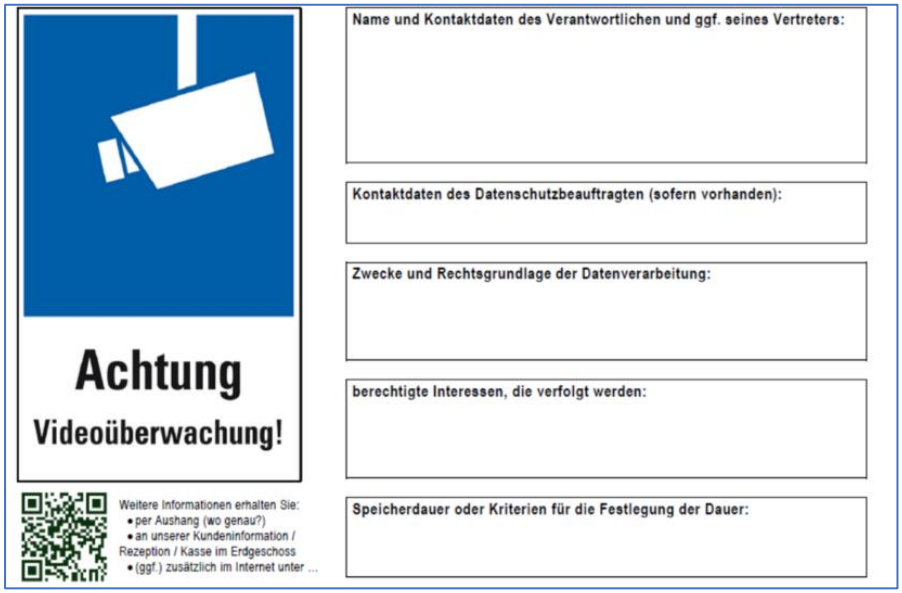
- Die Betroffenen müssen über die Videoüberwachung informiert werden, beispielsweise durch Schilder oder Hinweise bevor der Überwachungsbereich betreten wird.
- Die erhobenen Daten dürfen nur für den jeweiligen Zweck verwendet werden und müssen angemessen geschützt werden.



- Die Überwachung sollte auf das notwendige Maß beschränkt sein und keine Audio-Aufnahmen von Patientengesprächen oder medizinischen Untersuchungen umfassen.
- Eine Datenverarbeitung zur Erstellung von Bewegungsprofilen oder zur automatisierten Entscheidungsfindung ist in der Regel unzulässig.
- Eine Datenschutz-Folgenabschätzung sollte durchgeführt werden, um mögliche Risiken für die Betroffenen zu bewerten.
- Es sollte stets ein Datenschutzbeauftragter zu Rate gezogen werden.

Im Falle einer unrechtmäßigen Videoüberwachung können betroffene Personen Schadensersatzansprüche geltend machen und eine Beschwerde bei der Datenschutzaufsichtsbehörde einreichen.

11.2. Patienten-Parkplatz



Der Betreiber muss ein berechtigtes Interesse an der Überwachung nachweisen, wie beispielsweise die Erhöhung der Sicherheit oder die Verhinderung von Straftaten, mit Bezug auf vergangene und mehreren Vorfällen.

11.3. Wartezimmer

Die Videoüberwachung im Wartezimmer einer Arztpraxis ist grundsätzlich nur unter bestimmten erschwerten Voraussetzungen zulässig, da es sich um einen sensiblen Bereich handelt, in dem Patienten auf medizinische Hilfe warten und in der Regel nicht möglich.

11.4. Medizinisch erforderliche Videoüberwachung (Aufwachraum, MR, CT, Schlaflabor)

- Der Betreiber muss ein berechtigtes Interesse an der Überwachung nachweisen können, wie beispielsweise die Überwachung von Patienten, die sich in einem kritischen Zustand befinden, die nach einer Operation oder einer anderen medizinischen Behandlung aufwachen oder um sicherzustellen, dass sich keine Unbefugten im Aufwachraum aufhalten.
- Im Gesundheitsbereich, z.B. in radiologischen Praxen, kann es bei der medizinisch gebotenen Videoüberwachung von Patienten im Untersuchungs- oder Behandlungsgerät – u.a. aus strahlenschutztechnischen Gründen – geboten sein, dass trotz anwesenden medizinischen Personals, wegen des einzuhaltenden Abstands zum Patienten und der Strahlenquelle im Rahmen der Behandlung (und dazu gehört auch die Diagnostik) eine Videoüberwachung nötig sein. Eine

Aufzeichnung und Speicherung findet dabei nicht statt, was dem Grundsatz der Datenminimierung entspricht.

- Im medizinischen Schlaflabor dient die Videoüberwachung einem möglichst ungestörten Schlaf und damit einer besseren Diagnose. Auch in der Psychiatrie, bei orthopädischen Ganganalysen oder der Sportmedizin kann es medizinische Indikationen für die Videoaufnahme der Patienten zu diagnostischen Zwecken geben und für die Erfüllung der Dokumentationspflicht erforderlich sein.

Da die Videoüberwachung in diesem Fall im Rahmen der Behandlung stattfindet, dürften die Videoaufnahmen als Gesundheitsdaten, Art. 9 Abs. 1 DSGVO, einzustufen sein, bei denen keine Interessenabwägung vorgenommen werden kann. Stattdessen ergibt sich die Zulässigkeit der Datenverarbeitung aus Art. 9 Abs. 2 lit. h) DSGVO – „Verarbeitung für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich“. Ist der Patient nicht bei Bewusstsein, so kann die Rechtfertigung zur medizinisch gebotenen Videoüberwachung in der Wahrung lebenswichtiger Interessen des Patienten liegen, Art. 9 Abs. 2 unten c) DSGVO.

12. Angriff von außen

12.1. Phishing:

Angriffe sind eine der ältesten und effektivsten Methoden von Cyberangriffen, bei denen Angreifer versuchen, sensible Informationen wie Anmeldedaten, Kreditkartennummern oder vertrauliche Unternehmensinformationen von Benutzern abzufangen. Es gibt verschiedene Arten von Phishing-Angriffen, die sich in Technik und Zielsetzung unterscheiden.

12.2. Spear Phishing:

Spear Phishing ist eine zielgerichtete und persönlichere Form von Phishing, bei der Angreifer sich als Mitarbeiter eines Geschäftspartners oder einer bekannten Organisation. Sie führen im Voraus Recherchen in Sozial-Media-Plattformen durch, um die Zielperson oder Organisation besser kennenzulernen und ihre Vertraulichkeit auszunutzen.

12.3. Smishing:

Smishing ist eine Kurzform von SMS-Phishing und beinhaltet das Senden von gefälschten SMS-Nachrichten, die vorgeben, von vertrauenswürdigen Quellen zu stammen. Die SMS enthalten oft gefährliche URLs oder Angebote für Rabattaktionen, Freikarten oder andere Vorteile, die das Opfer dazu verleiten, auf die gefälschte URL zu klicken oder eine Antwort zu senden.

12.4. Abwehr-Tool

Die Seite https://www.virustotal.com ermöglicht es Benutzern, verdächtige Dateien und URLs zu analysieren, um Arten von Malware zu erkennen und sie automatisch mit der Sicherheitsgemeinschaft zu teilen. VirusTotal ist ein Online-Sicherheitsdienst, der von der gleichnamigen Firma betrieben wird. Die Plattform bietet mehrere Sicherheitsfunktionen, die im Folgenden erläutert werden:

- Datei-Analyse:
  Benutzer können Dateien hochladen, um sie auf Malware zu überprüfen. VirusTotal analysiert die Dateien mit Hilfe von 80+ Antiviren- und Anti-Malware-Programmen, um Sicherheitsbedrohungen zu erkennen. Wenn eine Bedrohung gefunden wird, zeigt VirusTotal eine Zusammenfassung der erkannten Bedrohungen und die Quelle der Erkennung an.
- URL-Analyse:

Benutzer können URLs eingeben, um sie auf Malware zu überprüfen. VirusTotal analysiert die URL und zeigt Informationen über Sicherheitsbedrohungen und die ermittelten Erkennungen an.

Es ist wichtig zu beachten, dass VirusTotal zwar eine nützliche Ressource für die Erkennung von Malware ist, aber keine Garantie für 100%ige Sicherheit bietet. Daher sollten Benutzer weiterhin auf dem Laufenden bleiben und geeignete Sicherheitsmaßnahmen ergreifen, um ihre Systeme und Daten zu schützen.

13. Angriff von innen - Hacking-Tools:

Die Praxis-EDV ist nicht nur von außen, sondern auch innerhalb der Praxisräume angreifbar. Praxisbesucher oder Dienstleister der Praxis können in unbeobachteten Momenten auf die EDV zugreifen. Über ungesicherte Schnittstellen, wie z. B. USB, aber auch über LAN-Anschlüsse sind diese für fremde Zugriffsversuche ohne Abwehrprogramme angreifbar, es kann in unbeobachteten Sekunden Schadsoftware eingeschleust oder Daten abgesaugt werden. Die Datendiebe verwenden dabei Hacking-Tools für wenige Euro.

13.1. Kartenkloner:

RFID-Karten üben auf Hacker eine besondere Faszination aus - besonders dann, wenn sie der Zugangskontrolle dienen und sensible Bereiche mit den Serverraum schützen. Das handliche Gerät klont solche und viele weitere Karten im Abstand von 1 Meter mit einem Knopfdruck. Aber auch die **Preis 375 €.**

13.2. Netzwerk-Hai:

Eine offen zugängliche Netzwerk-Buchse ist eine Einladung für Hacker. Das winzige SHARK Jack Cable nimmt diese Einladung gerne an: Im Gehäuse des Netzwerksteckers lauert ein angriffslustiger Linux Computer. Es feuert anschließend ein vorher festgelegtes Skript ab, zum Beispiel um das Netz auszukundschaften und zu attackieren. Der USB-C Anschluss dient nicht nur der Stromversorgung, sondern wird auch als Empfangsantenne für ein Android-Smartphone genutzt, um als USB-Terminal, Kommandos eingeben zu können. **Preis 74 €.**

13.3. Keyboard-Krokodil:

Hardware-Keylogger sind simpel, aber gefährlich: steckt man sie zwischen USB-Tastatur und Rechner, zeichnen sie sämtliche Tastatureingaben auf – Zugangsdaten, E-Mails und vieles mehr. Die Daten werden über WLAN übertragen, oder es werden beliebige Befehle in den Zielrechner gesendet, um zum Beispiel ein Backdoor zu installieren. **Preis 111 €.**

13.4. Hungriger Hase:

Dieser USB-Stick verfolgt seine eigene Agenda. Einmal eingesteckt saugt er bis zu 2 TByte Daten von der Festplatte des attackierten Rechners in sich auf.

Preis 111 €.

13.1. USB-Kabel des Grauens:

Dieses USB-Kabel ist ein voll funktionsfähiges USB-Kabel – es beinhaltet aber ein Angriffsmodul samt Keylogger. Auch für WLAN hat es noch genug Platz. Das Kabel gibt sich als USB-Tastatur und Maus aus, um den Rechner beliebig zu steuern. Über WLAN nimmt es Verbindung mit dem Hacker auf, der nun beliebigen Zugriff auf den PC hat. **Preis 111 €.**

14. Bußgelder und Urteile

Schadensersatzansprüche werden immer relevanter in der Welt des Datenschutzes. Die Häufigkeit der Klagen von Privatpersonen gegen Unternehmen wegen vermeintlicher Persönlichkeitsrechtsverletzungen durch einen Verstoß gegen die DSGVO steigt stetig. Prominentestes und aktuelles Beispiel sind sicherlich die Abmahnungen wegen dem Einsatz von Google Fonts auf Websites.

Art.82 DSGVO *„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“*

Pflichtverletzung

Zusätzlich fordert Art 82 DSGVO einen Verstoß gegen die Pflichten der DSGVO. Hier werden hinsichtlich der Weite des Anspruchs gegenteilige Auffassungen vertreten. Erwägungsgrund 146 Satz 1 DSGVO spricht davon, dass der Verstoß gegen Pflichten aus der DSGVO „aufgrund einer Verarbeitung“ erfolgen muss. Nach einer Ansicht fallen damit die Informationsrechte nicht mehr unter diese Vorschrift. Eine andere Ansicht vertritt, dass selbst Verstöße gegen Formvorschriften der DSGVO ausreichen, wie z.B. die unzureichende Umsetzung technischer und organisatorischer Maßnahmen.

Verschulden

Umstritten ist, ob für die Begründung eines Anspruchs auch ein Verschulden des Verantwortlichen notwendig ist oder ob es sich bei Art. 82 DSGVO um einen verschuldensunabhängigen Schadensersatzanspruch handelt. Die Formulierung „Verantwortlicher“ in der Vorschrift lässt für einige den Schluss zu, dass eine Verantwortlichkeit nur bei Verschulden möglich ist. Die Gegenseite weist darauf hin, dass das Deutsche Verständnis von Verantwortlichkeit hier nicht anwendbar sei und lediglich von Verantwortlichkeit als Rolle als Verantwortlicher im Sinne der DSGVO gesprochen würde.

Schaden

Um eine Forderung zu stellen, braucht es nach deutschem Recht einen Schaden. Hier ist es meist schwer, konkrete Summen zu beziffern, da es sich bei Schäden auf Betroffenenseite oftmals um immaterielle Schäden handelt. Grundsatzfrage ist hierbei, ob der Art. 82 DSGVO eine Sanktionsfunktion für Fehlverhalten hat, also ein Verstoß der DSGVO bereits zu einem Anspruch gegen den Verantwortlichen führt oder ob auch ein klar bezifferbarer Schaden vorliegen muss.

Urteile zu Schadenersatz

- OLG Frankfurt (3 U 21/20): Unzulässige Schufa Meldungen, **500 € Schadensersatz.**
  Hier wurde gegen Art. 6 DSGVO Verstoßen, da die streitgegenständliche Verarbeitung ohne Rechtsgrundlage erfolgte.
- LG München I (31 O 16606/20 1), LG Köln (28 O 328/21): Datenleck und nicht erfolgte Löschung von Kundendaten.
  Hier verstieß ein Verantwortlicher gegen Art. 32, Art 5 Abs. 1 f DSGVO, da keine geeigneten technischen organisatorischen Maßnahmen ergriffen wurden, **2.500 € / 1200 € Schadensersatz.**
- OLG Hamm (Az. 11 U 88/22): Datenpanne im Impfzentrum, **100 € Schadensersatz.**
- OLG Köln (15 U 137/21): Verspätete Auskunft nach Art. 15 DSGVO, **500 € Schadensersatz.**
- BAG (2 AZR 363/21): Auskunft nach Art. 15 DSGVO unvollständig, **1000 € Schadensersatz.**

Der Trend der letzten Jahre ist eindeutig. Schadensersatzklagen gegen Unternehmen häufen sich und werden zunehmend als Massenklagen geführt. Das macht durchaus Sinn, denn die Schadensersatzansprüche aus der DSGVO betreffen meist eine Vielzahl von Personen auf einen Schlag. Google Fonts wird nicht der letzte Anlass für eine Klagewelle gewesen sein. Unternehmen sollten insbesondere bei der Dokumentation und Umsetzung der Betroffenenrechte und der technischen und organisatorischen Maßnahmen besondere Sorgfalt walten lassen, um sich im Ernstfall gegen Schadensersatzansprüche verteidigen zu können.

15. TOP 2023 EU-Bußgelder

Unzureichende Auskunft: Millionen-Strafe für Spotify

Die schwedische Datenschutzbehörde leitete als federführende Behörde nach mehreren Beschwerden von Privatpersonen eine Untersuchung ein und entschied im Juni endgültig, dass der Musik-Streaming-Anbieter dem in der DSGVO verankerten Auskunftsrecht nicht ausreichend nachgekommen war. Da Spotify AB als Unternehmen mit Niederlassungen und Nutzern in vielen EU-Mitgliedstaaten agiert, waren aufgrund des grenzüberschreitenden Charakters alle Datenschutzbehörden der EU in den Fall involviert. Das Bußgeld in Höhe von 4,99 Millionen Euro wurde verhängt, weil Nutzer, die Auskunftsansprüche gegenüber Spotify geltend machten, regelmäßig keine vollständige Auskunft erhielten. Es fehlten die Zwecke der Verarbeitung, die Kategorien der personenbezogenen Daten, auf die sich die Verarbeitung bezieht, sowie die Kategorien der Empfänger der personenbezogenen Daten. Zudem fehlten Angaben zu den Sicherheitsmaßnahmen bei der Übermittlung personenbezogener Daten in Drittländer und der Zeitraum, in dem die personenbezogenen Daten erhoben wurden, war ungenau.

Behörde: Integritetsskydds myndigheten
Branche: Musikstreaming-Anbieter
Verstoß: Art. 12 Abs. 1 DSGVO, Art. 15 Abs. 1 lit. a)-d) DSGVO
Bußgeld: 4.992.038 Euro

> Das Auskunftsrecht ist als eines der stärksten Betroffenenrechte anzusehen. Dieses Beispiel aus der Praxis zeigt, wie sensibel die Aufsichtsbehörden reagieren, wenn Auskunftsersuchen nicht ausreichend nachgekommen wird.

E-Mail- Newsletter-System ohne Möglichkeit zur Abmeldung

Die Landesbeauftragte für den Datenschutz Niedersachsen verhängte ein Bußgeld nach der DSGVO in Höhe von 50.000 €, weil ein Versandhändler ein E-Mail-Newsletter-System betrieb, das über einen relevanten Zeitraum keine Abmeldung ermöglichte. Grund hierfür war eine technische Störung. Da das Unternehmen die Newsletter in einer relativ hohen Frequenz versandt hatte, führte dies bei einzelnen datenschutzrechtlich Betroffenen zu einer erheblichen Anzahl unerwünschter E-Mails. Einige Betroffene versuchten, sich auf anderem Wege zu helfen, indem sie ihre Betroffenenrechte geltend machten. Allerdings waren auch Abmeldungen vom Newsletter über die Servicemitarbeiterinnen und -mitarbeiter des Unternehmens erfolglos, so dass den Werbewidersprüchen letztlich nicht nachgekommen wurde. In mindestens einem Fall wurde auch die vom Betroffenen verlangte Auskunft nicht erteilt.

Behörde: Die Landesbeauftragte für den Datenschutz Niedersachsen
Branche: Versandhändler
Verstoß: Art. 15, 21 DSGVO
Bußgeld: 50.000 Euro

E-Mail-Marketing in Form von Newslettern erfreut sich nach wie vor großer Beliebtheit. Da dabei neben wettbewerbsrechtlichen vor allem datenschutzrechtliche Aspekte zu beachten sind, ist es nicht verwunderlich, dass sich auch die deutschen Aufsichtsbehörden mit diesem Thema beschäftigen. Sind die wichtigsten Aspekte jedoch umgesetzt, steht einer datenschutzkonformen Umsetzung des E-Mail-Marketings nichts mehr im Wege.

Alexa, eine Geldstrafe für Amazon bitte

Kein Bußgeld nach DSGVO, aber Aufsehen erregend: In einem umfangreichen Verfahren gegen Amazon und zwei seiner Tochtergesellschaften haben die Federal Trade Commission (FTC) und das Department of Justice (DOJ) ein Bußgeld in Höhe von 28,8 Millionen Euro verhängt. Die Strafe setzt sich aus zwei Fällen zusammen: Zum einen hat die von Amazon übernommene Sicherheitsfirma Ring Kundendaten nicht ausreichend geschützt und Sicherheitsmerkmale von Produkten falsch dargestellt. Außerdem habe Amazon Mitarbeitern und Auftragnehmern erlaubt, über Ring gesammeltes Videomaterial einzusehen, was zu einer schwerwiegenden Verletzung der Privatsphäre der Kunden geführt habe. Das Bußgeld wurde durch Alexa, Amazons sprachaktivierter Assistentin, noch verstärkt. Alexa speicherte Aufnahmen von Kinderstimmen auf unbestimmte Zeit, manchmal auch nachdem die Eltern um Löschung gebeten hatten. Unter den Aufzeichnungen befanden sich auch sensible Geolokalisierungsdaten. Außerdem wurde der Algorithmus mit diesen Daten trainiert.

Behörde: Federal Trade Commission
Branche: Onlineversandhändler
Verstoß: Sec. 5 FTC Act
Bußgeld: 28.802.378 Euro

Dass Amazon beim Thema Datenschutz wenig Ambitionen zeigt, ist bekannt. Auch nach unzähligen Verfahren und Skandalen rund um das Thema Datenschutz lernt der Konzern, der mit den Daten seiner Nutzer Prozesse optimiert und Umsätze steigert, offenbar nicht dazu.

Vorsicht beim Einsatz von Google Analytics

Und wieder die Schweden: Aufgrund einer Beschwerde leitete die schwedische Datenschutzbehörde IMY eine Untersuchung wegen der Übermittlung personenbezogener Daten in die USA ein. Im Ergebnis wurde ein Bußgeld in Höhe von 1.016.475 Euro verhängt. Grund dafür war, dass das betroffene Telekommunikationsunternehmen auf seiner Website das Statistik-Tool Google Analytics eingesetzt hatte. Die Übermittlung und Speicherung personenbezogener Daten durch Google Analytics in einem Drittland war auf die Standardvertragsklauseln gestützt worden. Die Behörde beanstandete jedoch, dass Google bzw. das Unternehmen keine ausreichenden zusätzlichen technischen Schutzmaßnahmen getroffen hatte, um einen Zugriff auf personenbezogene Daten durch US-Geheimdienste zu verhindern.
Behörde: Integritetsskydds myndigheten
Branche: Telekommunikationsunternehmen
Verstoß: Art. 44 DSGVO
Bußgeld: 1.016.475 Euro

Die schwedische Aufsichtsbehörde stützte sich in ihrer Bußgeldbegründung auf das allseits bekannte Schrems II-Urteil des EuGHs. Wie bereits berichtet, prüfen seitdem auch die deutschen Auf-

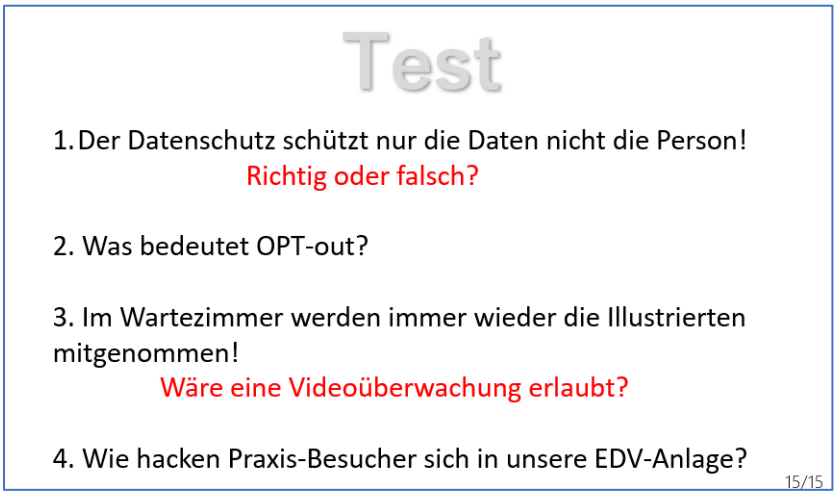
sichtsbehörden koordiniert Datenübermittlungen von Unternehmen in Drittstaaten. Gerade im Hinblick auf Google Analytics ist große Vorsicht geboten, da bereits mehrere europäische Aufsichtsbehörden den Einsatz von Google Analytics für unzulässig erklärt haben. Wer auf Nummer Sicher gehen will, sollte sich nach Alternativen umsehen. Wer das Tool dennoch einsetzen möchte, sollte dies zumindest datenschutzkonform tun.

Mangelnde Sicherheit aufgrund fehlender Multifaktor-Authentifizierung

Die isländische Aufsichtsbehörde verhängte ein Bußgeld gemäß der Datenschutz-Grundverordnung gegen ein im Gesundheitswesen tätiges Unternehmen. Grund dafür war das Fehlen einer Multifaktor-Authentifizierung für den Zugang von Mitarbeitern und Gesundheitsdienstleistern zu Informationssystemen mit Gesundheitsinformationen. Außerdem hatte das Unternehmen reale Daten für einen Test eines Sicherheitssystems verwendet.
Behörde: Persónuvernd
Branche: Gesundheitsunternehmen
Verstoß: Art. 5 Abs. 1 lit. f) DSGVO, Art. 25 DSGVO, Art. 32 DSGVO
Bußgeld**:** 13.468 Euro

Dieser Fall aus der Praxis zeigt, dass Verstöße gegen die Sicherheit der Datenverarbeitung nach Art. 32 DSGVO immer mehr in den Fokus rücken. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ist ein unumgängliches Thema. Um Daten zu schützen und vor Zugriffen zu sichern, gibt es verschiedene Möglichkeiten der Authentifizierung. Dies gilt umso mehr, wenn auch Gesundheitsdaten als besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO betroffen sind. Es ist daher gut und richtig, dass die Aufsichtsbehörden derartige Verstöße europaweit ahnden.

16. Test



Zu 1. Falsch! Die Person schützt den Einzelnen vor Datenmissbrauch. Daten ohne Personenbezug sind nicht datenschutzrelevant, mit Ausnahme von Gesundheitsdaten, die allein aufgrund ihrer Besonderheit einen möglichen Personenbezug enthalten.
Zu 2. Der Betroffene muss aktiv der Datenverarbeitung widersprechen, ansonsten werden seine Daten verarbeitet.
Zu 3. Nein! Die Verhältnismäßigkeit ist nicht gegeben. Recht auf eigenes Bild überwiegt minderem Sachwert.
Zu 4. Durch unbemerktes anstecken von Hacker-Geräten, an offenen zugänglichen Lan- und USB-Ports, z.B. „Hungriger Hase“