## Ausgabe 08 /2022

Liebe Leserin, lieber Leser,

das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) führt zurzeit anhand eines Prüfbogens eine Präventionsprüfung zur Absicherung von E-Mail-Accounts durch. Grund dafür ist ein verstärktes Aufkommen von Cyberattacken auf E-Mail-Accounts von Unternehmen in Bayern. Hierbei versuchen Kriminelle über E-Mail-Dienste die Angeschriebenen dazu zu verleiten, beispielsweise geänderte Zahlungsdaten zu berücksichtigen, enthaltene Links anzuklicken oder einen Dateianhang zu öffnen. Dies kann zu immensen Schäden führen.

Mit einer Handreichung bietet das BayLDA seine Unterstützung für den Schutz von E-Mail-Accounts an. Hier sind technische und organisatorische Maßnahmen dargestellt, die für alle Unternehmen interessant sind. Diese Maßnahmenempfehlungen helfen Ihnen, das Risiko einer Cyberattacke zu minimieren. Gerne sind wir Ihnen hierbei behilflich.

Unsere Themen und Quellen im Überblick:

- **Doctolib im Fokus der Aufsichtsbehörde**
  https://www.dr-datenschutz.de/doctolib-im-fokus-der-aufsichtsbehoerde/

- **Immer mehr Aufsichtsbehörden haben die Faxe(n) dicke**
  https://www.althammer-kill.de/aktuelles/news/detail/immer-mehr-aufsichtsbehoerden-haben-die-faxen-dicke

- **Aufsichtsbehörden veröffentlichen gemeinsame Prüfliste zur Bewertung von Auftragsverarbeitungsverträgen von Webhostern**
  https://www.datenschutz-notizen.de/aufsichtsbehoerden-veroeffentlichen-gemeinsame-pruefliste-zur-bewertung-von-auftragsverarbeitungsvertraegen-von-webhostern-2637101/

- **E-Rezept-Verfahren: maschinenlesbare Codes schützen!**
  https://www.datenschutzzentrum.de/artikel/1414-E-Rezept-Verfahren-maschinenlesbare-Codes-schuetzen!.html

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

## ➢ Doctolib im Fokus der Aufsichtsbehörde

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) hat am 24. Mai 2022 ihren Jahresbericht 2021 veröffentlicht und berichtet unter anderem von Untersuchungen, die das Ärzteportal Doctolib betreffen. Aufgrund von zwei Hinweisen prüfte die BlnBDI hierbei, ob Daten unzulässig an Dritte übermittelt werden, und ob der Anbieter seinen Löschverpflichtungen nach Schließung eines Kontos nachkommt.

Bei Doctolib handelt es sich um einen E-Health-Anbieter, der es dem Patienten ermöglicht, über ein Terminvermittlungsportal online selbst Arzttermine zu buchen. Auf der Webseite oder über die App kann der Patient in einem von ihm bestimmten Umkreis nach freien Terminen bei einem Facharzt suchen. Für die Buchung des Termins ist jedoch ein Nutzerkonto erforderlich, wobei ein Vertragsverhältnis zwischen dem Patienten und Doctolib zustande kommt. Neben der E-Mail-Adresse, des Geburtsdatums und einer Telefonnummer ist auch anzugeben, wie man versichert ist und was der Besuchsgrund ist. Insbesondere bei dem Besuchsgrund kann es sich um sehr sensible Daten handeln, die Rückschlüsse auf den körperlichen und geistigen Gesundheitszustand des Patienten erlauben. Besonders problematisch ist die Übermittlung sensitiver Daten (z. B. Symptome) an Unternehmen in Staaten mit einem unzureichenden Datenschutzniveau. Folgender Vorwurf ist im Jahresbericht der BlnBDI zu finden:

*„Durch die Sicherheitsforscher:innen wurde festgestellt, dass Daten u. a. an ein US-amerikanisches Unternehmen und damit in einen unsicheren Drittstaat übermittelt wurden.“*

In diesem Fall soll es sich um die Unternehmen Facebook und Outbrain handeln, die über den Einsatz von Cookies an sensible Informationen gelangt sind. Doctolib entfernte diese Cookies und veranlasste die Löschung der sensiblen Daten bei den genannten Unternehmen. Der Vorwurf des Datenschutzverstoßes bleibt jedoch bestehen.

Weiterhin kritisiert die Aufsichtsbehörde das Vorgehen der Berliner Senatsverwaltung im Rahmen einer Impfkampagne gegen Corona. Hierbei wurde Doctolib beauftragt, die Terminvergabe zu koordinieren. Im Fokus der Kritik steht, dass die Bürger im Rahmen des Online-Terminbuchungsprozesses mit der Anlage eines Nutzerkontos auch zwingend ein eigenes Vertragsverhältnis mit Doctolib eingehen müssen. Gefordert war die Einbindung des Unternehmens als Auftragsverarbeiter, da dieser die Daten ausschließlich im Auftrag und auf Weisung des Verantwortlichen verarbeiten darf. Zu lesen ist folgender Vorwurf:

*„Es ist für uns unverständlich, dass die zuständige Senatsverwaltung unsere wiederholten Hinweise zur Art und Weise der Einbindung des Unternehmens als Auftragsverarbeiter für die Terminbuchung in den Impfzentren bisher ignoriert hat.“*

Die BlnBDI sieht die Senatsverwaltung somit in der Pflicht, gegenüber Doctolib die Löschung der Nutzungskonten anzuweisen, sobald diese ihren Zweck erfüllt haben. Die Senatsverwaltung hingegen beruft sich auf das Vertragsverhältnis zwischen Doctolib und dem Nutzer und sieht die Verantwortung zum Löschen seiner Daten beim Nutzer. Was die Untersuchungen der Aufsichtsbehörden ergeben werden bleibt abzuwarten.

Was datenschutzrechtlich beim Einsatz von Terminverwaltungsunternehmen beachtet werden muss, beantwortet die Berliner Beauftragte für Datenschutz und Informationsfreiheit in einer Informationssammlung, die hier abgerufen werden kann:
https://www.datenschutz-berlin.de/themen/gesundheit/terminverwaltung

## ➢ Immer mehr Aufsichtsbehörden haben die Faxe(n) dicke

Bei der Übermittlung personenbezogener Daten sind immer technische und organisatorische Maßnahmen zu treffen, die einen angemessenen Schutz gewährleisten. Weitestgehend sicher vor einem unbefugten Zugriff ist ein Fax bei der Übermittlung durch ein klassisches Telefonnetz – hier liegt eine Ende-zu-Ende-Verschlüsselung vor. Heutzutage wird das Fax jedoch häufig über einen digitalen Anschluss über das Internet übertragen. Wird das Fax nicht verschlüsselt, können die Daten auf dem Verbindungsweg in falsche Hände geraten.

Dass sensible Daten noch per Fax übertragen werden, gefällt den Aufsichtsbehörden nicht. Folgendes ist in verschiedenen Tätigkeitsberichten zu lesen:

*„Aufgrund dieser Unwägbarkeiten hat ein Fax hinsichtlich des Schutzziels Vertraulichkeit das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail, die zu Recht als digitales Pendant zur offen einsehbaren Postkarte angesehen wird. Mehr nicht. Fax-Dienste enthalten in der Regel keinerlei Sicherungsmaßnahmen, um die Vertraulichkeit der Daten zu gewährleisten. Sie sind daher in der Regel nicht für die Übertragung personenbezogener Daten geeignet.“* **LfDI Bremen**

*„Im Interesse der Datensicherheit und vor dem Hintergrund der fortschreitenden Digitalisierung sollten Verantwortliche daher zeitnah alternative Kommunikationsmittel zum Fax prüfen und implementieren.“*
*„Personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, sollten daher grundsätzlich nicht per Fax übertragen werden, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind.“* **LfDI Hessen**

Wir empfehlen Ihnen, immer zu prüfen, ob eine Alternative zum Faxversand (z. B. eine inhaltsverschlüsselte E-Mail) besteht. In Einzelfällen ist eine datenschutzkonforme Faxübermittlung möglich, wenn eine besondere Eile besteht und dies mit Einwilligung der betroffenen Person (ausdrücklich und eigeninitiativ) passiert.

## ➢ Aufsichtsbehörden veröffentlichen gemeinsame Prüfliste zur Bewertung von Auftragsverarbeitungsverträgen von Webhostern

Die Datenschutz-Aufsichtsbehörden von Bayern, Berlin, Niedersachsen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt haben im Zusammenhang mit der geplanten Überprüfung von Auftragsverarbeitungsverträgen von „Webhosting“-Unternehmen eine Checkliste zur Prüfung von Auftragsverarbeitungsverträgen veröffentlicht. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) weist in diesem Zusammenhang darauf hin, dass die Checkliste auch als Standard für die AVV-Prüfung in anderen Bereichen angewendet werden könne.

Die Checkliste enthält in tabellarischer Form die einzelnen Prüfthemen und zeigt anhand von Kriterien an, ob die Anforderungen erfüllt sind oder nicht.

Hier ein paar interessante Ausführungen zu ausgewählten Prüfthemen:

- ein Auftragsverarbeitungsvertrag kann sehr wohl in Allgemeinen Geschäftsbedingungen (AGB) integriert sein
- der Auftragsverarbeitungsvertrag ist schriftlich oder in elektronischer Form abzufassen
- in Auftragsverarbeitungsverträgen müssen **keine** technischen und organisatorischen Maßnahmen konkret geregelt sein, ein Hinweis auf die Einhaltung der nach Art. 32 DSGVO erforderlichen Maßnahmen kann ausreichen
- die gesetzlichen Anforderungen an die Vereinbarung von Kontrollrechten zu Gunsten des Auftraggebers sind nicht erfüllt, wenn eine allgemeine Kostentragungspflicht seitens des Auftraggebers vorgesehen wird und diese keine Ausnahme für erforderliche Kontrollen oder Unterstützungsleistungen vorsieht

Hinweise zur Nutzung der Checkliste find Sie hier:
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/a/2022-BlnBDI-Checkliste_Pruefung_AVV_v1.0_Ausfuellhinweise.pdf

## ➢ E-Rezept-Verfahren: maschinenlesbare Codes schützen!

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stellt in diesem Artikel klar, dass das E-Rezept vom ULD weder aus datenschutzrechtlichen Gründen beanstandet noch eine Untersagung für das E-Rezept ausgesprochen wurde.

Folgendes ist vorgesehen:

1. Für Nutzende mit einem neueren Smartphone und einer kompatiblen Gesundheitskarte steht die **E-Rezept-App** zur Verfügung.
2. Alternativ kann ein **Ausdruck** erfolgen. Dieser unterscheidet sich vom bisherigen Verfahren (das rosafarbene Papier-Rezept) durch den maschinenlesbaren DataMatrix-Code (ähnlich einem QR-Code), der von der Apotheke gescannt werden kann.

Da nicht jeder ein geeignetes Smartphone besitzt, wird überlegt, welches digitale Verfahren zusätzlich genutzt werden kann. In diesem Zusammenhang sieht das ULD den Weg per E-Mail oder SMS äußerst kritisch. Zwar enthält der hierbei unverschlüsselt versendete DataMatrix-Code keine sensiblen Daten, ermöglicht dem Besitzer jedoch Zugriff auf die zentral gespeicherte vollständige ärztliche Verordnung. Hierzu ist auch die Einschätzung der Datenschutzbehörde Schleswig-Holstein interessant, die sie unter „Urteile“ finden können. Anstelle der E-Rezept-App oder dem Ausdruck kämen laut ULD beispielsweise die Nutzung des Systems „Kommunikation im Medizinwesen“ (KIM) oder ein digitaler Versand z. B. per E-Mail mit zusätzlicher Ende-zu-Ende-Verschlüsselung infrage.

## ➢ Urteile

Datenschutzbehörde Schleswig-Holstein: E-Rezept-QR-Code per E-Mail oder SMS verletzt DSGVO

Nach Einschätzung der Datenschutzbehörde Schleswig-Holstein verstößt die bislang vorgenommene Zusendung von E-Rezept-QR-Codes per E-Mail oder SMS gegen die Regelungen der DSGVO. Dies gilt auch für den Fall, dass der Patient der Zusendung zugestimmt hat.

Inhaltlich geht es um das E-Rezept und die Zusendung des QR-Codes per E-Mail oder SMS-Verfahren an Patienten oder Apotheken. Es genüge auch nicht, wenn der Patient der Zusendung zuvor ausdrücklich zugestimmt habe. Wie die Kassenärztliche Vereinigung Schleswig-Holstein mitteilt, wurde das QR-Code-Verfahren inzwischen eingestellt.

EUR 500 Schadensersatz für verspätete DSGVO-Auskunft

Die Klägerin war ehemalige Mandantin bei dem verklagten Rechtsanwalt, bei dem es um die Durchsetzung von Ansprüchen aus einem Verkehrsunfall ging. Hierbei kam es zum Streit und die Klägerin verlangte eine DSGVO-Auskunft. Diese erfolgte erst nach Ablauf eines Monats und somit verspätet.

Sie machte geltend, dass sie durch die verzögerte Datenauskunft des Beklagten psychisch belastet wurde und sie Stress und Sorge gehabt habe, ob ihre Ansprüche aus dem Verkehrsunfall überhaupt noch wirksam durchgesetzt werden könnten.

*Urteil des OLG Köln vom 14. Juli 2022 - Az.: 15 U 137/21*

## ➢ Weitere interessante Links

Die datenschutzkonforme Konfiguration von Microsoft Teams
Dieser Beitrag enthält eine Checkliste zur datenschutzkonformen Anwendung von MS Teams.
https://www.althammer-kill.de/aktuelles/news/detail/die-datenschutzkonforme-konfiguration-von-microsoft-teams

WLAN – Authentifizierungsmethoden und Angriffsvektoren
Viele werden es kennen: Das mobile Datenvolumen ist schon wieder aufgebraucht und man muss dringend etwas nachschauen. Die schnelle und einfache Lösung ist, das Einklinken in eine (am besten kostenlose) WLAN-Verbindung vom Café nebenan, vom Bahnhof oder ein freies Netzwerk eines Telefonanbieters. Wie sicher diese so einfach scheinende Lösung ist und warum sie einem schnell zum Verhängnis werden kann, klärt dieser Beitrag.
https://www.dr-datenschutz.de/wlan-authentifizierungsmethoden-und-angriffsvektoren/

Zahnärztliche Behandlungen: Anträge jetzt digital möglich
GKV-Spitzenverband und Kassenzahnärztliche Bundesvereinigung (KZBV) hatten sich hierzu auf das Elektronische Beantragungs- und Genehmigungsverfahren – Zahnärzte (EBZ) verständigt.
https://www.gkv-spitzenverband.de/gkv_spitzenverband/presse/pressemitteilungen_und_statements/pressemitteilung_1480960.jsp

Krankenkassen müssen Video-Ident-Verfahren abschalten
Den deutschen Krankenkassen ist die Identifikation ihrer Versicherten per Video-Ident-Verfahren durch die zuständige Gematik GmbH untersagt worden.
https://www.datenschutzticker.de/2022/08/krankenkassen-muessen-video-ident-verfahren-abschalten/

E-Rezept-Verfahren: maschinenlesbare Codes schützen!
Wichtige Informationen und Fragen und Antworten zum E-Rezept.
https://www.datenschutzzentrum.de/artikel/1414-E-Rezept-Verfahren-maschinenlesbare-Codes-schuetzen!.html

Kein Auftragsverarbeitungsvertrag mehr für Videokonferenz-Tools?
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hebt in ihrem neuen Tätigkeitsbericht etwas hervor, was durch Inkrafttreten des TTDSG Ende letzten Jahres längst Einzug in unsere Gesetze gefunden hat, aber an vielen vorbei gegangen ist.
https://www.datenschutz-notizen.de/kein-auftragsverarbeitungsvertrag-mehr-fuer-videokonferenz-tools-0237051/

Das wichtigste zum IT-Sicherheitskonzept und IT-Sicherheitsgesetz 2.0
Was ist überhaupt ein IT-Sicherheitskonzept und welche Regelungen bringt das IT-Sicherheitsgesetz 2.0 mit sich?
https://keyed.de/blog/das-wichtigste-zum-it-sicherheitskonzept-und-it-sicherheitsgesetz-2-0/

Patientendaten ungeschützt im Netz
Wegen einer Sicherheitslücke bei einer Praxissoftware waren laut *NDR* und *WDR* Daten von Behandlungsverläufen und Attesten für Fremde einsehbar. Ein Problem: Hersteller sind nicht verpflichtet, datenschutzkonforme Software zu liefern.
https://www.tagesschau.de/investigativ/ndr-wdr/sicherheitsluecke-arztsoftware-101.html?utm_source=pocket-newtab-global-de-DE

Die persönliche Haftung des Arbeitnehmers bei einem DSGVO Verstoß
Im deutschen Recht gilt grundsätzlich, dass derjenige, der einen Schaden zu vertreten hat, auch den entstandenen Schaden ersetzen muss (§ 276 BGB). Jeder ist also für sein eigenes Verhalten verantwortlich, egal ob in der Freizeit oder im Beruf. Das Bürgerliche Gesetzbuch (BGB) differenziert prinzipiell nicht nach dem Ort oder der Zeit, sondern, wenn überhaupt, nach dem Grad der persönlichen Pflichtverletzung.
https://www.datenschutz-notizen.de/die-persoenliche-haftung-des-arbeitnehmers-bei-einem-dsgvo-verstoss-4936926/