Newsletter

Ausgabe Februar 2023

Liebe Leserin, lieber Leser,

unser neuer Newsletter hält wieder interessante Themen für Sie bereit.

Unsere Themen und Quellen im Überblick:

- **EU-Ausschuss lehnt Angemessenheit des EU-US-Datenschutzrahmens in Entwurf einer Stellungnahme ab**
  https://www.datenschutzticker.de/2023/02/ausschuss-des-europaeischen-parlaments-lehnt-angemessenheit-des-eu-us-datenschutzrahmens-in-entwurf-einer-stellungnahme-ab/

- **Schutzziele der Informationssicherheit**
  https://www.dr-datenschutz.de/schutzziele-der-informationssicherheit/

- **vzbv prüft Datenschutz bei Anbietern von Videosprechstunden**
  https://www.dr-datenschutz.de/vzbv-prueft-datenschutz-bei-anbietern-von-videosprechstunden/

- **Phishing 2023**
  https://www.datenschutz-notizen.de/phishing-2023-1540544/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ EU-Ausschuss lehnt Angemessenheit des EU-US-Datenschutzrahmens in Entwurf einer Stellungnahme ab

In unserer Newsletter Ausgabe Dezember 2022 hatten wir Sie darüber informiert, dass die Europäische Kommission einen Entwurf für einen neuen Angemessenheitsbeschluss veröffentlicht hat. Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments hat nunmehr die Europäische Kommission dazu aufgefordert, den Entwurf nicht anzunehmen.

Verwiesen wird hierbei auf die Artikel über den Schutz der Privatsphäre und den Datenschutz und die Tatsache, dass der wahllose Zugriff von Nachrichtendiensten auf die elektronische Kommunikation das Grundrecht auf Vertraulichkeit der Kommunikation und das Wesen des Rechts auf einen Rechtsbehelf verletze. Eine Gleichwertigkeit der Datenschutzrahmen zwischen der EU und den USA werde nicht hergestellt, so dass unter diesen Voraussetzungen keine neue Angemessenheitsentscheidung getroffen werden könne. Der Ausschuss fordert die Kommission auf, die Verhandlungen mit ihren US-amerikanischen Partnern fortzusetzen, um so einen Mechanismus zu schaffen, der eine solche Gleichwertigkeit gewährleistet und das angemessene Schutzniveau bietet.

Es ist davon auszugehen, dass sich das EU-Parlament dieser Ansicht anschließen wird und somit kein neuer Angemessenheitsbeschluss für den Datentransfer in die USA zeitnah zur Verfügung steht.

➢ Schutzziele der Informationssicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ermöglicht mit seiner Methodik des IT-Grundschutzes ein effektives Management von Informationssicherheit. Folgende grundlegenden Schutzziele sind hierbei elementar und als Kriterien heranzuziehen:

- **Integrität:** Die Informationen sind verlässlich und können nicht manipuliert werden.
- **Vertraulichkeit:** Nur autorisierte Personen haben Zugriff zu den Informationen.
- **Verfügbarkeit**: Informationen sind zu den gewünschten Zeitpunkten verfügbar.

Auch wenn diese Ziele in den Unternehmen eine unterschiedlich große Rolle spielen, geht es in erster Linie um den Schutz vor Manipulation, Offenlegung, Datenverlust oder Diebstahl von Informationen.

Um den Schutzbedarf für Geschäftsprozesse im ersten Schritt einzuschätzen, ist eine Risikobewertung vorzunehmen, wobei folgende Kategorien berücksichtigt werden können:

- **Normal:** Die Auswirkungen eines Schadens sind begrenzt und überschaubar.
- **Hoch:** Die Auswirkungen eines Schadens können beträchtlich sein.
- **Sehr hoch:** Die Auswirkungen eines Schadens sind schwerwiegend, bzw. existenzbedrohend.

Der IT-Grundschutz bietet verschiedene Vorgehensweisen an, die sich an unterschiedliche Anwendergruppen richten und unterschiedliche Ziele verfolgen: Basis-, Standard- und Kern-Absicherung. Hierbei ist zu berücksichtigen, dass Informationen umso mehr zu schützen sind, je höher der Schutzbedarf ist. Dies bedeutet natürlich mehr Arbeit und finanziellen Aufwand. Die Standardabsicherung bildet für Unternehmen den ersten Schritt, wohingegen die Kernabsicherung Informationen mit sehr hohem Schutzbedarf schützt.

Weitere folgende Schutzziele können für die Informationssicherheit von Bedeutung sein:

- **Authentizität:** Es wird sichergestellt, dass der Absender der Information echt ist.
- **Nichtabstreitbarkeit:** Eine Kommunikation kann verbindlich einem Absender zugeordnet werden.
- **Verlässlichkeit:** Ein System übt seine Funktionsweise konsistent aus.

Bei der Erstellung von Schadensszenarien spielen die Auswirkungen eine große Rolle. Diese sind jedoch nicht immer einfach zu bewerten. So sind direkte finanzielle Schäden leichter zu erkennen, als solche, die beispielsweise durch einen Imageverlust entstehen. Um eine Grundlage für eine Priorisierung der Schutzmaßnahmen zu schaffen, ist die ganzheitliche Betrachtung von großer Bedeutung. Um möglichen Schäden vorzubeugen, ist eine Definition und Gewichtung von Schutzzielen sehr wichtig. Es ist somit zu empfehlen, sich mit diesem Thema auseinanderzusetzen und verschiedene Blickwinkel und Diskussionsgrundlagen mit einfließen zu lassen.

➢ vzbv prüft Datenschutz bei Anbietern von Videosprechstunden

Die Verbraucherzentrale Bundesverband e.V. (vzbv) hat diesen Monat die Analyse „Datenschutz bei Videosprechstunden“ veröffentlicht.

In der Analyse wurden neun Telemedizin-Plattformen und Arzttermin-Portale untersucht, die auch Videosprechstunden anbieten. Dies sind die Prüfkategorien, die sich an der DSGVO orientieren:

- Auffindbarkeit, Sprache und Aktualität der Datenschutzerklärung
- Informationen über Verantwortlichen und Datenschutzbeauftragten
- Benennung der Zwecke und Rechtsgrundlagen der Datenverarbeitung
- Ausdrückliche Einwilligung in die Verarbeitung von Gesundheitsdaten
- Empfänger und Dritte in der Datenschutzerklärung
- Widerruf der Datenverarbeitung
- Gastzugang zur Videosprechstunde
- Betroffenenrechte
- Datenübermittlung außerhalb der EU
- Speicherdauer

Im Ergebnis stellt der vzbv fest, dass viele Kategorien zufriedenstellend umgesetzt werden, es aber Datenschutzlücken gibt und einige Datenschutzstandards nicht eingehalten werden. So wird kritisiert, dass einige Portale keine wirksame, ausdrückliche Einwilligung zur Verarbeitung von Gesundheitsdaten einholen. Weiterhin wurde bei der Analyse festgestellt, dass acht der neun geprüften Portale Tracking-Anbieter einbinden. Diese sollten nach vzbv nur eingesetzt werden, wenn es unbedingt erforderlich ist. Ebenfalls bemängelt der vzbv, dass nur drei der Anbieter ein Löschkonzept vorweisen und fünf Anbieter die Daten nur nach Aufforderung durch den Nutzer löschen oder nach Widerruf der Einwilligung in die Datenverarbeitung.

➢ Phishing 2023

Phishing wird von Betrügern eingesetzt, um an Daten von Nutzern zu gelangen. Diese dienen dann beispielsweise dazu, auf Konten zuzugreifen, die Identität zu stehlen oder eine Schadsoftware zu installieren.

Eine neue Art des Phishings arbeitet mit digitalen Unterschriften. Verschiedene Anbieter ermöglichen es, Verträge papierlos zu unterschreiben und abzuschließen. Über einen Link, der per Mail verschickt wird, kann der Nutzer das Dokument aufrufen und digital unterschreiben. Sollten Sie eine Mail mit einem solchen Link erhalten - seien Sie misstrauisch. Insbesondere dann, wenn Sie keinen Vertrag zur Unterzeichnung erwarten.

Folgende Details in der E-Mail sind hilfreich, um eine etwaige Fälschung und somit einen Betrug zu erkennen:

- Achten Sie auf die vollständige Absenderadresse, insbesondere auf den Teil nach dem @-Zeichen, der Rückschlüsse auf den Absender zulässt. Häufig sind es auch nur kleine Rechtschreibfehler beim Namen des Anbieters, die den Empfänger stutzig machen sollten.
- Der Absender wird im E-Mail-Text absichtlich versteckt, indem blaue Schrift auf blauem Grund gewählt wird.
- Im Weiteren gibt es keine persönliche, namentliche Anrede und es wird Druck aufgebaut, da das Dokument beispielsweise nur noch für zwei Tage verfügbar ist.
- Fährt man zudem mit dem Mauszeiger über die Klick-Fläche, wird angezeigt, wohin man bei einem Klick weitergeleitet wird. Hier ist meist zu erkennen, dass es sich nicht um einen Link zu dem Anbieter handelt.
- Die Phishing-Mail bietet keine alternative Signiermethode.
- Auf die Abbestellmöglichkeiten und die App wird nicht verlinkt.

Der Artikel enthält beispielhafte Darstellungen von Originalnachrichten und Fälschungen, die sehr hilfreich sind. Bei Zweifeln an der Echtheit einer solchen E-Mail immer Rücksprache mit der IT oder dem Versender des Vertrags halten.

➢ Urteile

<u>Jameda.de darf Arzt-Daten auch ohne Zustimmung des Betroffenen auf Plattform speichern</u>

Die Online-Plattform Jameda.de ist berechtigt, allgemein zugängliche Arzt-Daten auch ohne Zustimmung des Betroffenen auf ihrer Plattform zu speichern, da ein Fall der berechtigten Interessen nach Art. 6 Abs.1 f) DSGVO vorliegt.

In diesem Fall hatte ein Arzt bei der verklagten Webseite Jameda.de keinerlei kostenpflichtige Angebotspakete gebucht. Auch hatte er nicht der Veröffentlichung seiner beruflichen Daten auf dem Portal zugestimmt. Jameda.de hielt auf ihrer Plattform auf Grundlage von öffentlich zugänglichen Daten ein sogenanntes Basis-Profi des Klägers und von zahlreichen weiteren Ärzten vor.

Der Kläger verlangte die Löschung, was der BGH jedoch ablehnte.

Urteil des Bundesgerichtshofs vom 13. Dezember 2022 - Az.: VI ZR 60/21

Zeitlicher Ablauf von Newsletter-Einwilligungen

Das AG München hat in einem Urteil entschieden, dass der Versand von E-Mail-Werbung wegen fehlender Einwilligung unzulässig sei, da diese Einwilligung infolge Zeitablaufs unwirksam wurde.

In diesem Fall war der Kläger bis zum Jahr 2017 Mitglied in einem Golfclub und im Rahmen dieser Mitgliedschaft Inhaber eines Accounts bei der Beklagten. Zu diesem Zeitpunkt lag eine ausdrückliche Einwilligung in die Zusendung von Newslettern vor. Gleichzeitig geht das Amtsgericht davon aus, dass das Abonnement wohl an eine Mitgliedschaft in dem Golfclub gekoppelt war.

Nach Ende der Mitgliedschaft im Golfclub sendete die Beklagte dem Kläger keine Newsletter mehr zu, bis der Kläger zum Ende des Jahres 2021, nach Ende der Kooperation der Beklagten mit dem Deutschen Golf Verband, doch wieder einen Newsletter erhielt. Innerhalb der vergangen vier Jahre nutzte der Kläger weder seinen Account bei der Beklagten, noch erhielt er E-Mails.

Das Amtsgericht geht davon aus, dass die ursprünglich erteilte Einwilligung „angesichts der Umstände des Einzelfalls infolge Zeitablaufs nicht mehr wirksam“ war.

Urteil des Amtsgerichts München vom 14. Februar 2023 - Az.: 161 C 12736/22

➢ Weitere interessante Links

IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit
Das IT-Grundschutz-Kompendium Edition 2023 ist seit dem 1. Februar 2023 verfügbar und löst damit die Edition 2022 ab. Hier gibt es das PDF zum Download.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Der Datenschutz bei Krankenkassen
Um ihre gesetzlichen Aufgaben ordnungsgemäß erfüllen zu können, benötigen Krankenkassen viele, vor allem auch sensible Daten ihrer Versicherten. Dabei greift in Deutschland seit Jahren eine bereichsspezifische Datenschutzregelung, der Sozialdatenschutz, der den Umgang mit den Daten sehr genau vorschreibt.
https://www.dr-datenschutz.de/der-datenschutz-bei-krankenkassen/

BSI bestätigt Ransomware-Angriffe nach Warnung italienischer Behörden
Nachdem die italienische Cyber-Sicherheitsbehörde ACN am Wochenende vor einer weltweisen Ransomware-Attacke gewarnt hatte, bestätigte das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun, dass auch in Deutschland zahlreiche Systeme betroffen sind.
https://www.datenschutzticker.de/2023/02/bsi-bestaetigt-ransomware-angriffe-nach-warnung-italienischer-behoerden/

Videoüberwachung am Arbeitsplatz: Das erlaubt der Datenschutz
Die Videoüberwachung am Arbeitsplatz ist ein heikles Thema, das oft kontrovers diskutiert wird. Dieser Artikel befasst sich daher mit den rechtlichen Grundlagen der Videoüberwachung am Arbeitsplatz.
https://www.dr-datenschutz.de/videoueberwachung-am-arbeitsplatz-das-erlaubt-der-datenschutz/

Datenschutz-Icons
Die hier zum allgemeinen Gebrauch angebotenen Icons sind aus den prämierten Einreichungen zu einem bundesweiten Designwettbewerb hervorgegangen.
https://www.baden-wuerttemberg.datenschutz.de/datenschutz-icons/

46 eAU weia! – Gesundheitsdaten und der Datenschutz
Ein Podcast zum Thema elektronische Arbeitsunfähigkeitsbescheinigung.
https://www.dr-datenschutz.de/podcast/46-eau-weia-gesundheitsdaten-und-der-datenschutz/

EDSA veröffentlicht Berichte zum Einsatz von Clouddiensten und Cookie-Bannern
Der EDSA hat nun einen Bericht über die Ergebnisse seiner ersten koordinierten Prüfung veröffentlicht, die sich auf die Nutzung von Cloud-basierten Diensten durch den öffentlichen Sektor konzentrierte.
https://www.datenschutz-notizen.de/edsa-veroeffentlicht-berichte-zum-einsatz-von-clouddiensten-und-cookie-bannern-5440495/

Berechtigungskonzept DSGVO
In diesem Blogbeitrag erfahren Sie, was ein Berechtigungskonzept ist und welche Merkmale in jedem Berechtigungskonzept enthalten sein sollten.
https://keyed.de/blog/berechtigungskonzept-dsgvo/