Newsletter

Ausgabe November 2022

Liebe Leserin, lieber Leser,

heute erhalten Sie unseren neuen Newsletter.

Angesichts massenhafter Abmahnschreiben wegen des Einsatzes von Google Fonts auf Webseiten ruft die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen die Betreiber der Seiten dazu auf, diese datenschutzkonform zu gestalten. Wir haben Sie bereits über die Möglichkeit der lokalen Einbindung informiert.

Beachten Sie bitte: Sollten Sie auf Ihrer Webseite Tools eingebunden haben, die Google Schriftarten verwenden, ist von den Nutzerinnen und Nutzern eine wirksame Einwilligung für den Einsatz von Google Fonts einzuholen. Hier eine Hilfestellung der LfD:

https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/abmahnungen-zu-datenschutzverstossen-auf-webseiten-vermeiden-google-fonts-lokal-einbinden-217509.html

Unsere Themen und Quellen im Überblick:

- **„Superschutz für Superdaten“ – das Datentransparenzverfahren**
  https://www.dr-datenschutz.de/superschutz-fuer-superdaten-das-datentransparenzverfahren/

- **Wenn Kranke nicht erfahren dürfen, wie krank sie sind**
  https://www.datenschutz-notizen.de/wenn-kranke-nicht-erfahren-duerfen-wie-krank-sie-sind-2239100/

- **Internationale Datentransfers: Muss in Datenschutzhinweisen das konkrete Drittland angegeben werden?**
  https://www.delegedata.de/2022/09/internationale-datentransfers-muss-in-datenschutzhinweisen-das-konkrete-drittland-angegeben-werden/

- **Speicherung von Passwörtern im Browser**
  https://www.datenschutz-notizen.de/speicherung-von-passwoertern-im-browser-3739064/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ „Superschutz für Superdaten“ – das Datentransparenzverfahren

Im Rahmen des Datentransparenzverfahrens sollen zukünftig Gesundheitsdaten für die Forschung besser verfügbar sein. Hierzu sollten die Krankenkassen bis zum 1. Oktober 2022 die ihnen vorliegenden Abrechnungsdaten der gesundheitlichen Versorgung einem Forschungsdatenzentrum (FDZ) bereitstellen. Dort sollen sie immer weiter ergänzt und bis zu 30 Jahre lang gespeichert werden.

Gesundheitsdaten zählen zu den sensibelsten Daten und werden durch die DSGVO besonders geschützt. Die Sprecherin des Chaos Computer Clubs (CCC) sowie eine weitere Person mit einer seltenen Krankheit haben Klage gegen dieses Verfahren, insbesondere gegen die Weitergabe ihrer Daten durch die Krankenkasse, erhoben. Befürchtet wird, dass Sicherheitsmängel bei der Weitergabe der Daten bestehen. Die Klage wendet sich somit nicht gegen die Sammlung der Datensätze als solche, sondern gegen deren konkrete Ausgestaltung. Die Weitergabe der Daten wurde im Eilverfahren untersagt, jetzt wird der Fall im Hauptverfahren eingehend geprüft.

Bei der Übermittlung der Daten werden die Daten lediglich pseudonymisiert. Das heißt, der Name und andere Identifikationsmerkmale werden durch ein Kennzeichen ersetzt, zu dem Zweck, die Bestimmung des Betroffenen zumindest wesentlich zu erschweren. Ohne Hinzuziehung zusätzlicher Informationen sollen die Daten nicht mehr einer spezifisch betroffenen Person zugeordnet werden können. Im Gegensatz zur Anonymisierung schließt dies die Möglichkeit einer Re-Identifizierung der Betroffenen jedoch nicht aus. Auch geben insbesondere seltene Krankheiten häufig Aufschluss darüber, wer sich hinter dem Datensatz verbirgt.

Weiterhin sieht das Datenschutztransparenzverfahren kein Widerspruchsrecht der Betroffenen vor, was gegen das Grundrecht auf informationelle Selbstbestimmung verstößt. Wichtig ist also zu prüfen, ob eine ausreichendes Sicherheitsniveau gewährleistet ist und der Staat seiner Schutzpflicht nachkommt.

In diesem Fall zeigt sich mal wieder, wie wichtig es ist, dass Forschung und Datenschutz Hand in Hand gehen. Die Nutzung von Gesundheitsdaten zu Forschungszwecken bietet einen Mehrwert für die Gesundheitsversorgung und ist durchaus unterstützenswert. Jedoch muss auch das Ziel, die Daten bestmöglich vor Missbrauch zu schützen, oberste Priorität haben. Wie der Richter entscheidet, wird sich zeigen.

➢ Wenn Kranke nicht erfahren dürfen, wie krank sie sind

Patienten haben grundsätzlich das Recht auf eine vollständige Kopie ihrer Patientenakte. Ausgenommen sind nur Fälle, bei denen der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Ob die Einsichtnahme durch den Arzt oder Psychotherapeuten verweigert werden kann, ist eine Einzelfallentscheidung. In vielen Fällen ist eine begleitete Einsicht mit dem Arzt oder einer Vertrauensperson eine gute Möglichkeit.

Folgende Fallgruppen lassen sich unterscheiden:

1. Schwere Krankheit oder Krankheit im Endstadium.
   Hat man früher nur die Angehörigen z.B. über Krebs im Endstadium informiert, ist dies mindestens seit der Sterbehilfe-Entscheidung des BVerfG nicht mehr haltbar.

2. Psychiatrische Diagnosen wie z. B. paranoider Wahn, oder die sog. Rentenneurose.
   Folgendes ist zu unterscheiden:
   a. Es kann sich darum handeln, dass das Vertrauensverhältnis des Patienten zum Behandler und eventuell zu weiteren Personen gestört oder zerstört wird, wenn ein Patient seine Diagnose erhält, solange er keine volle Einsicht in seine Krankheit und Therapiebedürftigkeit hat. Bei einer Paranoia kann die Offenlegung dazu führen, dass die Therapeutin oder der Psychiater vom Patienten dem „Feindeslager" zugeordnet werden und der Patient die Therapie abbricht. In so einem Fall erscheint die Vorenthaltung der Akte notwendig.
   b. Es kann befürchtet werden, dass bei einem traumatisierten Patienten durch die Konfrontation mit dem in der Akte dokumentierten Geschehen eine Re-Traumatisierung auftritt. Hier erscheint es sinnvoll, im ersten Schritt eine begleitende Einsichtnahme durchzuführen. Der Patient hat aber das Recht, sich zu re-traumatisieren, wenn er es will.

3. Verweigerung der Einsichtnahme in die Akte eines Kindes durch die Eltern.
   Z. B. im Fall von Kindesmisshandlungen, bei denen die Eltern als Täter in Frage kommen. Hier geht es nicht um den Schutz der betroffenen Person vor sich selbst, sondern um ihren Schutz vor anderen Personen.

Die Nicht-Herausgabe einer Patientenakte ist also nur in besonderen Fällen möglich und ist zu begründen. Dies stellt eine schwierige Aufgabe dar, da die Begründung dem Patienten möglicherweise Aufschluss über das gibt, was er nicht erfahren soll. Gerade deswegen ist für das Vertrauen zwischen Arzt und Patienten, wenn vertretbar, eine begleitete Einsichtnahme vorzunehmen.

➢ **Internationale Datentransfers: Muss in Datenschutzhinweisen das konkrete Drittland angegeben werden?**

Der Artikel wendet sich den Transparenzpflichten in Bezug auf eine Datenübertragung in ein Land außerhalb des europäischen Wirtschaftsraums (EWR) zu. Dies umfasst eine Informationspflicht des Verantwortlichen, welcher er mit Hilfe von Datenschutzhinweisen auf der Webseite oder gegenüber den Mitarbeitern gerecht werden kann. Der Verantwortliche hat nach § 13 Abs. 1 lit. f DSGVO den Betroffenen die Absicht mitzuteilen, *„die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind*".

Von einer Absicht ist auszugehen, wenn der Verantwortliche die Übermittlung plant und diese will. Hier stellt sich die Frage, ob das Drittland zu benennen ist. Natürlich ist man rechtlich auf der sicheren Seit, wenn der Verantwortliche die Drittländer immer benennt. Handelt es sich jedoch um eine große Anzahl an Drittländern, ist der Aufwand entsprechend hoch.

Was spricht gegen die genaue Angabe des Drittlandes?

- Der **Wortlaut** der Norm, denn es heißt dort „ein Drittland", nicht etwa „das betreffende Drittland" oder ähnlich.

- Der **EDSA** sieht die Benennung der konkreten Drittländer nach Ansicht von Carlo Piltz eher nicht als Pflicht an, sondern empfiehlt deren Angabe. Die Leitlinien sprechen zumindest nicht davon, dass die Information anzugeben ist oder stets angegeben werden muss, sondern verweisen auf den Grundsatz von Treu und Glauben.
- Der Vergleich mit der Pflicht des Art. 30 Abs. 1 lit. e DSGVO. Danach muss der Verantwortliche in dem Verzeichnis der Verarbeitungstätigkeiten gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, ***einschließlich der Angabe des betreffenden Drittlands*** dokumentieren. Hier sieht der Gesetzgeber ganz klar eine Pflicht zur Benennung des „betreffenden Drittlands" vor, was für oben genannten § 13 Abs. 1 lit f DSGVO nicht zutrifft.
- Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) weist in seiner Orientierungshilfe „Informationspflichten des Verantwortlichen" klar darauf hin, dass Art. 13 Abs. 1 lit. f DSGVO nicht die namentliche Nennung des betreffenden Drittlands erfordert. Gleichwohl empfiehlt der BayLfD (ebenfalls unter Verweis auf Transparenzgründe) diese Information bereitzustellen.

➢ Speicherung von Passwörtern im Browser

Eine gute Möglichkeit zur sicheren Aufbewahrung von Passwörtern ist die Verwendung eines Passwort-Managers. Ist jedoch die Speicherung von Anmeldedaten oder Passwörtern im Browser ebenfalls eine gute Lösung?

Folgende Gefahren sind hierbei zu berücksichtigen:

- Erhält ein unbefugter Dritter Zugriff, sei es durch Diebstahl des (mobilen) Geräts, durch kurze Abwesenheit z. B. von einem Laptop, hat dieser die Möglichkeit die gespeicherten Daten bequem zu nutzen.
- Das Einfangen von Viren im Internet (Software für Passwortdiebstähle sind eins der wichtigsten Mittel eines Cyberkriminellen).
- Ein Masterpasswort, das bei jeder neuen Sitzung einmalig eingegeben werden muss kann das Sicherheitsniveau gewiss etwas steigern, eine besonders hohe Sicherheit liegt dabei aber nicht vor. Zudem sollte man dabei darauf achten, dass die Anforderungen an ein sicheres Passwort stets eingehalten werden.

Mittlerweile nutzen Online-Dienste zunehmend die Zwei-Faktor-Authentifizierung, bei der neben Benutzernamen und Passwort eine zusätzliche Sicherheit (z. B. Freigabe durch ein Handy) benötigt wird. Dies minimiert das Risiko, da der Angriff auf mehreren Ebenen erfolgen muss. Grundsätzlich ist die Speicherung von Passwörtern im Browser nicht zu empfehlen. Sollte man sich dennoch dafür entscheiden, ist möglichst ein Online-Dienst mit Zwei-Faktor-Authentifizierung auszuwählen. Ebenso ist die regelmäßige Durchführung von Updates sowie die Nutzung eines Antivirenprogramms notwendig.

Möchte man auf Nummer sicher gehen, ist es ratsam bereits hinterlegte Passwörter zu löschen und die Funktion zur Speicherung von Passwörtern für die Zukunft zu deaktivieren.

➢ Urteile

Kommerzielle Webseite muss E-Mail-Adresse zur Kontaktaufnahme angeben

Die Beklagte, die Fluggesellschaft Brussels Airlines, hatte auf ihrer Webseite im Impressum keine E-Mail-Adresse angegeben.

Das LG Düsseldorf sah hierin einen Rechtsverstoß und unterstrich die Notwendigkeit einer E-Mail-Adresse einer kommerziellen Webseite zur Kontaktaufnahme.

Urteil des Landgerichts Düsseldorf vom 17. August 2022 - Az.: 12 O 2019/22

Datenverarbeitender muss angemessene Maßnahmen treffen, um Dritte über Löschungsbegehren zu informieren

Der für die Verarbeitung personenbezogener Daten Verantwortliche muss geeignete technische und organisatorische Maßnahmen treffen, um die anderen Verantwortlichen, die ihm diese Daten übermittelt haben bzw. denen er die Daten weitergeleitet hat, über den Widerruf der Einwilligung der betroffenen Person zu informieren. Stützen sich verschiedene Verantwortliche auf ein und dieselbe Einwilligung der betroffenen Person, genügt es, wenn sich diese Person an irgendeinen der Verantwortlichen wendet, um ihre Einwilligung zu widerrufen.

Urteil des Europäischen Gerichtshofes vom 27. Oktober 2022 - Az.: C-129/21

➢ Weitere interessante Links

Microsoft 365 nicht datenschutzrechtskonform?
Die Datenschutzkonferenz berichtet…
https://www.datenschutzticker.de/2022/11/microsoft-365-nicht-datenschutzrechtskonform/

ChatBots auf Webseiten – Was ist zu beachten?
Live-Chats und Messenger-Dienste halten auch in der Kundenkommunikation immer mehr Einzug. Dieser Artikel erklärt, was ein Chatbot überhaupt ist und was zu beachten ist.
https://www.dr-datenschutz.de/chatbots-auf-webseiten-was-ist-zu-beachten/

Form und Geltungsdauer eines Werbewiderspruchs
Das Amtsgericht München hat sich mit seinem Urteil vom 05.08.2022 – Aktenzeichen 142 C 1633/22 – konkrete Anforderungen an die Form und Geltungsdauer des Widerspruchs aufgestellt.
https://www.datenschutz-notizen.de/form-und-geltungsdauer-eines-werbewiderspruchs-1038986/

IDS und IPS: Ein zusätzlicher Schutz gegen Cyberangriffe
Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) überwachen ein Netzwerk, eine einzelne Netzwerkkomponente oder auch einen gesamten Server innerhalb einer Infrastruktur und analysieren den entstandenen „Traffic“ auf Signaturen, die auf Cyberangriffe deuten könnten. Dieser Blogartikel soll zeigen, was mit der Nutzung von IDS und IPS erreicht werden kann.
https://www.dr-datenschutz.de/ids-und-ips-ein-zusaetzlicher-schutz-gegen-cyberangriffe/

Aktuelles zur Meldung von Datenpannen aus dem Tätigkeitsbericht des TLfDI
Im aktuellen Tätigkeitsbericht berichtet der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) auch über die Entwicklung von Meldungen von Datenpannen im Jahr 2021.
https://www.datenschutz-notizen.de/aktuelles-zur-meldung-von-datenpannen-aus-dem-taetigkeits-bericht-des-tlfdi-1238870/

Handreichung: Einbindung von Videos in eigene Webseiten
Als Hilfestellung zu diesem Thema hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in einer Kurzübersicht Hinweise zur Einbindung von Videos in eigene Webseiten formuliert.
https://www.baden-wuerttemberg.datenschutz.de/handreichung-einbindung-videos-eigene-webseiten/

Ransomware-Angriffe nehmen zu: Auf den Ernstfall vorbereiten!
Der Beitrag zeigt, warum sich Ransomware-Angriffe weiter häufen und welche Gegenmaßnahmen getroffen werden können.
https://www.dr-datenschutz.de/ransomware-angriffe-nehmen-zu-auf-den-ernstfall-vorbereiten/

Google reCaptcha und der Datenschutz
In diesem Beitrag geht es um Captchas und den Google reCaptcha insbesondere.
https://www.dr-datenschutz.de/google-recaptcha-und-der-datenschutz/

Da kommt was auf uns zu – die EU plant zahlreiche neue Datenschutzgesetze
Die DSGVO ist im fünften Jahr ihrer Gültigkeit. Nun will die EU nachlegen und hat einige ambitionierte Gesetzinitiativen aufgelegt.
https://www.althammer-kill.de/aktuelles/news/detail/da-kommt-was-auf-uns-zu-die-eu-plant-zahlreiche-neue-datenschutzgesetze