Spirit Legal / Neumarkt 16-18 / 04109 Leipzig / Germany

Empfänger: Landgericht Frankfurt am Main
Gerichtsstraße 2
60313 Frankfurt am Main

Übermittlung per beA

AZ: 22/725/PHE/CSC

Bearbeiter: Peter Hense

Ihr Zeichen:

Datum: 20.10.2022

Standort: Leipzig

Spirit Legal Fuhrmann Hense
Partnerschaft von Rechtsanwälten

Standort Leipzig:
Neumarkt 16-18
04109 Leipzig
Germany

Tel.: +49 (0) 341 / 39 29 78 90
Fax: +49 (0) 341 / 39 29 78 99

Standort Frankfurt am Main:
Bethmannstraße 58
60311 Frankfurt am Main
Germany

Tel.: +49 (0) 69 / 34 86 71 990
Fax: +49 (0) 69 / 34 86 71 999

Standort Dresden:
An der Herzogin Garten 1
01067 Dresden
Germany

Tel.: +49 (0) 351 / 21 78 88 00
Fax: +49 (0) 351 / 21 78 88 09

E-Mail: info@spiritlegal.com
Web: www.spiritlegal.com

AG Leipzig
Partnerschaftsregister No. 243

Klage

des **padeluun**, Marktstraße 18, 33602 Bielefeld

– Kläger –

Prozessbevollmächtigte: alle in Deutschland zugelassenen Rechtsanwälte der Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten, Neumarkt 16-18, 04109 Leipzig

g e g e n

die **DB Vertrieb GmbH**, DB Tower, Europa-Allee 78-84, 60486 Frankfurt am Main, vertreten d. d. Geschäftsführer:innen Georg Lauber, Nils Hartgen, Carmen Maria Parrino, Thomas Hermann

– Beklagte –

Wegen: Unterlassung der Verletzung von Persönlichkeitsrechten sowie der Grundrechte auf Datenschutz und Privatsphäre

Streitwert: EUR 7.500,00

Namens und in Vollmacht des Klägers erheben wir Klage und werden beantragen,

Der Beklagten wird bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR und für den Fall, dass dieses nicht beigetrieben werden kann, einer Ordnungshaft oder einer Ordnungshaft bis zu sechs Monaten, diese zu vollziehen an ihren gesetzlichen Vertretern,

<u>untersagt</u>,

ohne informierte Einwilligung des Klägers auf dessen Endeinrichtungen wie PC, Tablet, Laptop oder Telefon Cookies und ähnliche Technologien einzusetzen, insbesondere Identifikatoren auf seinen Endeinrichtungen zu speichern oder aus diesen Endeinrichtungen auszulesen, um das Verhalten des Klägers im Internet zu Zwecken der Werbung oder Marktforschung zu verfolgen bzw. verfolgen zu lassen,

wenn das geschieht, wie unter I.4. dieser Klageschrift dargestellt.

Inhaltsverzeichnis

Aus Gründen der Übersichtlichkeit stellen wir unseren Ausführungen ein Inhaltsverzeichnis voran:

I. Sachverhalt

1. Kläger

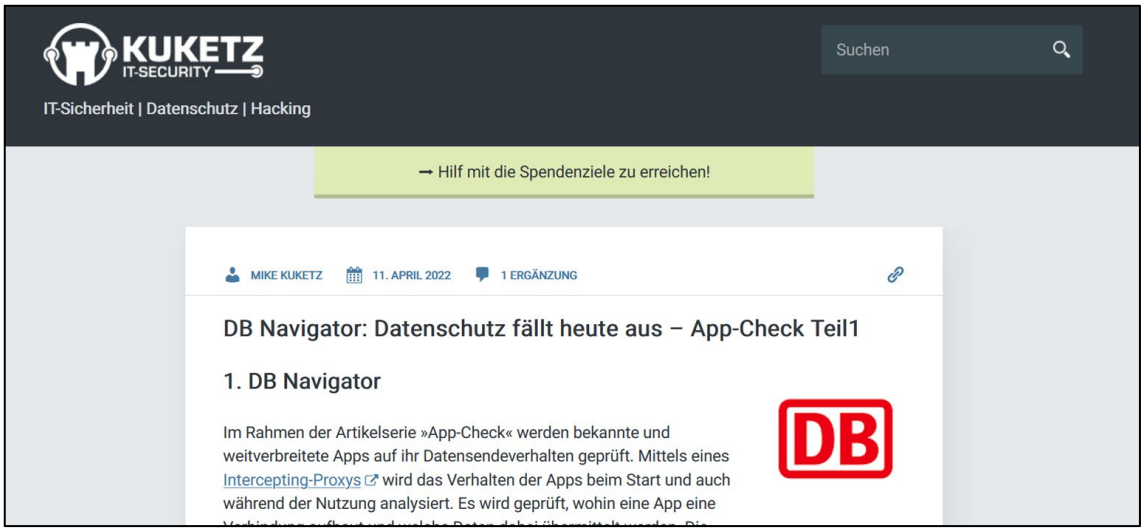
Der Kläger handelt seit 1976 unter seinem Pseudonym „padeluun“. Er ist ein bekannter deutscher Künstler und Netzaktivist, der für digitale Bürgerrechte eintritt und Sachverständiger in der Internet-Enquete-Kommission des Bundestags war. Er ist Mitbegründer und Vorsitzender des Grundrechte- und Datenschutzvereins Digitalcourage (vormals „FoeBuD“), seit Gründung aktiv im Arbeitskreis Vorratsdatenspeicherung und einer der Organisatoren sowie Jurymitglied der deutschen Big Brother Awards, die seit dem Jahr 2000 jährlich in Bielefeld verliehen werden.

2. Beklagte

Die DB Vertrieb GmbH mit Sitz in Frankfurt am Main ist eine hundertprozentige Tochter der Deutschen Bahn AG („DB“). Sie entstand 2005 aus der DB Personenverkehr GmbH. Die Beklagte ist Anbieterin der bekannten Website bahn.de sowie der nicht weniger bekannten App „DB Navigator“.

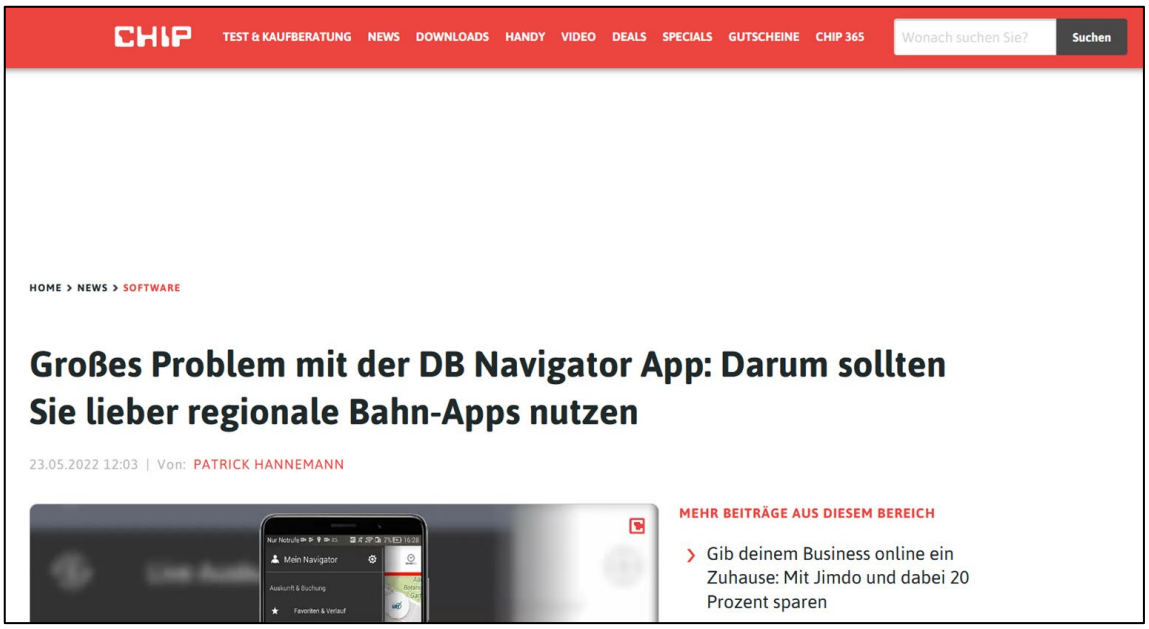
3. Vorgeschichte

Im April 2022 starteten der bekannte IT-Sicherheitsexperte Mike Kuketz und der Unterzeichner Untersuchungen bekannter Mobilgeräte-Apps in Bezug auf deren Datenverarbeitung in technischer und rechtlicher Hinsicht. Zum Auftakt der Prüfreihe „AppCheck“, deren Ergebnisse in Blogbeiträgen der Öffentlichkeit zugänglich gemacht wurden, stand die Prüfung des DB Navigators an. Unter dem Titel „DB Navigator: Datenschutz fällt heute aus“ fassten die Autoren zusammen, was an der derzeitigen Konfiguration der App der Beklagten technisch und rechtlich defizitär sei. Und das war und ist einiges. Der Beitrag kann jederzeit online im Blog von Herrn Kuketz unter www.kuketz-blog.de nachgelesen werden:

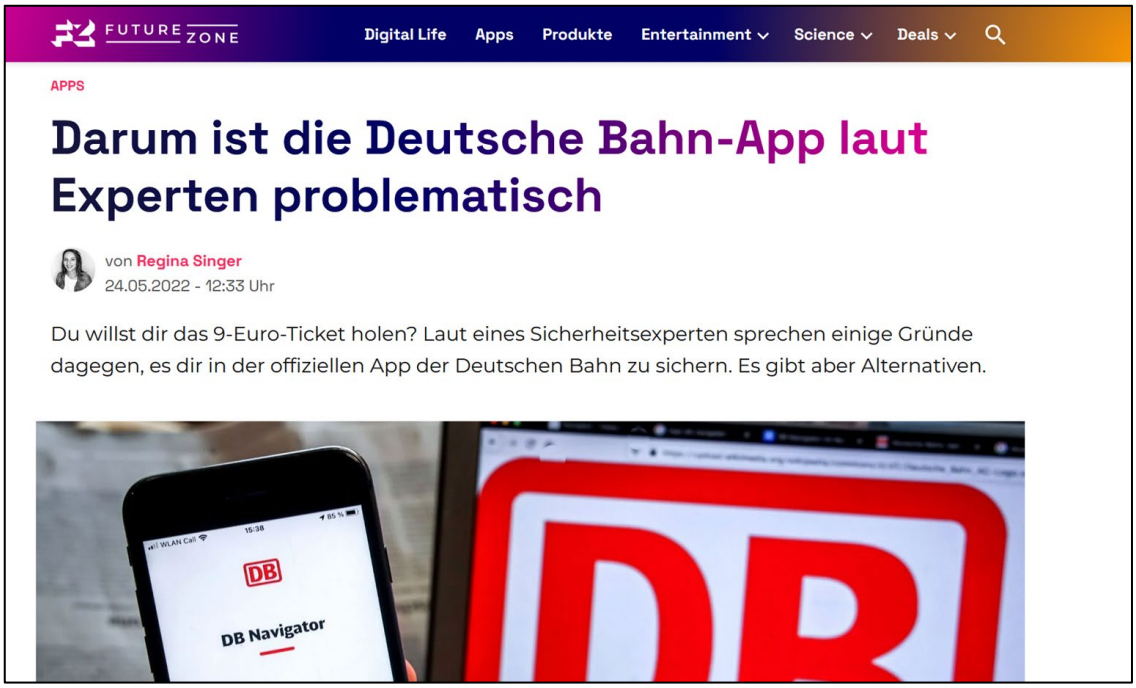


Quelle: https://www.kuketz-blog.de/db-navigator-datenschutz-faellt-heute-aus-app-check-teil1/

Der Beitrag schlug medial Wellen, da der Blog von Herrn Kuketz eine der meistgelesenen Quellen zum Thema IT-Sicherheit und Datenschutz in Deutschland ist:



Quelle: https://www.chip.de/news/Grosses-Problem-mit-der-DB-Navigator-App-Darum-sollten-Sie-lieber-regionale-Bahn-Apps-nutzen_184249733.html



Quelle: https://www.futurezone.de/apps/article329170/db-navigator-app-sicherheitsprobleme.html

Die Ergebnisse der Untersuchung wurden der Konzerndatenschutzbeauftragten der DB zur Kenntnis gebracht und es wurde der Pressestelle Gelegenheit zur Stellungnahme gegeben.

Deren Rückmeldung wurde am 14.4.2022 veröffentlich:

MIKE KUKETZ 14. APRIL 2022 | 09:47 UHR

Presserückmeldung der Deutschen Bahn (DB Navigator) eingegangen

Ich hatte bei der Deutschen Bahn um eine Stellungnahme bezüglich des rechtswidrigen Datensendeverhaltens der DB-Navigator-App gebeten. Die Antwort der Pressestelle ist wie folgt:

> Sehr geehrter Herr Kuketz,
>
> vielen Dank für Ihre umfangreiche Analyse. Wir nehmen Ihre Kritik und Ihre Hinweise sehr ernst und setzen uns damit auseinander. Als einer der größten Mobilitätsdienstleister in Deutschland ist es unser Anspruch und unsere Aufgabe, unseren Kund:innen eine qualitativ hochwertige und stets verfügbare App anzubieten. Alle in diesem Zusammenhang eingesetzten Dienstleister sind vertraglich gebunden, handeln nicht in eigenem Interesse und streng nach unserer Weisung. Sie sind deshalb nicht Dritte im Sinne der DSGVO.
> Wir haben den Consent-Layer der für uns zuständigen Datenschutzaufsichtsbehörde zur Bewertung vorgestellt. Bitte haben Sie Verständnis, dass wir die noch ausstehende Antwort selbst prüfen wollen. Sollten nach Ansicht der Aufsichtsbehörde Änderungen erforderlich sein, werden wir darüber transparent informieren.
>
> Eine Bitte: Wenn Sie mich zitieren möchten, dann bitte nicht namentlich, sondern als Sprecherin, o.ä.
>
> Viele Grüße
>
> XY

Ich möchte eigentlich nur kurz auf eine Aussage eingehen:

> Alle in diesem Zusammenhang eingesetzten Dienstleister sind vertraglich gebunden, handeln nicht in eigenem Interesse und streng nach unserer Weisung. Sie sind deshalb nicht Dritte im Sinne der DSGVO.

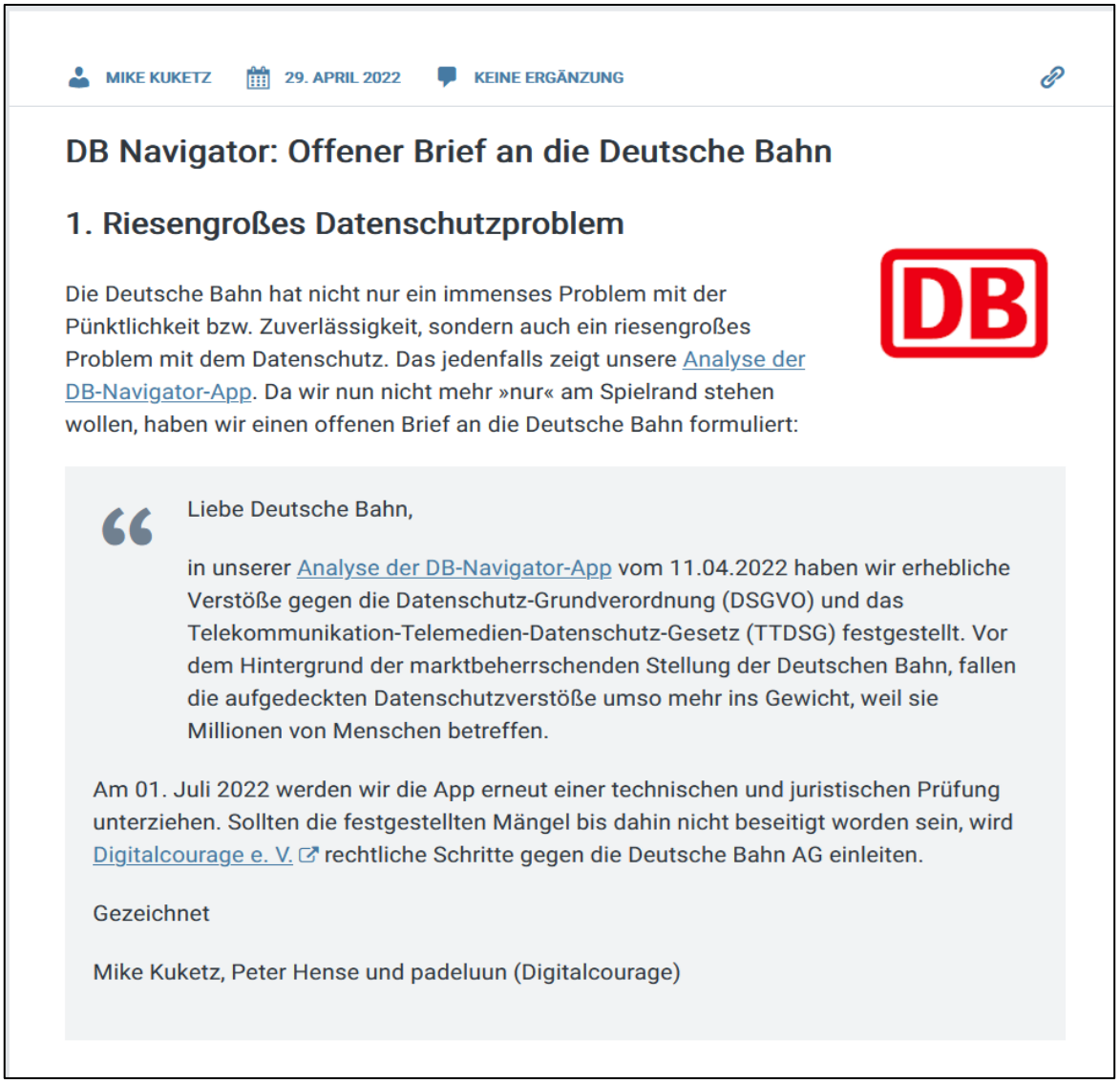
Das hat niemand bezweifelt. Dieses Derailing bzw. das Umlenken der Diskussion auf einen Sachverhalt, der so gar nicht beanstandet wurde, bringt uns in der Sache nicht weiter. Insgesamt will man sich also nicht zu den Rechtsverstößen äußern. Zur Kenntnis genommen.

Den Rest der Presserückmeldung lasse ich unkommentiert.

Quelle: https://www.kuketz-blog.de/presserueckmeldung-der-deutschen-bahn-db-navigator-eingegangen/

Durch die Berichterstattung wurde Digitalcourage e.V. auf den Sachverhalt aufmerksam und schloss sich der Bewertung durch die Autoren des Blogbeitrags an. Digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter.

Am 29.4.2022 wurde gemeinsam mit den Autoren des Beitrags ein knapper offener Brief an die Deutsche Bahn formuliert und eine Frist für Nachbesserungen in der App bis zum 1.7.2022 gesetzt:



MIKE KUKETZ 29. APRIL 2022 KEINE ERGÄNZUNG

DB Navigator: Offener Brief an die Deutsche Bahn

1. Riesengroßes Datenschutzproblem

Die Deutsche Bahn hat nicht nur ein immenses Problem mit der Pünktlichkeit bzw. Zuverlässigkeit, sondern auch ein riesengroßes Problem mit dem Datenschutz. Das jedenfalls zeigt unsere Analyse der DB-Navigator-App. Da wir nun nicht mehr »nur« am Spielrand stehen wollen, haben wir einen offenen Brief an die Deutsche Bahn formuliert:

> Liebe Deutsche Bahn,
>
> in unserer Analyse der DB-Navigator-App vom 11.04.2022 haben wir erhebliche Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) festgestellt. Vor dem Hintergrund der marktbeherrschenden Stellung der Deutschen Bahn, fallen die aufgedeckten Datenschutzverstöße umso mehr ins Gewicht, weil sie Millionen von Menschen betreffen.
>
> Am 01. Juli 2022 werden wir die App erneut einer technischen und juristischen Prüfung unterziehen. Sollten die festgestellten Mängel bis dahin nicht beseitigt worden sein, wird Digitalcourage e. V. rechtliche Schritte gegen die Deutsche Bahn AG einleiten.
>
> Gezeichnet
>
> Mike Kuketz, Peter Hense und padeluun (Digitalcourage)

2. Erfolgt eine Reaktion?

Wir geben der Deutschen Bahn also die Gelegenheit innerhalb der nächsten zwei Monate nachzubessern. Anfang Juli werden wir dann eine erneute Prüfung vornehmen. Sofern die festgestellten Mängel bis dahin nicht beseitigt wurden, wird Digitalcourage e. V. rechtliche Schritte einleiten.

Dieser Brief geht an folgende Adressaten:

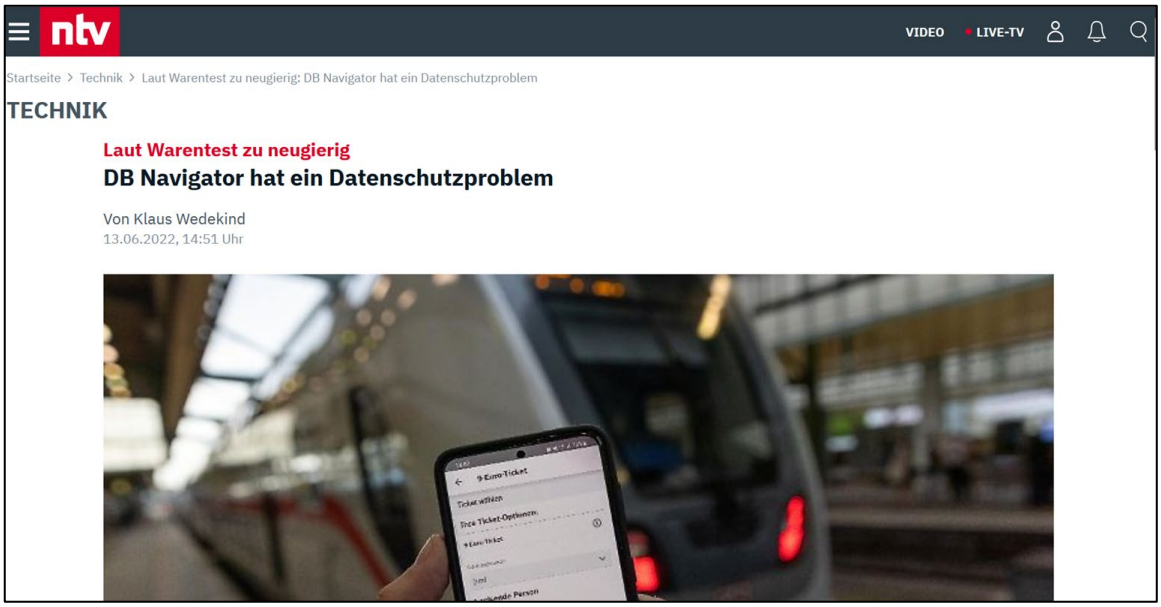
- Dr. Marein Müller, Konzerndatenschutzbeauftragte Deutsche Bahn AG: konzerndatenschutz@deutschebahn.com
- Verantwortliche Datenschutz, DB Vertrieb GmbH: p.d-datenschutz@deutschebahn.com
- Verantwortliche Datenschutz, DB Fernverkehr AG: fv-datenschutz@deutschebahn.com
- Verantwortliche Datenschutz, DB Regio AG: datenschutz.regio@deutschebahn.com
- Pressestelle der Deutschen Bahn: presse@deutschebahn.com
- Entwicklerteam DB Navigator: mobile@bahn.de

Quelle: https://www.kuketz-blog.de/db-navigator-offener-brief-an-die-deutsche-bahn/

Im Juni 2022 prüfte die Stiftung Warentest ihrerseits das Datensendeverhalten des DB Navigator und kam zu einem ähnlich kritischen Ergebnis:

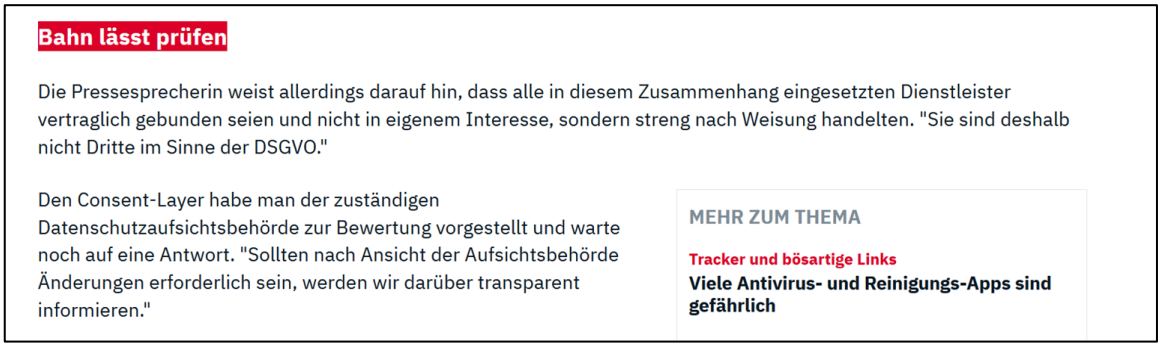
Quelle: https://www.test.de/Bahn-Apps-DB-Navigator-uebermittelt-mehr-Daten-als-noetig-5889807-0/

Das mediale Interesse hielt an, da nunmehr beide Untersuchungen voneinander unabhängig erhebliche Mängel bestätigten:



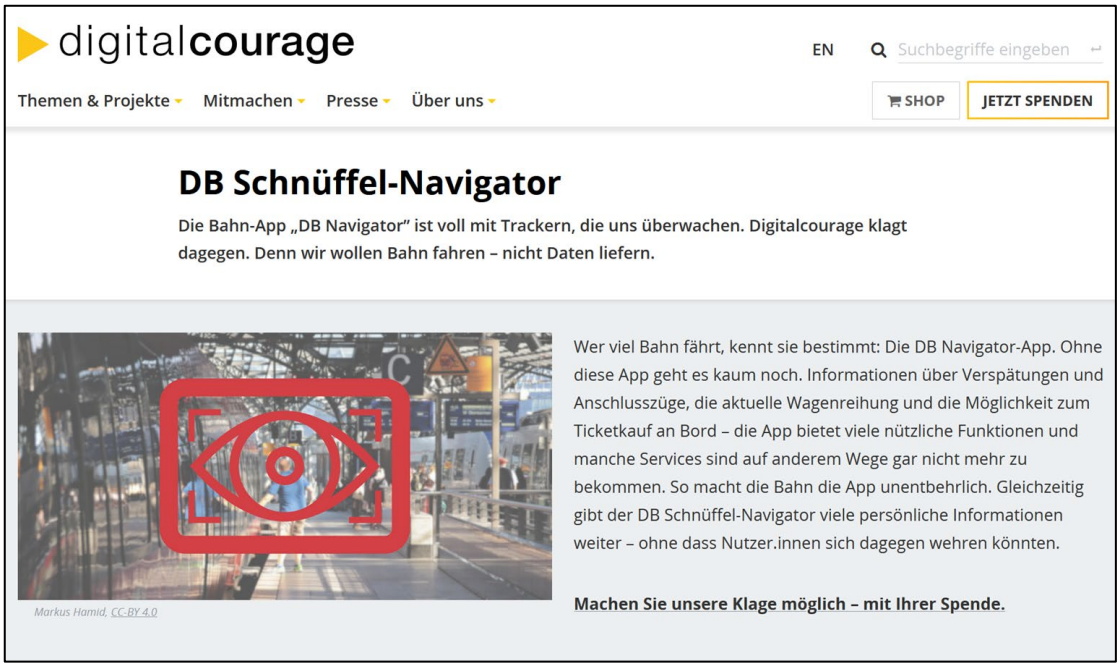
Quelle: https://www.n-tv.de/technik/DB-Navigator-hat-ein-Datenschutzproblem-article23394308.html

Gegenüber ntv ließ sich die Pressesprecherin der DB mit den folgenden Aussagen zitieren:



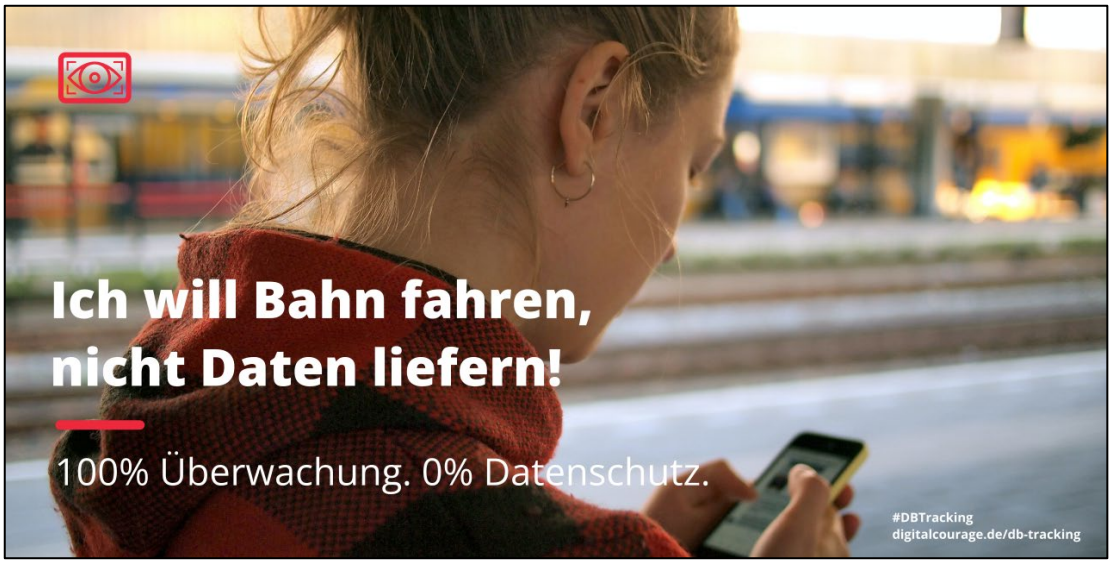
Quelle: https://www.n-tv.de/technik/DB-Navigator-hat-ein-Datenschutzproblem-article23394308.html

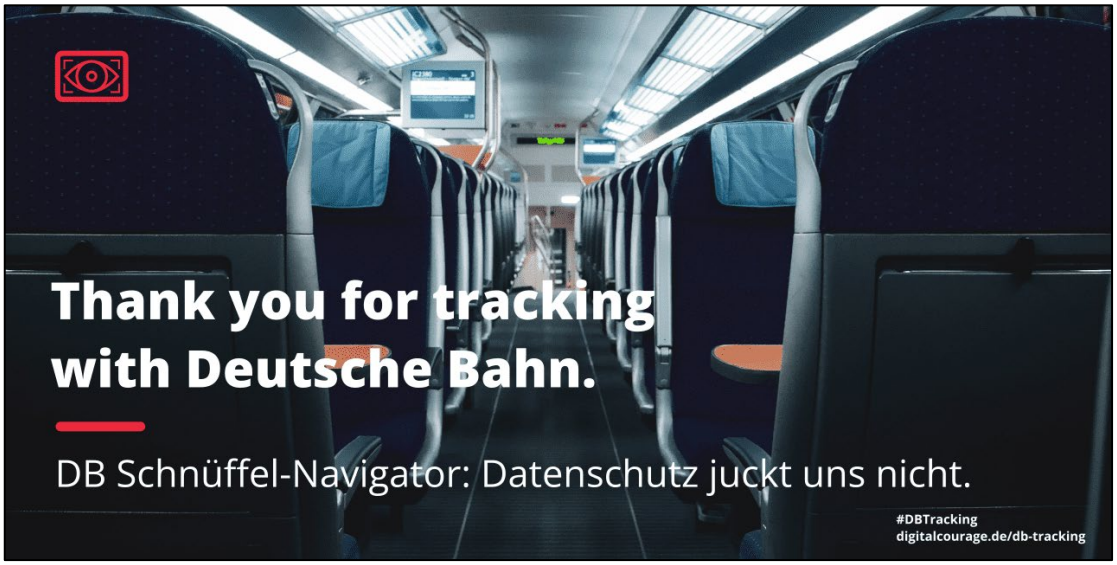
Am 20.7.2022 und damit deutlich nach Ablauf der für ein Umschwenken in Richtung rechtskonformer Datenverarbeitung gesetzten Frist machte Digitalcourage e.V. öffentlich, dass eine Klage gegen die als übergriffige „Datenschnüffelei“ des DB Navigator erhoben werde.



Quelle: https://digitalcourage.de/db-tracking

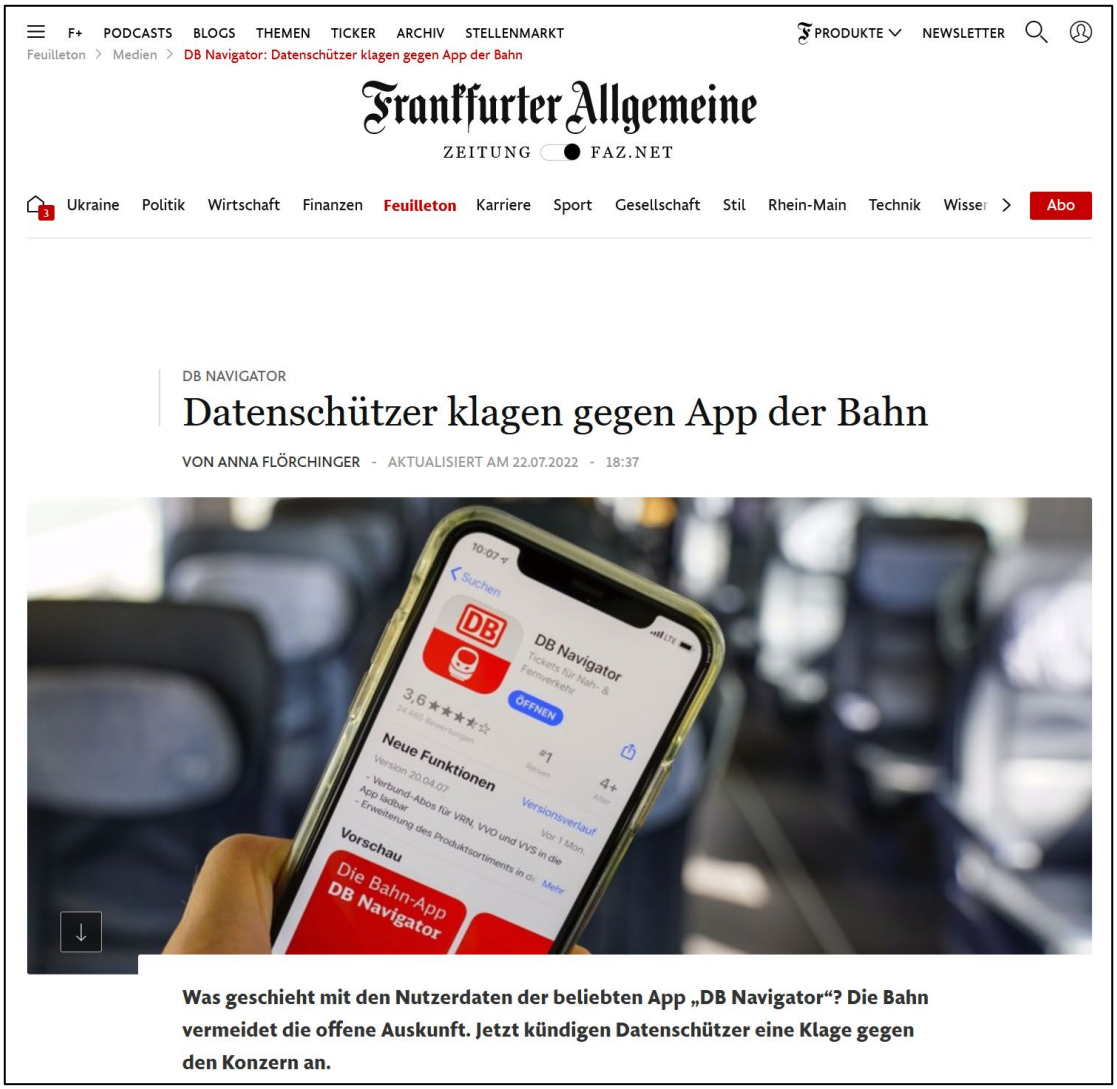
Digitalcourage e.V. ließ Worten Taten folgen und warb öffentlich um Verständnis und Unterstützung für das Anliegen, die DB zur Einhaltung datenschutzrechtlicher Vorgaben zu zwingen:





Quelle: https://digitalcourage.de/db-tracking

Das mediale und persönliche Interesse von Bahnfahrer:innen bestand ungebrochen fort:



F+ PODCASTS BLOGS THEMEN TICKER ARCHIV STELLENMARKT PRODUKTE NEWSLETTER

Feuilleton > Medien > DB Navigator: Datenschützer klagen gegen App der Bahn

Frankfurter Allgemeine
ZEITUNG FAZ.NET

Ukraine Politik Wirtschaft Finanzen Feuilleton Karriere Sport Gesellschaft Stil Rhein-Main Technik Wisser Abo

DB NAVIGATOR

Datenschützer klagen gegen App der Bahn

VON ANNA FLÖRCHINGER - AKTUALISIERT AM 22.07.2022 - 18:37

Was geschieht mit den Nutzerdaten der beliebten App „DB Navigator“? Die Bahn vermeidet die offene Auskunft. Jetzt kündigen Datenschützer eine Klage gegen den Konzern an.

Quelle: https://www.faz.net/aktuell/feuilleton/medien/db-navigator-datenschuetzer-klagen-gegen-app-der-bahn-18193268.html

Quelle: ZD-Aktuell 2022, 01288

Deutschlandweit verliehen mehrere tausend Personen ihrer Sorge um den Schutz ihrer Privatsphäre durch Unterstützerunterschriften und Spenden Ausdruck.

Am 26.7.2022 reagierte die DB öffentlich und erklärte die geäußerte Kritik in einer Pressemitteilung für „haltlos“:

Deutsche Bahn

Konzern | Presse | Investoren | Karriere | Digitalisierung | Nachhaltigkeit | Geschäfte

Startseite > Presse > Presseinformationen zentral > Deutsche Bahn: Kritik am DB Navigator haltlos

Deutsche Bahn: Kritik am DB Navigator haltlos

Kundendaten sind sicher • Cookies werden datenschutzkonform eingesetzt • DB in engem fachlichem Austausch mit Datenschutz-Expert:innen

Die DB weist die Kritik des Vereins Digitalcourage e.V. an ihrer App DB Navigator entschieden zurück. Bei der Nutzung des DB Navigator fließen keinerlei Kundendaten an Drittanbieter. Alle Dienstleister, mit der die DB beim DB Navigator zusammenarbeitet, sind vertraglich gebunden, handeln nicht in eigenem Interesse und streng nach Weisung der DB und sind deshalb nicht Dritte im Sinne der DSGVO.

Alle Technologieanbieter, die im DB Navigator in der Kategorie „erforderlich" aufgelistet sind, verarbeiten Daten ausschließlich zu den Zwecken, die vielfältigen Funktionen und die Stabilität der App für mehr als zwei Millionen Kunden täglich zu gewährleisten. Verarbeitet werden dabei keine identifizierenden personenbezogenen Informationen, sondern nur pseudonymisierte Daten, die sich für den einzelnen Anbieter isoliert als anonyme Dateninhalte darstellen. Keiner der Anbieter ist in der Lage, die Daten an anderer Stelle oder gar zu eigenen Marketingzwecken einzusetzen. Ein Webseiten- oder App-übergreifendes Nachverfolgen von Kund:innen mit diesen Cookies ist nicht möglich.

Die DB legt großen Wert auf die sparsame Erhebung und den sorgsamen Umgang mit den Daten ihrer Kund:innen. Eine Sprecherin: „Zu den von Digitalcourage e.V. im Internet veröffentlichten datenschutzrechtlichen Bedenken haben wir sehr detailliert Stellung genommen. Wir haben außerdem ein persönliches Gespräch zu einem fachlichen Austausch angeboten. Weder auf unsere fachlichen Ausführungen noch auf unser Gesprächsangebot hat der Verein Digitalcourage bis heute reagiert. Wir nehmen die jüngsten öffentlichkeitswirksamen Aktivitäten daher mit Befremden zur Kenntnis."

Die DB ist sich ihrer besonderen Verantwortung für die Daten ihrer Kund:innen, Mitarbeitenden und Geschäftspartner:innen bewusst. Die Datenschutzeinheit innerhalb der DB unterstützt die Geschäftsbereiche u.a. bei der Einhaltung der DSGVO. Um sicherzustellen, dass Systeme und Prozesse auch bei Neuerungen in der Gesetzgebung alle Anforderungen erfüllen, stehen die DB-Datenschützer:innen in engem Austausch mit den zuständigen Datenschutzbehörden und einem Kreis unabhängiger Expert:innen im DB-Datenschutzbeirat.

Kontakt

Dagmar Kaiser

Leiterin Konzernkommunikation Extern/Intern Kommunikation Personal und Recht
Deutsche Bahn AG

E-Mail

+49 (0) 30 297-61030

Downloads

Presseinformation als pdf (PDF | 143.8 KB)

https://www.deutschebahn.com/de/presse/pressestart_zentrales_uebersicht/Deutsche-Bahn-Kritik-am-DB-Navigator-haltlos--8200944?

Beweis: Blogbeitrag „Datenschutz fällt heute aus" sowie nachfolgende Medienberichte und Reaktionen in chronologischer Reihenfolge

vorgelegt **als Anlagenkonvolut K 1**

Im vorliegenden Verfahren soll am Beispiel des Ticketkaufs durch einen typischen Bahnkunden geklärt werden, ob die an der DB geäußerte Kritik tatsächlich „haltlos" ist oder aber die DB durch die Beklagte als Konzerntochter ungebremst Datenschutzrechte verletzt.

4. Verletzungshandlungen

Der Kläger ist, wie die meisten Deutschen, Kunde der DB und nutzt regelmäßig den DB Navigator der Beklagten, um Zugtickets zu buchen.

a. Aufruf des DB Navigators, Tracking bereits vor Interaktion des Klägers mit der App

Der Kläger öffnete am 7.9.2022 die App DB Navigator zur Buchung eines Zugtickets auf seinem Mobiltelefon („Endeinrichtung“). Unmittelbar nach dem Start und bevor eine Interaktion mit der Consent-Management-Lösung („CMP“=“Cookie-Banner“) der App erfolgen konnte, stellte die App mehrere Verbindungen zu Drittanbietern her, die auf die Endeinrichtung des Klägers zugreifen. Diese Zugriffe erfolgten ohne Einwilligung des Klägers. Dabei erfolgte ein Verbindungsaufbau zu folgendem externen Anbieter von zur Analyse und Tracking von Nutzerverhalten, nämlich der Adobe, Inc. (USA).

Die App baut eine Verbindung mit der Domain *assets.adobedtm.com* auf (DTM steht für „Dynamic Tag Management“), die von der zu Adobe Inc., einem Unternehmen aus den USA betrieben wird. Adobe bietet Marketing-Lösungen für Großunternehmen anbietet. Bereits dieser Endeinrichtungszugriff der Beklagten erfolgt zu Trackingzwecken, wie die Dokumentation von Adobe, Inc. belegt:

Integrieren mit Adobe Dynamic Tag Management

Integrieren Sie Adobe Dynamic Tag Management mit AEM, sodass Sie Ihre Dynamic Tag Management-Webeigenschaften für das Tracking von AEM Sites verwenden können. Dynamic Tag Management ermöglicht Marketingexperten die Verwaltung von Tags für die Datensammlung und die Verteilung von Daten auf Systeme für Digital Marketing. Verwenden Sie Dynamic Tag Management zum Beispiel für die Erfassung der Nutzungsdaten zu Ihrer AEM-Website und die Verteilung der Daten für die Analyse in Adobe Analytics oder Adobe Target.

Vor der Integration müssen Sie die Dynamic Tag Management-Webeigenschaft erstellen, die für das Tracking der Domäne Ihrer AEM-Site zuständig ist. Die Hosting-Optionen der Webeigenschaft konfiguriert werden, damit Sie AEM für den Zugriff auf die Dynamic Tag Management-Bibliotheken konfigurieren können.

Quelle: https://experienceleague.adobe.com/docs/experience-manager-65/administering/integration/dtm.html?lang=de

Zudem erfolgt ein Verbindungsaufbau mit der Domain *deutschebahn.sc.omtrdc.net*. Der Domainbestandteil „omtr“ steht für „Omniture“, ein Unternehmen für Webanalyse, das 2009 von Adobe erworben wurde und dessen Domainname bis heute weitergenutzt wird. Der Domainnamensbestandteil „dc“ steht wohl für „Discover“, ein früheres Tracking-Tool von Omniture:

Metrics

Metrics are the specific data that you can display in the columns of your report. Standard metrics include:

- **Traffic metrics**: Show data about the volume of visitors to your Web site.
- **Conversion metrics**: Show data about success events on your Web site. Success events may include purchases, downloads, or any other action that you want users to take on your Web site.
- **Calculated metrics**: Customizable metrics created by combining other metrics. For example, you could create a metric that subtracts the keyword cost and the cost of goods from the revenue to get net revenue. You could then divide this by the total number of orders to get average net revenue per order.

For more information, see "Working with Metrics" on page 69.

Comparisons

Comparisons let you put information about multiple segments in a side-by-side format so you can compare and contrast differences for multiple segments of visitors. Like segments and metrics, Discover provides you with a tool that lets you create your own comparisons for use in your reports.

For more information, see "Running Comparison Reports" on page 16.

Visualization Reports

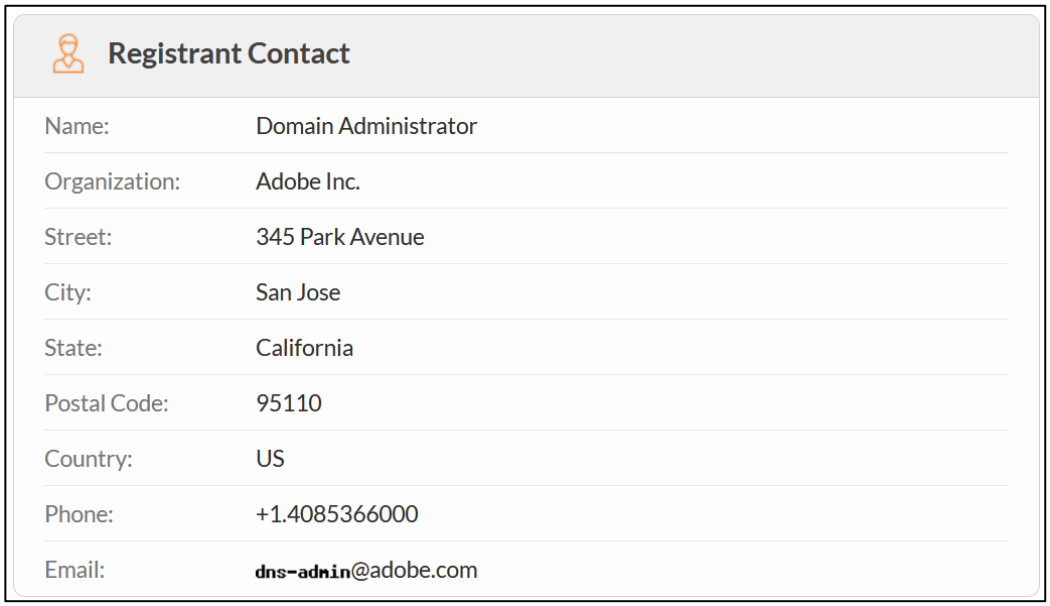
In addition to the reports that show you chart and table information, Discover offers a variety of specialized visualization reports that let you look at your Web site data from different perspectives. Some of these include:

- **Fallout Reports**: Show how many of your visitors progressed through your Web site to the destination you want.
- **Page Flow Reports**: Show which pages were most frequently visited before and after a designated page.
- **Site Analysis Report**: Graphically displays traffic and revenue patterns for your entire Web site.
- **Virtual Focus Group Report**: Graphically recreates Web site visits for visitors toy your Web site, including time spent on page and other data

For more information, see "Running Visualization Reports" on page 57.

Quelle: Auszüge aus dem Benutzerhandbuch von Omniture Discover (2009)

Die Domain *omntrdc.net* gehört ebenfalls zur Adobe Inc.:



Registrant Contact

Name:	Domain Administrator
Organization:	Adobe Inc.
Street:	345 Park Avenue
City:	San Jose
State:	California
Postal Code:	95110
Country:	US
Phone:	+1.4085366000
Email:	dns-admin@adobe.com

Quelle: https://www.whois.com/whois/omtrdc.net

Das Präfix „*deutschebahn.*“ ist eine Subdomain, die von Adobe für die Beklagte konfiguriert wurde.

Diese Domain gehört zur „Adobe Marketing Cloud“ und erhält in der Standardkonfiguration Tracking- und Analysedaten über die Nutzer der Endeinrichtung (Smartphone, PC etc.), die diese Verbindung initiiert hat.

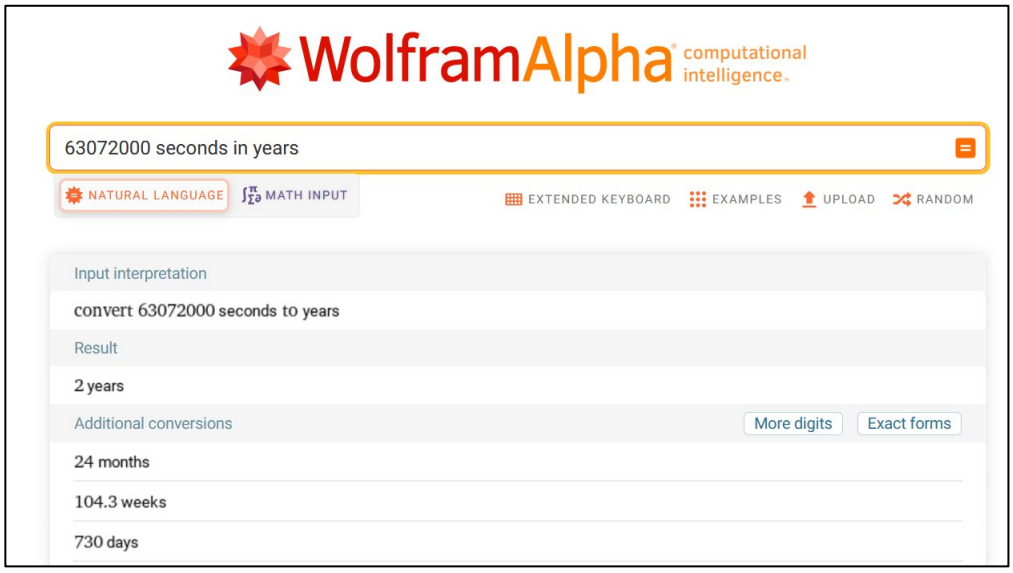
Von dem angefragten Server wurde dem Kläger eine eindeutige Kennziffer von der Beklagten („ID“) zugewiesen. Diese ID hat den nachfolgenden Wert:

{"id":"318C3854E4E79F75-60001C92355D2B6D"}

Darüber hinaus wurde aufgrund des Verbindungsaufbaus ein Cookie auf dem Endgerät des Klägers gesetzt, das die folgenden Werte enthält und zur Identifikation und Wiedererkennung des Klägers genutzt wird:

set-cookie: s_vi=[CS]v1|318C3854E4E79F75-60001C92355D2B6D[CE]; Path=/; Domain=omtrdc.net; Max-Age=63072000; Expires=Fri, 06 Sep 2024 10:21:21 GMT; SameSite=None; Secure

Dieses Cookie und damit der dem Kläger zugewiesene Identifikator haben eine Laufzeit von 24 Monaten, was sich aus dem „max-age“-Wert von 63072000 ergibt, der in Sekunden angegeben wird:



Quelle: https://www.wolframalpha.com

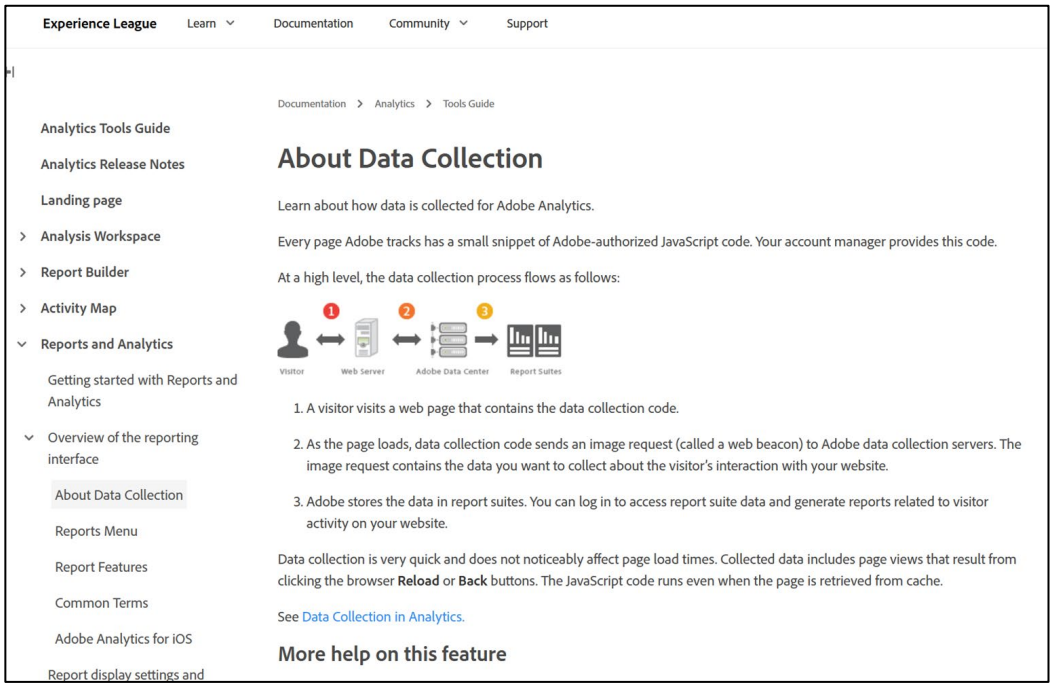
Der Kläger ist über dieses Cookie für die Beklagte und deren Dienstleister über einen Zeitraum von zwei Jahren wiedererkennbar.

Die Beklagte selbst formuliert es in ihren Datenschutzhinweisen wie folgt:

Einsatz von Adobe Analytics

Um unsere Website zu steuern und die Performance optimieren zu können, nutzen wir den Webanalysedienst der Adobe Systems Software Ireland Limited (Adobe Systems Software Ireland Limited, 4-6 Riverwalk, Citywest Business Campus, Dublin 24, Republic of Ireland). Die verwendeten Cookies haben eine Laufzeit von 24 Monaten. Die mittels des Cookies verarbeiteten Informationen sind nicht personenbezogen oder auf eine Person zurückzuführen. Mithilfe dieser Informationen messen und bewerten wir die Nutzung der Website und erstellen Statistiken. Auf diese Weise können wir sehen, welche Rubriken und Texte auf unserer App wie oft gelesen und genutzt werden und ob die Gestaltung unserer App einen Einfluss auf den Umfang der Nutzung hat. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten.

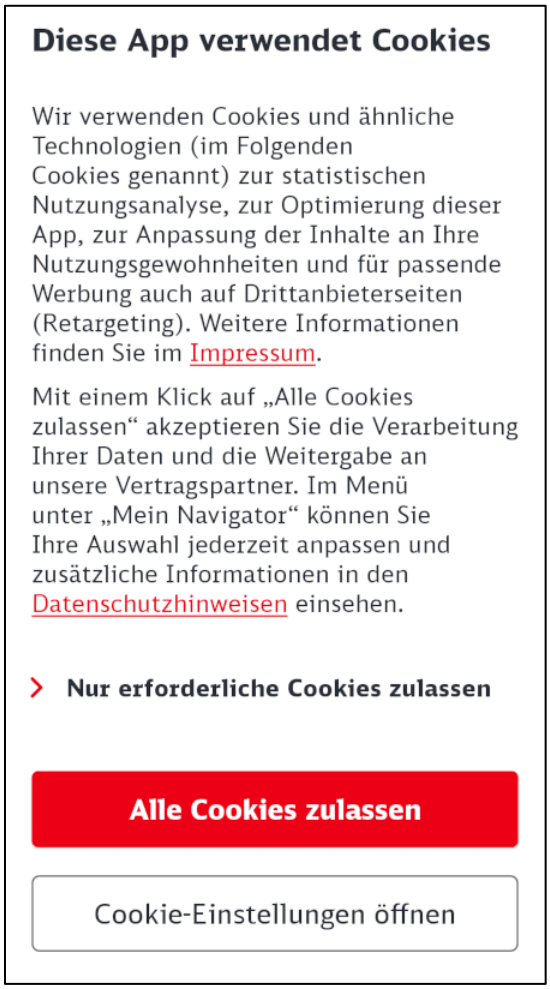
Adobe wiederum beschreibt die Funktionsweise des eigenen Trackings detaillierter:



Quelle: https://experienceleague.adobe.com/docs/analytics/analyze/reports-analytics/reporting-interface/overview-data-collection.html?lang=en

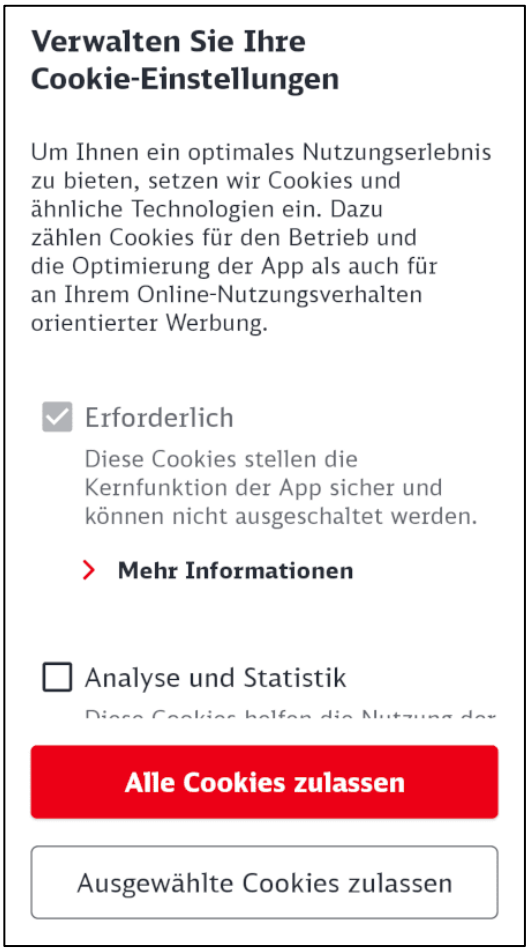
b. Anmeldung des Klägers mittels Bahn-Login und Buchung einer Fahrkarte, Tracking während des Buchungsvorgangs

Nach Aufruf der App erscheint ein „Cookie-Banner“, mithilfe dessen die Beklagte ihre Kunden, darunter den Kläger, zur Abgabe von Willenserklärungen, hier Einwilligungen, zwingen will.



Obwohl gegenüber der Globaleinwilligungsoption „Alle Cookies zulassen“ vom Design in den Hintergrund gerückt, hatte der der Kläger sich der aufdringlichen Gestaltung entzogen und die aus Sicht eines durchschnittlich informierten Verbrauchers objektiv am wenigsten datenschutzschädliche Option *„Nur erforderliche Cookies zulassen“* gewählt. Dass es sich hierbei um keine echte Wahlmöglichkeit handelt, sondern bestenfalls um einen erzwungenen Klick auf eine von mehreren schlechten Alternativen, liegt auf der Hand. Ob der Nutzer „zulässt“ oder nicht, spielt technisch keine Rolle, da er ja bereits vor seiner „Auswahl“, wie gezeigt, getrackt wird.

Was sich hinter „erforderliche Cookies“ verbirgt und was „erforderlich“ in der Sprache der Deutschen Bahn überhaupt bedeuten soll, bleibt dem Nutzer verborgen. Auch der ausgegraute Text, welcher über die „Cookie-Einstellungen“ erreichbar ist, birgt wenig Aufklärungspotenzial:



Entscheidend ist dabei offenbar die Information, dass „erforderliche Cookies“ angeblich *„nicht ausgeschaltet“* werden können, was zumindest aus Nutzerperspektive zutrifft.

Was die Beklagte aber jenseits des bereits dargestellten Trackings durch Adobe, Inc unter „erforderlichen Cookies“ versteht, legt eine Analyse des Netzwerkverkehrs der App (teilweise) offen.

(1) Tracking durch Optimizely, Inc

Bei der durch den Kläger erfolgten Anmeldung mit seinen Login-Daten zur Buchung einer Fahrkarte und ohne, dass der Kläger dem Tracking durch die Beklagte zugestimmt hätte, wurde eine Serveranfrage an *accounts.bahn.de* initiiert und dabei dem Kläger eine „EndUserID“ zugewiesen und in einem Cookie auf der Endeinrichtung des Klägers gespeichert. Der im Cookie gespeicherte Identifikator hat den Wert:

optimizelyEndUserId=27347A95-8958-4FB5-A84F-E97DA9F1158E

Bei dieser „EndUserID“ handelt es sich um einen Nutzerkennung, mit deren Hilfe ein

Dienstleister der Beklagten (Optimizely, Inc., USA) den Kläger im Verlauf der Benutzung der App wiedererkennen und analysieren kann. Dies geschieht durch Optimizely in dem Moment, in dem der Nutzer die Benutzung der App aufnimmt um, wie der Kläger, eine Fahrplanauskunft abzufragen oder eine Fahrkarte zu buchen. Dabei nimmt der DB Navigator Kontakt zu der Domain *logx.optimizely.com* auf und von dieser Domain aus wird der Cookie dann zu Identifikationszwecken immer wieder ausgelesen, um so die zeitgenauen Details der Nutzung mit dem Profil des Nutzers hinter der „EndUserID“ zu verknüpfen.

Die Beklagte selbst formuliert es in ihren Datenschutzhinweisen wie folgt:

Einsatz von Optimizely

Um Ihnen unsere App mit leicht variierten Inhalten anzeigen zu können, führen wir ein sog. A/B-Testing mithilfe des Webanalysedienstes 'Optimizely' durch. Hierfür werden Cookies auf Ihrem Endgerät mit einer Laufzeit von 24 Monaten gespeichert. Betreiber des Dienstes ist Optimizely (631 Howard Street, Suite 100, San Francisco, CA 94105, United States). Die anonymisierten Daten werden in der Regel auf einem Server von Optimizely in den USA verarbeitet.

Was „A/B-Testing“ bedeutet, bleibt dem Durchschnittsbahnkunden verborgen. Die Angaben in den Datenschutzinformationen der Beklagten schweigen sich über die Funktionsweise von „A/B-Testing“ aus. Nutzer wie der Kläger sind daher auf eigene Recherchen auf der Websit von Optimizely, Inc angewiesen, um zu verstehen, was mit ihren Daten geschieht:

A/B-Test für mobile Apps

Was ist A/B-Testing für mobile Apps?

Beim A/B-Testing für mobile Apps bedient man sich der Methode des A/B-Testings, um Variationen innerhalb einer App zu testen. Dabei werden die Nutzer einer App nach dem Zufallsprinzip in verschiedene Segmente der App umgeleitet, die sich alle unterschiedlich darstellen. Nachdem genügend Nutzer das Experiment durchlaufen haben, kann man den statistisch belegten Beweis antreten, welche Version der App höhere Conversion Rates erzielt.

So könnte z. B. ein App-Entwickler ein mobiles Spiel anbieten, das Extra-Level als In-App-Käufe anbietet. Er könnte nun verschiedene Banner testen wollen, mit denen er diese In-App-Käufe bewirbt, um herauszufinden, welches dieser Banner am häufigsten angeklickt wird.

Genau dies kann er anhand eines A/B-Tests mit seinen tatsächlichen Nutzern herausfinden. Nachdem der Test statistische Signifikanz erreicht hat, kann die als beste Variation ermittelte Version in die App integriert und in der Folge allen Nutzern angezeigt werden, was sich positiv auf die Conversion Rate auswirken wird.

Quelle: https://www.optimizely.com/de/optimization-glossary/mobile-app-ab-testing/

https://support.optimizely.com/hc/en-us/articles/4410288998797-Experiment-Types-AB-Multivariate-and-Multi-page

Optimizely, Inc ermöglicht es Anbietern von Apps und Websites, das Nutzungsverhalten von Kunden auszuwerten und das eigene Marketing zu optimieren.

Die Formulierung *„die anonymisierten Daten werden in der Regel auf einem Server von Optimizely in den USA verarbeitet“* in den abgebildeten Datenschutzhinweisen der Beklagten muss man dabei nicht zu ernst nehmen. Es handelt sich, wie anhand der „EndUserID“ gezeigt, nicht um anonyme Daten im Sinne des europäischen Datenschutzrechts, also Daten, die keinen Personenbezug aufweisen. Vielmehr scheint der Beklagten ein bedauerlicher Kopierfehler unterlaufen zu sein, als sie in Eile einige Angaben aus den Marketingunterlagen von Optimizely, Inc übernehmen wollte. Eigentlich wollte die Beklagte wohl formulieren: „nicht anonymisierte Daten“, wie es der Sach- und Rechtslage entspräche.

(2) Tracking durch Google Crashlytics

Unmittelbar nach Auswahl der Option „Nur erforderliche Cookies zulassen“ kommt ein weiterer Beteiligter ins Spiel. Die Beklagte hat zu „Analysezwecken“ auch einen Google-Service namens „Crashlytics“, dem Namen nach ein Kompositum aus „Crash“ und „Analytics“, beauftragt. Dieses „Crashlytics“ ist ein Analysedienst von Google für

Apps und soll dazu dienen, nicht näher definierte Analysen bereitzustellen, wenn eine App nicht mehr funktioniert („crasht“). Wer „Crashlytics“ in seine App integriert, gibt damit Zugriff auf alle Daten, die in der App verarbeitet werden, darunter auch sensible Informationen. Insbesondere sammelt Google als Anbieter von „Crashlytics“ detaillierte Informationen zum Gerät, zu der App-Version, die installiert ist, sowie andere Informationen, vor allem in Bezug auf die Soft- und Hardware des Nutzers. Da Crashlytics wenig bis nichts kostet, muss der Service sich für Google auf andere Weise refinanzieren. Zu diesem Zweck fragt Google bei Nutzung von Crashlytics automatisch über die Domain *firebase-settings.crashlytics.com* die Google Crashlytics „Installations-ID“ ab, im Falle des Klägers lautet diese eindeutige Kennung

(d8c07fab5d174eb386da237b4c5e378b).

Zusätzlich abgefragt wird die „APP-ID“ zur Identifikation der installierten App und damit insgesamt hochgradig personenbezogene Identifikatoren, die aus unterschiedlichen Gründen auf dem Gerät gespeichert sein können. Diese identifizierenden Endeinrichtungszugriffe bieten keinen Mehrwert für die Analyse des Absturzverhaltens einer App für Unternehmen wie die Beklagte, wohl aber einen Mehrwert für Google, die auf diesem Wege personenscharf und detailliert über die App-Nutzung durch Bahnkunden wie den Kläger informiert werden.

Auch hier sind der Beklagten beim Abfassen der gesetzlichen Pflichtinformationen ein paar unbeabsichtigte Fehler unterlaufen. Denn hätten die an Google übermittelten Daten tatsächlich *„keinen personenbezogenen Kontext“*, müsste sie mangels Anwendbarkeit der DSGVO weder in den Datenschutzhinweisen mit dem Satz *„Mit diesem Hinweis informieren wir Sie darüber, welche Daten wir von Ihnen erheben“* über diese informieren, noch eine Rechtsgrundlage für die Verarbeitung personenbezogener (!) Daten nach DSGVO angeben. Dass die Beklagte es dennoch tut, zeugt von einem materiellen Problembewusstsein bei zugleich leichten Mängeln in der B-Note aufgrund der widersprüchlichen Angaben gegenüber Nutzern wie dem Kläger:

> **Einsatz von Firebase Crashlytics (nur im DB Navigator für Android)**
>
> In unserer App wird Firebase Crashlytics, ein Dienst der Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA), eingesetzt. Mit Hilfe dieses Werkzeugs werden uns Informationen im Fall eines App-Absturzes anonymisiert übertragen, um die Ursache des jeweiligen Absturzes nachvollziehen und schneller beheben zu können. Die übertragenen Daten sind rein technischer Ausprägung und besitzen keinen personenbezogenen Kontext. Rechtsgrundlage hierfür ist Art. 6 Abs. 1 lit. f) DSGVO.

Die beschriebenen Verarbeitungen personenbezogener Daten des Klägers dürften unstreitig sein. Die Beklagte berühmt sich zumindest in ihren Datenschutzhinweisen, wenngleich nicht in demselben Detailgrad, diese Verarbeitungen vorzunehmen.

Für die Details der Verarbeitung sowie die Rechtmäßigkeit dieser ist die Beklagte aufgrund der gesetzlichen Regelung in Art. 5 Abs. 2 DSGVO vollständig darlegungs- und beweisbelastet (siehe sogleich unter II.2.).

II. Rechtliche Würdigung

1. Zuständigkeit

Das Landgericht Frankfurt am Main ist örtlich und sachlich zuständig, §§ 17, 32 ZPO.

2. Beweislast

Da der Kläger keinerlei Einblick in die Verarbeitungsprozesse der Beklagten hat, trägt die Beklagte die volle Beweislast für die Einhaltung der Vorschriften der DSGVO.

Diese Beweislastverteilung ist in der DSGVO in Art. 5 Abs. 2 geregelt und wurde erst kürzlich vom Europäischen Gerichtshof und direkt im Anschluss vom deutschen Bundesverwaltungsgericht (BVerwG) bestätigt. Der EuGH hat mit Urteil vom 24.02.2022 (C-175/20 – Valsts ieņēmumu dienests = ZD 2022, 271 ff. klargestellt, dass die Beweislast für die Einhaltung der DSGVO vollständig beim Verantwortlichen liegt, hier also bei der Beklagten:

> *„(77) In diesem Zusammenhang ist darauf hinzuweisen, dass der für die Verarbeitung Verantwortliche nach dem in Art. 5 Abs. 2 der Verordnung 2016/679 verankerten Grundsatz der Rechenschaftspflicht nachweisen können muss, dass er die in Abs. 1 dieses Artikels festgelegten Grundsätze für die Verarbeitung personenbezogener Daten einhält.*
>
> *(…)*
>
> *(81) Wie sich oben aus Rn. 77 ergibt, obliegt die Beweislast insoweit der lettischen Steuerverwaltung.“*

Die Entscheidung des EuGH wurde bereits wenige Tage später in der höchstrichterlichen deutschen Rechtsprechung rezipiert, das Bundesverwaltungsgericht entschied (Urteil vom 02.03.2022, BVerwG 6 C 7.20, Rn. 50):

„Nach dieser Rechtsprechung enthält Art. 5 Abs. 2 DSGVO mithin eine Beweislastregelung für Streitigkeiten, in denen die Einhaltung der Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 DSGVO in Frage steht."

Auch im Schrifttum wurde das Urteil des EuGH begrüßt (Zerdick, EuZW 2022, 527, 533):

„Gleichzeitig bekräftigt der EuGH in zu begrüßender Weise, dass der in Art. 5 II DS-GVO neu verankerte und zentrale Grundsatz der datenschutzrechtlichen Rechenschaftspflicht des Verantwortlichen vollumfänglich für den öffentlichen Bereich gilt (Rn. 77). Die Rechenschaftspflicht geht insoweit einher mit einer Beweislast des Verantwortlichen (Rn. 81). Damit erteilt der EuGH einer im deutschen Schrifttum vertretenen „engen Auslegung" der Rechenschaftspflicht (s. zum Meinungsstand Jaspers/Schwartmann/Thüsing/Kugelmann, DS-GVO/BDSG/Herman, 2. Aufl. 2020, Art. 5 Rn. 80 mwN) eine klare Absage."

Die Entscheidung des EuGH bringt Klarheit für die Beweislast bei komplexen Sachverhalten vor Gericht (Hense, ZD 2022, 413, 414):

„Eine europarechtliche Beweislastumkehr ist „nihil sub sole novi", nichts Neues unter der Sonne des Prozessrechts und demnach auch kein Grund zur Aufregung, sondern ein freundlicher Appell an die Verantwortlichen komplexer Datenverarbeitungsvorgänge, ihre Dokumentation in den Griff zu bekommen, wenn sie nicht vor Gericht Schiffbruch erleiden wollen."

Demnach trägt die Beklagte die volle Beweislast für die Rechtmäßigkeit ihrer Datenverarbeitung, insbesondere für die ordnungsgemäße Konfiguration ihrer Systeme gemäß den Grundsätzen von Privacy by Design und Privacy by Default nach Art. 25 Abs. 1 und 2 DSGVO, was bedeutet, dass sie verpflichtet ist, vollständig anhand von Aufzeichnungen und Zeugenaussagen darzulegen, ob und inwieweit sie bereits in der Designphase der App die Einhaltung des Datenschutzgrundsatzes der Datenminimierung geachtet hat.

Denn auch das fordert der EuGH in C-175/20, Rn. 78:

„Folglich obliegt es der lettischen Steuerverwaltung, nachzuweisen, dass sie gemäß Art. 25 Abs. 2 dieser Verordnung versucht hat, die Menge der zu erhebenden personenbezogenen Daten so gering wie möglich zu halten."

Das OLG Stuttgart (Urteil vom 18.5.2021 – 12 U 296/20 = ZD 2022, 105, 106, Rn. 26) stellte bereits 2021 zutreffend fest:

„Wenn Art. 5 Abs. 2 DS-GVO als spezielles Datenschutzgesetz bestimmt, dass der (für die Datenerhebung) Verantwortliche für die Einhaltung der Rechtmäßigkeit der Datenerhebung (vgl. auch Art. 5 Abs. 1 DS-GVO) verantwortlich ist und dessen Einhaltung nachweisen können muss, ist nicht ersichtlich, dass diese Pflicht nicht auch ggü. dem von der DS-GVO geschützten Bürger gelten soll. Der Nachweis der Rechtmäßigkeit der Überwachung ist daher auch im Zivilprozess vom Bekl. zu erbringen […]"

In einem Verfahren über die Zulässigkeit von Tracking-Diensten stellte das LG Rostock (Urteil vom 15. September 2020 – 3 O 762/19, Volltext zitiert nach juris, dort Rn. 67) in Bezug auf die Beweislast in Bezug auf unzulässiges Werbetracking zutreffend fest, dass die Beklagte die Darlegungs- und Beweislast für rechtskonformes Verhalten trifft:

> *„Im Übrigen hat sie jedoch lediglich pauschal bestritten, dass eine websiteübergreifende Datenübertragung erfolgt. Das ist insoweit unzureichend, da die Beklagte die Darlegungs- und Beweislast dafür trifft, dass die Gestaltung der Website datenschutzrechtskonform ist, wie sich aus Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO ergibt (vgl. BeckOK DatenschutzR/Schantz, 32. Ed. 1.5.2020, DS-GVO Art. 5, Rn. 39 m.w.N.).*
>
> *Nachdem die vom Kläger konkret benannten Tracking-Technologien (vgl. Schriftsatz vom 04.06.2020, S. 7) nicht nur grundsätzlich in der Lage sind, sondern regelmäßig auch gerade dafür eingesetzt werden, personengebundene Daten zu erheben und an Drittanbieter zu übermitteln, müsste die Beklagte also konkret vortragen und darlegen, dass die genannten Cookies keine personenbezogenen Daten an andere Websites übermitteln. Dieser Darlegungs- und Beweislast ist sie nicht nachgekommen."*

Aufgrund des geschilderten datenverarbeitungsintensiven Verhaltens der App, welches nicht vom Himmel fällt, sondern von Menschen so programmiert und konfiguriert wurde, steht für den Kläger fest, dass die Beklagte offenlegen muss, was sie sich beim Design ihrer Verarbeitungsvorgänge gedacht hat und welchen Stellenwert die gesetzlichen Vorgaben hierbei gespielt haben.

3. Unterlassungsansprüche

Die Beklagte greift heimlich, ohne den Willen des Klägers oder eine sonstige gesetzliche Gestattung, auf dessen Endeinrichtung zu, um dort zunächst „Cookies" mit identifizierenden Kennungen zu speichern sowie später auf diese immer wieder zuzugreifen. Darüber hinaus übermittelt die Beklagte gespeicherten Identifikatoren an Dritte. Mit Hilfe dieser Cookies verfolgt die Beklagte den Kläger zumindest bei der Nutzung der App, und zwar

entweder selbst oder durch arbeitsteilige Einbindung von Dritten.

Dieses Verhalten ist rechtswidrig und begründet Unterlassungsansprüche des Klägers:

a. Unterlassungsanspruch aus § 823 Abs. 2 BGB, § 1004 Abs. 1 S. 2 analog i. V. m. § 25 TTDSG

Der Zugriff auf die Endeinrichtung des Klägers zur Speicherung und zum Auslesen von Cookies und den darin enthaltenen Identifikatoren verstößt gegen § 25 Abs. 1 S. 1 TTDSG („Schutz der Privatsphäre bei Endeinrichtungen"), da der Kläger nicht „auf der Grundlage von klaren und umfassenden Informationen" in diesen Zugriff eingewilligt hat und keine Ausnahme von der Einwilligungspflicht nach § 25 Abs. 2 TTDSG vorliegt.

Eine solche wäre nur gegeben, wenn sowohl die Speicherung der Cookies nebst IDs als auch das Auslesen dieser Identifikatoren „unbedingt erforderlich" gewesen wäre, „damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann" (Wortlaut von § 25 Abs. 2 Nr. 2 TTDSG).

Eine solche „unbedingte Erforderlichkeit" ist vorliegend nicht ersichtlich. Im Gegenteil, denn zur Vorgängervorschrift des § 15 Abs. 3 TMG entschied der BGH in der bekannten „Cookie-Einwilligung II"-Entscheidung (NJW 2020, 2540, Leitsatz 2):

> *„§ 15 III 1 TMG ist mit Blick auf Art. 5 III 1 der RL 2002/58/EG dahin richtlinienkonform auszulegen, dass der Diensteanbieter Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers einsetzen darf."*

Diese klare Rechtsprechung wurde von den Instanzgerichten bislang einhellig umgesetzt (vgl. LG Frankfurt, Urt. v. 19.10.2021 – 3-06 O 24/21 = MMR 2022, 152 f.), darunter auch im einstweiligen Rechtsschutz (LG Köln, Beschluss vom 29.10.2020 – 31 O 194/20 = MMR 2021, 437 f.; LG Köln, Beschluss vom 13.04.2021 – 31 O 36/21 = BeckRS 2021, 12261; mit Besprechung Herbrich, jurisPR-ITR 15/2021 Anm. 4) sowie LG Rostock (Urteil vom 15.9.2020 – 3 O 762/19 = ZD 2021, 166, redaktionelle Leitsätze Nr. 1 und 2):

> *„Werbetreibende dürfen keine Cookies für das Tracking von Nutzern zu Analyse- und Marketingzwecken verwenden, die personenbezogene Daten von Nutzern an Dritte übermitteln und die Nachverfolgung des Surf- und Nutzungsverhaltens ermöglichen, wenn keine Einwilligung für diese Datenverarbeitung vorliegt. […]*

Werden durch die Einbindung von Drittanbieter-Cookies (z.B. Google-Analytics-Cookies) personenbezogene Daten an Drittanbieter übertragen und von diesen (auch) für eigene Zwecke verarbeitet, liegt ein Fall gemeinsamer Verantwortung nach Art. Artikel 26 DS-GVO und keine bloße Auftragsverarbeitung gem. Art. 28 DS-GVO vor."

§ 25 Abs. 1 S. 1 TTDSG ist eine wortgetreue Umsetzung des europäischen Richtlinientextes in Art. 5 Abs. 3 S. 1 der ePrivacy-Richtlinie (2002/58/EG in der Form der Richtlinie 2009/136/EG), auf den der BGH im obigen Zitat referenziert (Taeger/Gabel/Ettig, 4. Aufl. 2022, TTDSG § 25 Rn. 10).

Die Vorschrift ist ein Schutzgesetz i. S. v. § 823 Abs. 2 BGB, da die Norm den Individualschutz bereits im Namen trägt, aber auch inhaltlich den Schutz der Privatsphäre von Endnutzern sicherstellt. Die Verletzung von § 25 Abs. 1 TTDSG stellt somit die Verletzung eines Schutzgesetzes dar, womit die haftungsbegründende Kausalität für § 823 Abs. 2 BGB erfüllt ist und der Unterlassungsanspruch nach § 1004 BGB analog eingreift.

b. Unterlassungsanspruch aus § 823 Abs. 1 BGB, § 1004 Abs. 1 S. 2 analog i. V. m. dem Allgemeinen Persönlichkeitsrecht (APR) in seiner Ausprägung der Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die in den Cookies enthaltenen eindeutigen Identifikatoren sind personenbezogene Daten, so wie auch die IP-Adresse einer Endeinrichtung ein personenbezogenes Datum darstellt (vgl. LG München, Endurteil vom 20.01.2022 – 3 O 17493/20 = GRUR-RS 2022, 612). Das Speichern und Auslesen dieser Cookie-IDs und anderer Identifikatoren zu werblichen Zwecken stellt demnach eine Verarbeitung personenbezogener Daten des Klägers dar.

Die Cookies sollen den Kläger bei der Nutzung seiner Endeinrichtung über einen längeren Zeitraum für die Beklagte und Dritte eindeutig identifizieren und wiedererkennen.

Bereits die heimliche Kennzeichnung des Klägers und seiner Endreinrichtung mit einem Identifikator (sog. „Hidden Identifiers", Erwägungsgrund 24 der RL 2002/58/EG), der jederzeit durch die Beklagte und deren Dienstleister, aber auch durch Dritte ausgelesen werden kann und ausgelesen wird, stellt eine Verarbeitung personenbezogener Daten dar, für die die Beklagte keine Rechtsgrundlage vorweisen kann.

Die von der Beklagten durchgeführte rechtswidrige Verarbeitung personenbezogener Daten verletzt Persönlichkeitsrechte des Klägers, namentlich dessen Allgemeines Persönlichkeitsrecht in der Ausprägung der verfassungsmäßigen Rechte auf informationelle Selbstbestimmung (BVerfGE 65, 1 ff.) sowie auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfGE 120, 274 ff.).

Das Allgemeine Persönlichkeitsrecht in seinen unterschiedlichen Ausprägungen ist ein sonstiges Recht i. S. v. § 823 Abs. 1 BGB. Seine Verletzung löst einen quasinegatorischen Unterlassungsanspruch nach § 1004 BGB aus (Grüneberg/Sprau, § 823 Rn. 132).

Das OLG Stuttgart stellt zutreffend fest (Urteil vom 18.5.2021 – 12 U 296/20 = ZD 2022, 105, Rn. 4 ff.)

> *„§ 1004 BGB ist bei der Verletzung absoluter und deliktisch geschützter Rechte, insb. auch aller nach § 823 Abs. 2 BGB geschützten Rechtsgüter, entsprechend anwendbar (vgl. nur Palandt/Herrler, BGB, 80. Aufl., § 1004 BGB Rn. 4 mwN). Das durch die Art. 1 und Art. 2 GG geschützte allgemeine Persönlichkeitsrecht wird bzgl. personenbezogener Daten durch das BDSG und seit 25.5.2018 ergänzt durch die DS-GVO geschützt (vgl. nur Palandt/Sprau, BGB, 80. Aufl., § 823 BGB Rn. 85 mwN).“*

Zuvor positionierte sich bereits das OLG Dresden (Beschluss vom 06.01.2021 – 4 U 1928/20 = BeckRS 2021, 3457):

> *„Das durch § 823 BGB unter anderem geschützte allgemeine Persönlichkeitsrecht beinhaltet auch das Recht auf Informationelle Selbstbestimmung. Dies bedeutet, dass der Betroffene die unbefugte Benutzung seiner persönlichen Daten nicht dulden muss (vgl. Palandt/Sprau, BGB, 80. Aufl., § 823 Rz. 115 m.w.N.). Die unrechtmäßige Verarbeitung personenbezogener Daten der Klägerin im Sinne des Art. 6 DSGVO stellt überdies die Verletzung eines Schutzgesetzes nach § 823 Abs. 2 BGB dar, die ebenfalls mit einem Unterlassungsanspruch nach § 1004 BGB geltend gemacht werden kann […]“*

Diese Rechtsauffassung bestätigt das OLG Dresden (Urteil vom 14.12.2021 – 4 U 1278/21 = ZD 2022, 235, Leitsatz 3):

> *„Neben Ansprüchen aus der DS-GVO bleibt die Durchsetzung von Unterlassungsansprüchen nach § 823, § 1004 BGB möglich.“*

c. Unterlassungsanspruch aus § 823 Abs. 2 BGB, § 1004 Abs. 1 S. 2 BGB analog i. V. m. Art. 6 DSGVO

Dem Kläger steht zudem ein Unterlassungsanspruch aufgrund der Verletzung von Art. 6 DSGVO („Rechtmäßigkeit der Verarbeitung") zu. Art. 6 Abs. 1 DSGVO statuiert ein präventives Verbot mit Erlaubnisvorbehalt für die Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO. Eine solche Rechtsgrundlage ist nicht ersichtlich, insbesondere hat die Beklagte für ihre Verarbeitung personenbezogener Daten wie der genannten Identifikatoren keine informierte Einwilligung des Klägers eingeholt, sondern diese Datenverarbeitung heimlich durchgeführt.

Das LG Hamburg (Urteil vom 13.2.2020 – 312 O 372/18 = ZD 2020, 477, Leitsatz 2) konstatiert kurz und knapp:

> *„Art. 6 DS-GVO stellt ein Schutzgesetz dar. Die Verletzung von Art. 6 DS-GVO begründet Unterlassungsansprüche nach §§ 823 Abs. 2, 1004 BGB."*

Das OLG München (Urteil vom 19.1.2021 – 18 U 7243/19 = GRUR-RS 2021, 11593, Rz. 28) bestätigt das Bestehen eines deliktischen Unterlassungsanspruchs bei Verletzung von Art. 6 DSGVO als Schutzgesetz:

> *„Dem Kläger stehen gegen die Beklagte Ansprüche auf Unterlassung der Veröffentlichung eines ihn betreffenden Profils im tenorierten Umfang nach § 823 Abs. 2, § 1004 Abs. 1 Satz 2 BGB analog in Verbindung mit Art. 6 Abs. 1 f) DSGVO zu."*

d. Unterlassungsanspruch aus Art. 17 DSGVO

Darüber hinaus ergibt sich ein Unterlassungsanspruch gegenüber der Verarbeitung personenbezogener Daten des Klägers auch aus Art. 17 DSGVO, da die Beklagte, wie gezeigt, personenbezogene Daten des Klägers in rechtswidriger Weise ohne Rechtsgrundlage verarbeitet (vgl. BGH NJW 2022, 1098, 1107).

e. Possessorischer Unterlassungsanspruch aus §§ 858 Abs. 1, 862 Abs. 1 BGB

Das Speichern von Cookies und anderen Identifikatoren zu Zwecken der heimlichen Profilbildung über die Nutzung der Endeinrichtung des Klägers stellt zudem eine Störung des Besitzes an dieser Endeinrichtung und damit verbotene Eigenmacht dar (§ 858 Abs. 1 BGB), weshalb dem Kläger ein Unterlassungsanspruch nach § 862 Abs. 1 zusteht.

Einerseits wird durch die „Verwanzung“ des Mobiltelefons des Klägers mithilfe von „Hidden Identifiers“ (Erwägungsgrund 24 der RL 2002/58/EG) rein technisch dauerhaft Speicherplatz auf der Endeinrichtung genutzt, darüber hinaus werden diese heimlich abgelegten Identifikatoren dazu verwendet, um das Verhalten des Klägers auszuwerten. In der fachlich einschlägigen Literatur ist anerkannt (Hoeren, DuD 1998, 455 f., „Web-Cookies und das römische Recht“, aufgrund der mangelnden Verfügbarkeit in digitalen Archiven hier als **Anlage K 2** beigefügt, sowie wiederum Hoeren, NJW 2008, 3099, 3100), dass eine Cookie-Speicherung ohne den Willen des Besitzers einer Endeinrichtung als Besitzstörung anzusehen ist.

Denn Besitzstörung ist jede Beeinträchtigung der Gebrauchs- und Nutzungsmöglichkeiten, die nicht vom Willen des Besitzers gedeckt und nicht gesetzlich gestattet ist. Entsprechend positioniert sich die Kommentarliteratur zum identischen Störerbegriff beim Eigentum (BeckOK BGB/Fritzsche, 61. Ed. 1.2.2022, BGB § 903 Rn. 24):

> *„Das Kopieren von Daten, die sich auf einem Trägermedium befinden, erfordert eine Einwirkung auf dieses Medium, egal auf welchem technischen Wege sie im konkreten Fall erfolgen mag, sodass eine abwehrfähige Benutzung anzunehmen ist;“*

Sowie daran anschließend zur Störung des Besitzes (BeckOK BGB/Fritzsche, 61. Ed. 1.2.2022, BGB § 858 Rn. 15):

> *„Was Einwirkungen auf Computer, Server oder Router angeht, so gilt: Das Speichern sog. Cookie durch den Betreiber einer Internetseite auf dem Endgerät eines Besuchers ohne dessen Einwilligung ähnelt zumindest wegen der Verringerung des Speicherplatzes einer Besitzstörung […]“*

Entscheidend für die Bewertung ist, dass sowohl Eigentümer als auch Besitzer einer Endeinrichtung durch heimliche technische Maßnahmen von der freien Nutzung ihrer Endeinrichtung ausgeschlossen werden, denn eine permanente Überwachung des Internetverkehrs und der besuchten Webseiten durch Cookies und andere Tracking-Technologien stellt eine erhebliche Beeinträchtigung dieser absoluten Rechte dar.

Dass die Installation von Programmcode, der eine heimliche (auch örtliche) Überwachung der Endeinrichtung eines Nutzers durch Dritte ermöglicht, eine Eigentumsstörung ist, hat zuletzt das OLG Dresden für die Installation einer Überwachungs-App auf einem Mobiltelefon festgestellt (Beschluss vom 15.06.2021 – 4 U 993/21 = GRUR-RS 2021, 19014, amtliche Leitsätze):

1) Ein Unterlassungsantrag, der den Download von Apps auf "sonstigen Endgeräten", eines Dritten begehrt, die diesem vom Unterlassungsgläubiger überlassen wurden, ist hinreichend bestimmt.

2) Die Installation von Programmen durch einen Dritten, die diesem erlauben, jederzeit auf den Positionsstandort eines Smartphones zuzugreifen, verletzt das Nutzungsrecht des Eigentümers.

3) Eine solche Tathandlung begründet die Wiederholungsgefahr kerngleicher Verletzungshandlungen auf weiteren Geräten, auf die der Verletzer Zugriff hat. Allein durch das Löschen der das Nutzungsrecht beeinträchtigenden Software kann diese Wiederholungsgefahr nicht beseitigt werden.

4. Wiederholungsgefahr

Der heimliche Zugriff auf die Endeinrichtungen des Klägers kann sich jederzeit wiederholen. Aufgrund der bekannten absoluten marktbeherrschenden Alleinstellung der Beklagten ist der Kläger gezwungen, den DB Navigator zu nutzen. Da infolge der Verletzungshandlungen bereits ein rechtswidriger Eingriff insbesondere in grundrechtlich geschützte Rechte des Klägers erfolgt ist, besteht eine tatsächliche Vermutung für das Vorliegen einer Wiederholungsgefahr.

5. Streitwert

Den Streitwert beziffert der Kläger mit EUR 7.500,00.

Dieser rechtfertigt sich

- aus dem Umfang der rechtswidrigen Verarbeitung personenbezogener Daten und
- der Intensität des Eingriffs in die Privatsphäre durch die Überwachung des Aufrufs von Websites sowie
- der Unausweichlichkeit der Nutzung des Angebots der Beklagten für den Kläger als Kunden der DB.

Die Übermittlung des Schriftsatzes erfolgt im elektronischen Rechtsverkehr und ausdrücklich im Namen der Kanzlei Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten. Aufgrund der elektronischen Übersendung per beA sind Abschriften nicht beigefügt (§ 133 Abs. 1 S. 2 ZPO). Für die rechtsgültige Unterschrift siehe Empfangs- und Signaturprotokoll Ihrer empfangenden Fernmeldeanlage.

Peter Hense
Rechtsanwalt

Anlagen:

Anlagenkonvolut K 1	Blogbeitrag „Datenschutz fällt heute aus“ sowie nachfolgende Medienberichte und Reaktionen in chronologischer Reihenfolge
Anlage K 2	Hoeren, DuD 1998, 455 f., *„Web-Cookies und das römische Recht“*