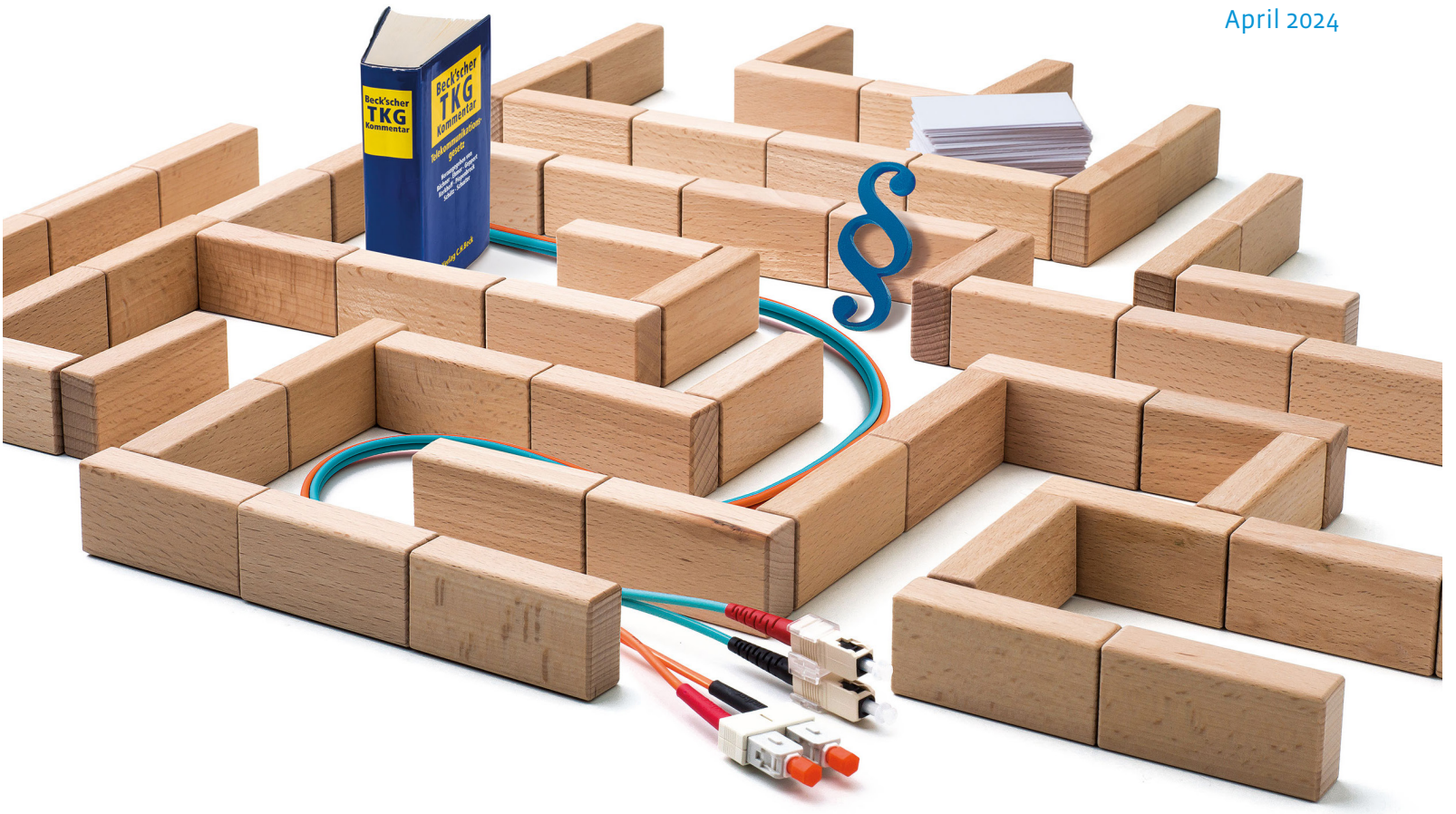
„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

DFN infobrief recht

4 / 2024
April 2024



Google Topics: Das Ende der nervigen Cookie-Banner?

Mit Topics will Google personalisierte Werbung ermöglichen und gleichzeitig den Datenschutz verbessern

Ich glaub, es hackt

EuGH-Urteil zu Haftungsrisiken infolge eines Hackerangriffs: Angst vor Datenmissbrauch als immaterieller Schaden

Die Bretonage der europäischen Datenstrategie

Lähmt das Cyber-Sicherheitsrecht die europäische Datenwirtschaft?

Kurzbeitrag: Wie gewonnen, so zerronnen

Abgelehnter Bewerber verlangt Schadensersatz nach Auskunftsbegehren

Google Topics: Das Ende der nervigen Cookie-Banner?

Mit Topics will Google personalisierte Werbung ermöglichen und gleichzeitig den Datenschutz verbessern

von Marc-Philipp Geiselmann

Um Cookie-Banner endlich loszuwerden, hat Google sich eine Alternative einfallen lassen. Mit Topics soll nun alles besser werden: Eine dezentrale Speicherung auf dem Endgerät ohne Weiterleitung an externe Server und eine nur drei Wochen lange Speicherung der Inhalte lassen aufhorchen und hoffen.

I. Einleitung

Wer im Internet surft, wird auf beinahe jeder Seite mit einem Cookie-Banner konfrontiert. Diese werden oft mit einem schnellen Klick auf „Alle Akzeptieren“ goutiert. Damit wird eine Einwilligung zum Setzen von Cookies (von Drittanbietern) erteilt.
Cookies werden zum Beispiel verwendet, um dem Kunden beim Einkaufen im Internet einen Warenkorb zur Verfügung zu stellen, sodass er mehrere Produkte auf einmal erwerben kann. Diese vom Betreiber selbst verwendeten Cookies werden als „Erstanbieter-Cookies“ bezeichnet. Werden die erhobenen Daten hingegen an einen Dritten weitergegeben, spricht man von „Drittanbieter-Cookies“. Die Weitergabe von Informationen über einen Nutzer durch mehrere Seitenbetreiber an einen Dritten ermöglicht es diesem, Nutzerprofile zu erstellen. Diese Nutzerprofile können sehr detaillierte Informationen über den Nutzer beinhalten und bilden daher das Rückgrat der Werbeindustrie für personalisierte Werbung. Wer seine Werbeanzeige an einen Nutzer ausspielen kann, von dem angenommen wird, dass er sich für das beworbene Produkt interessiert, ist bereit, mehr Geld für die Platzierung der Werbung zu bezahlen. Viele Website-Betreiber sind auf die so generierten Werbeeinnahmen angewiesen.

Die Erstellung von Nutzerprofilen und die Verknüpfung von Daten birgt aber auch potenzielle Sicherheitsrisiken, da der Nutzer immer gläserner wird.

Aus diesem Grund haben Apple im Safari- und Mozilla im Firefox-Browser Drittanbieter-Cookies bereits blockiert. Da Google jedoch viel Geld mit personalisierter Werbung verdient, kommt eine einfache Blockade von Drittanbieter-Cookies im Chrome-Browser für Google nicht infrage. Im Jahr 2022 betrug der Werbeumsatz von Google 224,47 Milliarden US-Dollar.[1] Mit „Topics“ führt Google seit 2024 eine Alternative ein, die sowohl die Privatsphäre der Nutzer respektieren als auch die Anzeige personalisierter Werbung ermöglichen soll.

II. Funktionsweise von Topics

Der Nutzer merkt zunächst gar nicht, dass er Topics nutzt. Topics ist eine Anwendung, die sich im Chrome-Browser von Google befindet und bei künftigen Software-Updates automatisch mitgeliefert wird. Schon jetzt ist im Chrome-Browser im Menü (Symbol ⋮) unter „Einstellungen“ > „Datenschutz und Sicherheit“ > „Datenschutz bei Anzeigen“ der entsprechende Bereich eingerichtet.

Mit Topics ist die von Google selbst vorgenommene Unterteilung in Themen gemeint. Insgesamt sollen zu Beginn 350 verschiedene Themen zur Verfügung stehen. Die endgültige Anzahl der Themen stehe jedoch noch nicht fest. Eine größere Auswahl an Themen würde die Zielgenauigkeit für die Werbeindustrie erhöhen. Eine

1 https://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/ (zuletzt abgerufen am 05.03.2024).

zu große Anzahl von Themen könnte jedoch dazu führen, dass so wenige Nutzer einem „Nischenthema“ zugeordnet werden, dass diese wieder identifiziert werden können. Die vom Nutzer aufgerufene Website wird einem Thema wie „Autos & Fahrzeuge“, „Bücher & Literatur“ oder „Rock Musik“ zugeordnet.

Topics verwendet für die Zuordnung in erster Linie den Hostnamen der Website. Um die Zuordnung zu verbessern, wird Topics laufend trainiert und verfeinert. Website-Betreiber haben zudem die Möglichkeit, Informationen im Quellcode der Seite anzugeben, um die Zuordnung zu verbessern.

Topics speichert dann bis zu drei Themen aus dem Inhalt der Website, um ein Nutzerprofil zu erstellen. Dieses besteht dann nur noch aus den fünf relevantesten Themen der Woche. Diese Themen werden drei Wochen lang gespeichert und anschließend gelöscht. Somit hat Topics stets 15 Themen des Nutzers zur Verfügung. Diese sollen jedoch nicht auf einem zentralen Server gespeichert werden, sondern dezentral, in einem gesicherten Bereich des Browsers, der Privacy Sandbox.

Dadurch sollen die während des Surfens übertragenen Daten in engeren Grenzen gehalten werden. Ein Caller, der in die besuchte Website integriert ist, fragt die bevorzugten Themen des Nutzers ab. Dabei wird auch die IP-Adresse des Nutzers übermittelt. Der Caller kann jedoch nicht beliebig viele Themen abfragen, sondern erhält maximal drei Themen, die aus den Top 5 Themen des Nutzers ausgewählt werden. Diese übermittelt der Caller dann an das Werbenetzwerk, das die personalisierte Werbung ausspielt. So soll eine Identifizierbarkeit des Nutzers für die werbenden Unternehmen ausgeschlossen werden. Dies soll auch dadurch sichergestellt werden, dass eine der übermittelten Kategorien in 5 Prozent der Fälle eine der übermittelten Kategorien eine zufällige Kategorie ist, die nicht auf dem vergangenem Nutzerverhalten basiert.[2] Darüber hinaus soll das weitere Surfverhalten geschützt werden und kein seitenübergreifendes Tracking möglich sein.

Sensible Kategorien wie Religion, Ethnie oder Geschlecht sollen von vornherein gänzlich ausgenommen werden. Der Nutzer selbst soll in den Browsereinstellungen für ihn nicht relevante Kategorien löschen können. Über eine Opt-Out-Funktion will Google es den Nutzern auch ermöglichen, die Übermittlung von Kategorien gänzlich auszuschließen.

Obwohl dadurch weniger Daten übermittelt werden, sollen die Ergebnisse für die Werbewirtschaft annähernd gleich gut sein. Verglichen mit den Ergebnissen mit Drittanbieter-Cookies liegt die Wahrscheinlichkeit, dass ein Nutzer auf eine Werbeanzeige klickt, immerhin bei 90 Prozent des aktuellen Niveaus.[3]

III. Auswirkungen auf Cookie-Banner

Bislang ist für das Setzen von Cookies eine Einwilligung des Nutzers gemäß Art. 25 Abs. 1 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) erforderlich. Einwilligung und Information müssen den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen.[4] Die Weiterverarbeitung der durch die Cookies gewonnen Daten unterliegt hingegen der DSGVO. Daher muss jede Website, die Cookies von Drittanbietern verwendet, zwei Einwilligungen vom Nutzer einholen.
Google hat mit Topics die Möglichkeit, die Einwilligung für die Speicherung der Themen sowie für den Zugriff durch den Caller und die Weiterverarbeitung durch diesen einzuholen. So würden drei Einwilligung zu einer zusammengefasst und es müsste nicht mehr auf jeder Website eine Einwilligung eingeholt werden.[5]

IV. Ausblick

Ob sich Topics durchsetzen wird, bleibt abzuwarten. Eine sinnvolle Nutzung hängt auch davon ab, wie gut der Browser die Kategorien zuordnet und ob viele Websites von ihren Betreibern angepasst werden, um die Zuordnung zu einzelnen Topics zu erleichtern.

2 Muttach/Köppel/Hornung, Google Topics als Ausweg aus dem Cookie-Dilemma?, CR 10/2023, 644, 646 Rn. 11.

3 https://www.heise.de/news/Topics-Google-findet-seinen-Cookie-Nachfolger-gut-8970454.html (zuletzt abgerufen am 27.10.2023).

4 Art. 25 Abs. 1 S. 2 TTDSG.

5 Muttach/Köppel/Hornung, Google Topics als Ausweg aus dem Cookie-Dilemma?, CR 10/2023, 644, 646 Rn. 61.

Mit der Marktmacht des Chrome-Browsers[6] hat Google jedoch gute Chancen, Topics zu einem neuen Standard in der Branche der personalisierten Werbung zu machen.

V. Kritik

Ob dies ein Fortschritt im Kompromiss zwischen den widerstreitenden Interessen des Datenschutzes und der personalisierten Werbung ist, bleibt jedoch umstritten.

Wenn sich Topics durchsetzt, wird Googles Chrome-Browser der einzige Ort sein, an dem werberelevante Informationen gespeichert werden. Dies stärkt die Marktmacht von Google.

Google wird deshalb vorgeworfen, mit den Beschränkungen Dritte zu blockieren, während es für seine eigenen Werbedienste weiterhin alle Daten nutzen möchte. Zudem wird Google vorgeworfen kartellrechtswidrig zu handeln und keinen nennenswerten Beitrag für den Datenschutz zu leisten.[7] Diese Kritik wird von Google zurückgewiesen und stattdessen der Druck der europäischen Datenschutzbehörden angeführt,[8] der Google dazu veranlasste, Google Topics zu entwickeln.

Cookie-Banner für Erstanbieter-Cookies werden durch Topics nicht obsolet. Ob Cookie-Banner jemals ganz der Vergangenheit angehören werden, wird die Zukunft zeigen. Möglicherweise erzielt die Initiative der EU-Kommission im Zurückdrängen der Cookie-Banner Fortschritte.[9]

VI. Hochschulbezug

Auf den Computern der Mitarbeiter der Universitäten sind teilweise viele Cookies installiert. Nutzer des Chrome-Browsers können sich im Menü (Symbol ⋮) unter „Einstellungen“ > „Datenschutz und Sicherheit“ > „Drittanbieter-Cookies“ > „Alle Websitedaten und -berechtigungen ansehen“ eine Liste der Websites anzeigen lassen, die Cookies gesetzt haben. Schon aus diesem Grund lohnt es sich, diesen Infobrief zum Anlass zu nehmen, um die Datenschutzeinstellungen des Browsers auf den Prüfstand zu stellen.

Für Hochschulen kann es ratsam sein, ihre Website so zu optimieren, dass der Browser des Besuchers sie in die richtige Kategorie einordnet.
Wenn sich die Technologie durchsetzt, werden zudem bald keine Drittanbieter-Cookies mehr auf den Rechnern der Hochschulen gesetzt, da Google diese in Zukunft blockieren wird.

---

6 64,84 % im Januar 2024 weltweit, abrufbar unter https://de.statista.com/statistik/daten/studie/157944/umfrage/marktanteile-der-browser-bei-der-internetnutzung-weltweit-seit-2009/ (zuletzt abgerufen am 05.03.2024).

7 Höppner/Westerhoff, Datenschutz ist nicht Schutz von Datenimperien, Politik und Recht, S. 42 f., abrufbar unter file:///U:/InfoBriefe/2024%2004%20-%20Google%20Topics/print-more_2021_03_ho-ppner_westerhoff.pdf (zuletzt abgerufen am 05.03.2024).

8 https://www.faz.net/aktuell/wirtschaft/unternehmen/cookies-google-kippt-das-system-des-kostenlosen-internets-19547200.html (zuletzt abgerufen am 05.03.2024).

9 https://www.spiegel.de/netzwelt/cookies-eu-kommission-will-banner-auf-websites-abschaffen-a-898055cb-c2f1-440f-b1fb-b9175dc6d0cc (zuletzt abgerufen am 05.03.2024).

Ich glaub, es hackt

EuGH-Urteil zu Haftungsrisiken infolge eines Hackerangriffs: Angst vor Datenmissbrauch als immaterieller Schaden

von Johannes Müller

Der Europäische Gerichtshof (EuGH) - Urteil vom 14.12.2023 – C-340/21[1] - hat sich in jüngster Zeit mit den Voraussetzungen und Rechtsfolgen eines datenschutzrechtlichen Schadensersatzanspruchs aufgrund eines Verstoßes gegen die IT-Sicherheitspflichten beschäftigt. Das Urteil stärkt das Verständnis für Haftungsrisiken, die bei Datensicherheitsverstößen auftreten können.

I. Haftungsrisiken aufgrund von Verstößen gegen die Datensicherheit

Cybersicherheit ist infolge der hohen Anzahl von Hackerangriffen in der jüngsten Zeit immer stärker ins öffentliche Bewusstsein gerückt.[2] Als mögliche finanzielle Schäden eines Cybersicherheitsangriffs sind der Kontrollverlust über wertvolle Daten und mögliche Lösegeldforderungen von Hackern weitestgehend bekannt. Darüber hinaus darf jedoch das Risiko einer zivilrechtlichen Haftung nicht vernachlässigt werden. Dies kann in Form eines datenschutzrechtlichen Schadensersatzanspruchs gemäß Art. 82 Datenschutzgrundverordnung (DSGVO) geltend gemacht werden. Der datenschutzrechtliche Schadensersatzanspruch ist die momentan wohl am stärksten diskutierte Thematik im Datenschutzrecht. In letzter Zeit sind mehrere Urteile zu der Frage ergangen, unter welchen Voraussetzungen nicht nur materielle, sondern auch immaterielle Schäden eines Datenschutzverstoßes zu ersetzen sind.[3] Ein solcher Datenschutzverstoß kann auch durch einen Hackerangriff erfolgen. Werden dabei personenbezogene Daten „gestohlen", ist es möglich, dass die betroffenen Personen den Verantwortlichen in Anspruch nehmen, dessen Dateisystem infolge unzureichender Schutzmaßnahmen gehackt wurde.

II. Anforderungen an die Datensicherheit in Art. 32 DSGVO

Art. 32 DSGVO trifft Regelungen zu den Sicherheitsanforderungen, die der Verantwortliche einer Datenverarbeitung für personenbezogene Daten treffen muss. Diese dienen dem Schutz von personenbezogenen Daten, sollen also gemäß Art. 4 Nr. 12 DSGVO die Vernichtung, den Verlust, die Veränderung oder die Offenlegung von personenbezogenen Daten verhindern, sofern diese unbeabsichtigt oder rechtswidrig wären. Art. 32 Abs. 1 DSGVO trägt gemeinsam mit Art. 24 DSGVO den Verantwortlichen und Auftragsverarbeitern auf, technische und organisatorische Maßnahmen (kurz TOMs) festzulegen, um ein angemessenes Schutzniveau sicherzustellen. Verantwortliche und Auftragsverarbeiter müssen die Risiken ihrer jeweiligen Verarbeitung reflektieren und risikoadäquate Maßnahmen ergreifen, die zu einem möglichst hohen Maß an Datensicherheit führen. Aus Art. 32 Abs. 1 DSGVO lässt sich ein Katalog verschiedener TOMs entnehmen, der nicht abschließend ist. Er gliedert sich in konkrete Maßnahmen wie z.B. die Pseudonymisierung (Abs. 1 lit. a) und in abstrakte Maßnahmen, die eher Zielvorgaben ähneln (lit. b und c). Welche Maßnahmen Verantwortliche und Auftragsverarbeiter ergreifen, steht grundsätzlich in ihrem eigenen Ermessen, sofern sie ein dem Risiko angemessenes Schutzniveau gewährleisten. Die Orientierung des Schutzniveaus an dem Risiko im Einzelfall

1 Die Pressemitteilung des EuGHs zum Urteil kann unter dem folgenden Link nachgelesen werden https://curia.europa.eu/jcms/jcms/p1_4220393/de/ (zuletzt abgerufen am 08.03.2024).

2 Vgl. John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 04/2023.

3 Vgl. Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht, 07/2023; ausführlich zum Ersatz immaterieller Schäden infolge eines Datenschutzverstoßes, Müller, Morgen Kinder werden wir klagen, DFN-Infobrief Recht 12/2022.

ist als Ausprägung des risikobasierten Ansatzes einzuordnen, der sich in der DSGVO häufig findet.

Werden die erforderlichen, dem Sicherheitsrisiko entsprechenden Pflichten verletzt, liegt ein Verstoß gegen Art. 32 DSGVO vor. Resultiert dieser in einem Sicherheitsvorfall, der den betroffenen Personen einen Schaden zufügt, können diese gemäß Art. 82 DSGVO Schadensersatz verlangen. Zu den konkreten Anforderungen hat nun der EuGH Stellung genommen.

III. Sachverhalt des EuGH-Urteils

Infolge eines Cyberangriffs auf die bulgarische Nationale Agentur für Einnahmen (NAP) wurden 2019 personenbezogene Daten von mehr als sechs Millionen Personen im Internet veröffentlicht. Einige Hundert von ihnen, darunter die Klägerin des Ausgangsverfahrens, verklagten daraufhin die NAP auf der Grundlage von Art. 82 DSGVO auf Ersatz des entstandenen immateriellen Schadens. Dieser ergebe sich aus einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO und insbesondere aus einer Verletzung der Sicherheit, die dadurch verursacht worden sei, dass die NAP gegen ihre Verpflichtungen aus Art. 5 Abs. 1 Buchst. f sowie aus Art. 24 und 32 DSGVO (TOMs) verstoßen habe. Der Schaden der Klägerin bestehe in der Befürchtung, dass ihre personenbezogenen Daten künftig missbräuchlich verwendet würden. Die NAP verteidigte sich und legte unter anderem Dokumente zum Nachweis dafür vor, dass sie alle erforderlichen TOMs ergriffen habe. Ihrer Ansicht nach seien Angst und Befürchtungen zudem auch nicht als immaterielle Schäden ersatzfähig. Überdies könne sie nicht für die schädlichen Folgen dieser Verletzung verantwortlich gemacht werden, da sie selbst durch Personen, die nicht ihre Bediensteten seien, böswillig geschädigt worden sei.

Das erstinstanzliche Verwaltungsgericht der Stadt Sofia schloss sich der Auffassung der NAP an und wies die Klage mit Entscheidung vom 27. November 2020 ab.

Die Klägerin des Ausgangsverfahrens legte gegen diese Entscheidung Kassationsbeschwerde beim Obersten Verwaltungsgericht in Bulgarien ein. Sie stützt ihr Rechtsmittel darauf, dass das erstinstanzliche Gericht bei der Verteilung der Beweislast hinsichtlich der von der NAP ergriffenen Sicherheitsmaßnahmen einen Rechtsfehler begangen habe. Ferner sei die Befürchtung eines möglichen künftigen Missbrauchs ihrer personenbezogenen Daten ein tatsächlicher immaterieller und kein hypothetischer Schaden.

IV. Relevante Rechtsfragen

Das Oberste Verwaltungsgericht Bulgarien legte dem Europäischen Gerichtshof mehrere Rechtsfragen vor. Besonders relevant ist die Frage, ob jede unbefugte Offenlegung von Daten einen Verstoß gegen die Anforderungen in Art. 24 und 32 DSGVO indiziert. Ihre Bejahung durch den EuGH würde bedeuten, dass bei jedem erfolgreichen Hackerangriff, der personenbezogene Daten betrifft, ein Pflichtenverstoß des verantwortlichen Datenverarbeiters anzunehmen ist. Für den Fall, dass der EuGH die Frage verneint, wollte das Oberste Verwaltungsgericht in Bulgarien wissen, wer die Beweispflicht dafür trägt, dass die Maßnahmen zur Wahrung der Datensicherheit angemessen im Sinne von Art. 32 DSGVO waren.

Darüber hinaus wurden relevante Fragen zum Schadensersatzanspruch nach Art. 82 DSGVO gestellt. Der EuGH sollte die Frage beantworten, ob bei einem Verstoß von Dritten gegen die DSGVO der Verantwortliche selbst von der Haftung befreit wird. Bei Bejahung dieser Frage wären die Haftungsrisiken eines Datenverarbeiters durch einen Hackerangriff weitestgehend reduziert, da die unmittelbare Offenlegung der Daten durch die Hacker und nicht den Verantwortlichen der Datenverarbeitung erfolgte. Darüber hinaus wollte das nationale Gericht wissen, ob Sorgen, Befürchtungen und Ängste einer von einem Hackerangriff betroffenen Person vor einem möglichen künftigen Missbrauch der personenbezogenen Daten einen immateriellen Schaden darstellen.

V. Das Urteil des EuGHs

Der EuGH stellte zunächst klar, dass nicht jede unbefugte Offenlegung personenbezogener Daten für die Annahme genügt, dass die getroffenen technischen und organisatorischen Maßnahmen ungeeignet im Sinne von Art. 24 und 32 DSGVO waren. Dies begründet er unter anderem damit, dass der Unionsgesetzgeber die Sicherheitsrisiken lediglich „eindämmen“ wollte, ohne zu behaupten, dass sie vollkommen beseitigt werden würden. Diese Ansicht des EuGHs entlastet die Haftungsrisiken von Datenverarbeitern erheblich. Nicht jeder Cybersicherheitsvorfall erlaubt hiernach den Rückschluss, dass der Verantwortliche

seine Sicherheitsrisiken verletzt hat.
Zu der Beweislast bezüglich der Angemessenheit der Maßnahmen führt der EuGH aus, dass diese bei dem verantwortlichen Datenverarbeiter liegt. Er muss demnach nachweisen, dass TOMs, die er getroffen hat, ein angemessenes Datensicherheitsniveau gewahrt haben. Denn gem. Art. 5 Abs. 2 DSGVO gilt, dass der Verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO aufgestellten Grundsätze einhält. Zu diesen Grundsätzen zählt auch die durch Art. 32 DSGVO konkretisierte Pflicht zur Einhaltung der Datensicherheit. Ebenso lasse sich dem Wortlaut von Art. 24 und Art. 32 DSGVO entnehmen, dass dem Verantwortlichen die Beweislast zur Einhaltung der Schutzpflichten obliege. Darüber hinaus würde der datenschutzrechtliche Schadensersatzanspruch seine Wirkung teilweise verlieren, wenn die betroffene Person als Kläger nachweisen müsste, dass der Verantwortliche seine Pflichten nicht eingehalten hat.

Zum Schadensersatzanspruch selbst hat der EuGH ausgeführt, dass der Verantwortliche von seiner Schadensersatzpflicht nach Art. 82 Abs. 1 und 2 DSGVO nicht allein deshalb befreit ist, weil dieser Schaden Folge einer unbefugten Offenlegung von personenbezogenen Daten durch „Dritte“ im Sinne von Art. 4 Nr. 10 DSGVO ist. Sofern also Cyberkriminelle selbst unmittelbar verantwortlich für einen Datenschutzverstoß sind, steht dies einer Haftung des Datenverarbeiters nicht entgegen, sofern dieser seine Pflichten aus Art. 24 und 32 DSGVO verletzt hat.

Zum Inhalt eines möglichen Schadensersatzanspruchs gegen den Datenverarbeiter gab der EuGH an, dass als immaterieller Schaden bereits die Befürchtung in Betracht käme, dass personenbezogene Daten durch Dritte missbräuchlich verwendet werden könnten. Hierbei wiederholte er seine vorherige Rechtsprechung, dass der Ersatz eines immateriellen Schadens nach Art. 82 Abs. 1 DSGVO nicht davon abhängig gemacht werden dürfe, dass eine gewisse Erheblichkeit erreicht werde.[4] Zudem unterscheide die DSGVO nicht, ob der von der betroffenen Person behauptete „immaterielle Schaden“ mit einer bereits erfolgten missbräuchlichen Verwendung ihrer personenbezogenen Daten durch Dritte verbunden sein muss oder ob er mit Angst vor einer solchen Verwendung in der Zukunft verknüpft sei. Allerdings muss die betroffene Person nachweisen, dass die Folgen des Verstoßes einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen. Unter Verweis auf Erwägungsgrund 85 der DSGVO begründet der EuGH, dass der Verlust der Kontrolle über personenbezogene Daten bereits einen möglichen Schaden darstellt. Dieses sehr weite Schadensverständnis relativiert der EuGH dann jedoch auch wieder teilweise, indem er erneut auf seine vorherige Rechtsprechung verweist, nach der die betroffene Person nachweisen muss, dass sie tatsächlich einen Schaden erlitten hat.[5] Das jeweilige nationale Gericht müsse im individuellen Fall überprüfen, ob die behauptete Befürchtung der betroffenen Person auch als begründet angesehen werden kann.

VI. Auswirkungen des Urteils für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen sind in jüngster Zeit wiederholt Opfer von Cyberangriffen geworden. Es ist davon auszugehen, dass hierbei auch personenbezogene Daten verloren gegangen sind. Als Verantwortliche der jeweiligen Datenverarbeitungen müssen sie die notwendigen technischen und organisatorischen Maßnahmen treffen, um die Sicherheit der Daten zu garantieren. Anders als private Unternehmen kann eine etwaige Pflichtverletzung durch öffentliche Einrichtungen nicht durch Bußgelder geahndet werden.[6] Damit bilden zivilrechtliche Schadensersatzansprüche gemäß Art. 82 DSGVO das primäre Haftungsrisiko für öffentliche Forschungseinrichtungen, die Opfer von Hackerangriffen werden. Das Verständnis für die Haftungsrisiken kann nun durch das Urteil erheblich geschärft werden. Universitäten werden zunächst durch die Entscheidung, dass nicht jede unbefugte Offenlegung automatisch zur Annahme eines Verstoßes gegen Art 32 DSGVO führt, entlastet. Gleichzeitig müssen Forschungseinrichtungen gegebenenfalls imstande sein, nachzuweisen, dass sie ausreichende Maßnahmen zum Schutz der Datensicherheit getroffen haben. Hierzu sollten getroffene TOMs sorgfältig dokumentiert werden. Kann eine Forschungseinrichtung nicht darlegen, dass sie die erforderlichen Sicherheitsmaßnahmen getroffen hat, ist sie für Schäden verantwortlich, die infolge der Nachlässigkeit – auch durch Dritte – entstehen. Mögliche Schäden können auch in Form plausibel dargelegter emotionaler Einschränkungen bestehen, wie die Furcht vor einer zukünftigen missbräuchlichen Verwendung ihrer Daten durch Dritte.

4 Hierzu Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

5 Voget, Kurzbeitrag: Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

6 Vgl. Müller, Bußgeldberechnung für Dummies, DFN-Infobrief Recht 10/2022.

Die Bretonage der europäischen Datenstrategie

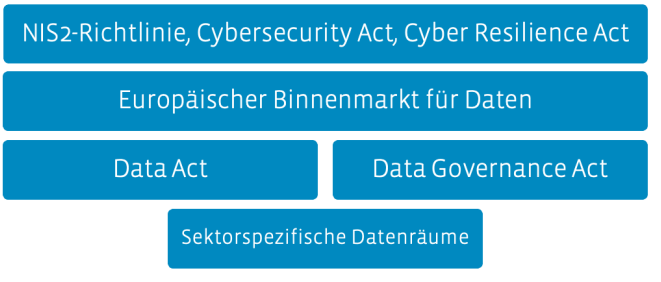
Lähmt das Cyber-Sicherheitsrecht die europäische Datenwirtschaft?

Von Ole-Christian Tech

Der European Cyber Resilience Act (CRA) hat ein ambitioniertes Ziel: Er soll verbindliche Cybersecurity Anforderungen für Hardware- und Softwareprodukte mit digitalen Elementen auf dem gesamten europäischen Binnenmarkt schaffen. Hersteller werden dadurch für die Sicherheit ihrer Produkte über die gesamte Lebensdauer verantwortlich gemacht.

I. Der Cyber Resilience Act im Überblick[1]

Durch den CRA soll nicht nur der gemeinsame Markt und der Verbraucher geschützt, sondern zugleich auch die gesamte Datenstrategie der EU abgesichert werden, da das Sicherheitsrecht (NIS-2, CSA, CRA)[2] über allen Datenräumen thront und das entfesselte, industrieübergreifende Teilen und Nutzen von Daten absichert.
Hier ein vereinfachter Überblick:



Der CRA ist die erste Verordnung der Europäischen Union zur sektorübergreifenden, horizontalen Stärkung der Cybersicherheit von Produkten mit digitalen Elementen.[3]

Ende 2023 wurde im Trilogverfahren die politische Einigung erzielt, bereits 2024 soll diese Fassung verabschiedet werden und dann, nach weiteren 36 Monaten, in allen Mitgliedstaaten unmittelbar Anwendung finden.

Hintergrund des Gesetzes ist die Erkenntnis, dass sich Cybersicherheitslecks bei Produkten im Binnenmarkt auch im gesamten europäischen Datenraum auswirken und daher ein einheitliches Sicherheitsniveau erforderlich ist.

Einerseits soll hierfür das Sicherheitsniveau der Produkte insgesamt erhöht und durch entsprechende Sicherheitsupdates auch beibehalten werden.

Andererseits sollen Informationsasymmetrien zulasten der Endnutzer und Verbraucher abgebaut werden, etwa durch Informationspflichten für den Hersteller.

Der Pflichtenkatalog für die Hersteller umfasst dabei Prozess- und Dokumentationspflichten (aufgelistet in Art. 10 CRA-E) sowie Meldepflichten (Art. 11 CRA-E).

---

1 Vertiefend hierzu Palenberg, Cyber Angriff ade mit dem CRA-E? in DFN-Infobrief Recht 9/2023 S. 2ff.

2 Die NIS-2-Richtlinie (Network and Information Security (NIS) Directive) ist am 16.01.2023 in Kraft getreten und enthält die Cyber- und Informationssicherheit von Unternehmen, siehe hierzu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS? in DFN-Infobrief Recht 4/2023; der Cyber Security Act (CSA) ist seit dem 27. 06 2019 in Kraft und enthält einen Zertifizierungsrahmen für IT-Produkte.

3 Kipker in: Ebers, StichwortKommentar Legal Tech, Cybersecurity Rn. 24.

Bei genauerem Blick verfolgt der CRA also mit dem Regelungszweck der Cybersicherheit zugleich auch den Käufer- und Verbraucherschutz.

Damit aber nicht genug. In Erwägungsgrund 17 zum CRA erklärt die Kommission: „Durch den Schutz von Verbrauchern und Organisationen vor Cybersicherheitsrisiken sollen die in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen auch dazu beitragen, den Schutz personenbezogener Daten und den Schutz der Privatsphäre natürlicher Personen zu verbessern." Das Gesetz soll also zudem auch Synergieeffekte im Zusammenspiel mit der Datenschutzgrundverordnung (DSGVO) erzeugen und somit dem Datenschutz dienen.

II. Ein Datenminimierungsgrundsatz im CRA?

Dabei verfolgt auch der CRA – ähnlich wie bereits die DSGVO – keinen absoluten Schutz, sondern eine Risikobewertung und ein dem Risiko angemessenes Schutzniveau. Dies bestätigt Art. 10 Abs. 2 CRA, der eine Verpflichtung der Hersteller zur Bewertung der Cybersicherheitsrisiken normiert.

Soweit so gut, scheint es. Der CRA schafft also, was er verspricht: resiliente und sichere Verarbeitungs- und Übermittlungsumgebungen, um die Datenwirtschaft anzukurbeln. Bei genauerer Lektüre des Entwurfs taucht jedoch ein Fremdkörper in dem Regelwerk auf: Anhang I Abschnitt 1 trägt den unschuldig anmutenden Titel „Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen". Dahinter verbirgt sich in Absatz 3 lit. e jedoch folgende Formulierung: „Auf der Grundlage der Risikobewertung gemäß Artikel 10 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,(…) die Verarbeitung personenbezogener oder **sonstiger Daten**[4] auf solche, die angemessen und relevant sind, und auf das für die bestimmungsgemäße Verwendung des Produkts erforderliche Maß beschränken (‚Datenminimierung')."

Ein Grundsatz der Datenminimierung für nicht personenbezogene Daten?

Der Grundsatz der Datenminimierung – umgangssprachlich auch Datensparsamkeit genannt – ist bisher fast ausschließlich im Kontext mit der DSGVO aufgetaucht.

III. Der Datenminimierungsgrundsatz im Datenschutzrecht

Abgeleitet wird dieser aus Art. 8 Abs. 1 und 2 der Charta der Grundrechte der Europäischen Union (GRCh) und dem informationellen Selbstbestimmungsrecht in den Mitgliedstaaten, in Deutschland also Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 Grundgesetz (GG).[5] In Artikel 5 Abs. 1 lit. c DSGVO erhält die Datenminimierung sogar den Rang eines allgemeinen Grundsatzes für die Verarbeitung personenbezogener Daten.

Der Datenminimierungsgrundsatz nach der DSGVO verbietet die Verarbeitung personenbezogener Daten, die angesichts des Verarbeitungszwecks inadäquat, unerheblich oder entbehrlich sind. Diese Kriterien sind im Einzelfall durchaus wertungsoffen und können in der Praxis zu einer gewissen Rechtsunsicherheit führen. Diese Rechtsunsicherheit nimmt der europäische Gesetzgeber jedoch bewusst in Kauf, da die informationelle Selbstbestimmung des Betroffenen als Rechtsgut von Verfassungsrang auf dem Spiel steht.

Insbesondere da, wo zahlreiche für sich genommen unverfängliche, personenbezogene Daten kombiniert werden, kann durch die Kombination dieser Punkte womöglich ein detailliertes Persönlichkeitsprofil erstellt oder sogar besonders sensible persönliche Daten ermittelt werden.[6]

Was für personenbezogene Daten aber sinnvoll ist, kann für „sonstige Daten" zu einem echten Hemmnis werden.

IV. Das Problem

Hersteller sollen Produkte so designen, einstellen und instand halten, dass sie nur die für den jeweils im Vorhinein definierten Produktzweck unbedingt erforderlichen Daten verarbeiten,

4 Hervorhebung durch den Autor.

5 So etwa auch Spiecker gen. Döhmann/Bretthauer in: Spiecker gen. Döhmann/Bretthauer, Dokumentation zum Datenschutz, G 2.4.56.

6 Zu dem Problem der „Daisy Chains" siehe bereits Tech, Doppelgänger Delights: How to prevent the perfect impersonation (Or Not) in DFN-Infobrief Recht 4/2023.

selbst wenn dies nur harmlose Maschinendaten oder z. B. Wetterdaten sind.

Ein Einsatz dieser Daten für eine spätere Sekundärnutzung ist dadurch erheblich erschwert, schließlich mangelt es bei strenger Beachtung der Datensparsamkeit bereits an deren Verfügbarkeit. Unklar ist damit insbesondere das Regelungsziel mit Blick auf den Anfang 2024 in Kraft getretenen Data Act, dessen erklärtes Ziel eine effiziente und niedrigschwellige Datennutzung ist.[7]

V. Kritik

Ein Grundsatz der Datenminimierung für nicht personenbezogene Daten wirkt wie der etwas plumpe Ansatz „Keine Verarbeitung ist die sicherste Art der Verarbeitung". Sicher ein risikoaverser Ansatz, jedoch keiner, den sich ein europäischer Binnenmarkt im globalen Wettbewerb leisten kann.

Ein klassisches Beispiel der fast schon naiven Überregulierung also?

Hierzu findet sich im Zusammenhang mit dem verantwortlichen EU-Kommissar für den Binnenmarkt Thierry Breton (in dessen Zuständigkeit auch die Datenstrategie fällt) ein interessanter Neologismus: bretonieren [bʁe:toˈni:ʁən].[8] Es bedeutet so viel wie, durch schlechte und von falschen, sachfremden Interessen geleitete Regulierung, technologische und ökonomische Chancen bereits im Keim zu ersticken.

Was auf den ersten Blick wie die lobenswerte und konsequente Weiterentwicklung eines etablierten und fundamentalen Grundsatzes der DSGVO scheint, birgt jedoch hinsichtlich der bisherigen Datenstrategie der EU einige Probleme.

Das erklärte Ziel der Datenstrategie war ursprünglich einmal, Datenoligopole aufzubrechen und Daten im europäischen Binnenraum möglichst frei zirkulieren zu lassen, um Erkenntnisse und Wertschöpfung aus diesen zu generieren. Dass dieses Ziel mit dem Datenschutz in Einklang zu bringen ist, ist offensichtlich. Nicht umsonst postulierte jeder Rechtsakt der Datenstrategie schon fast gebetsmühlenartig, er stehe im Einklang mit der DSGVO.[9]

Vor diesem Hintergrund erscheint ein Datenminimierungsgrundsatz im CRA zwar redundant – schließlich hat die DSGVO ja Vorrang[10] – aber zumindest unschädlich. Für die „sonstigen Daten" hingegen führt der Grundsatz zu einem Problem: Das eigentliche, übergeordnete Ziel der gesamten Datenstrategie wird hierdurch konterkariert. Erkenntnis und Wertschöpfung resultieren häufig gerade erst aus der Sekundärnutzung von Daten, also der Nutzung zu einem anderen Zweck als dem der ursprünglichen Datenerhebung. Erst durch große Datenmengen (Big Data) können Muster erkannt werden, nach denen womöglich gar nicht gezielt gesucht wurde. All dies wird nun erschwert, da der Datenminimierungsgrundsatz bereits die Menge an erhobenen Daten auf ein (willkürliches) Minimum begrenzt.

Gut gemeint ist eben nicht immer gut gemacht.

VI. Ausblick

Mit Inkrafttreten des CRAs werden die Compliance Anforderungen im Bereich der IT-Sicherheit nun weiter erhöht. Die Vermischung von IT-Sicherheitsrecht mit anderen, sachfremden Erwägungen macht die Handhabung für Hersteller und die gesamte Lieferkette jedoch undurchsichtiger. Jedenfalls die unter der DSGVO geltende Gewissheit, ohne personenbezogene Datenverarbeitung relativ frei schalten und walten zu können, ist damit dahin. Die Euphorie der Datenwirtschaft über die Datenstrategie und das große Sammeln und Wertschöpfen könnte hierdurch gedämpft werden.

---

7 Siehe hierzu vertiefend Müller, Die Daten sind frei? In DFN-Infobrief Recht 3/2024 und Schaller, Data Act: Mehr Daten für alle – check! in DFN-Infobrief Recht 6/2022.

8 Siehe hierzu auch Franz, https://www.cr-online.de/blog/2023/12/11/bretonieren-b%CA%81e%CB%90to%CB%88ni%CB%90%CA%81%C9%99n/.

9 So auch Veil, ZGI 2022, 197 (197); Genauer: Der Data Act Entwurf (COM(2022) 68 final) in Erwägungsgrund 7; der EHDS-VO Entwurf (COM(2022) 197 final) in Art. 1 Abs. 4; und der DGA Entwurf (COM(2020) 767 final) in Erwägungsgrund 3.

10 So auch ausdrücklich Erwägungsgrund 17 zum Cyber Resilience Act.

DFN Infobrief-Recht-Aktuell

Arbeitsrecht: Rat und Parlament der EU erzielen Einigung über die Richtlinie über Plattformarbeit

Am 08. Februar 2024 wurde eine vorläufige Einigung über die Richtlinie über Plattformarbeit zwischen dem Ratsvorsitz und den Verhandlungsführern des Europäischen Parlaments erzielt. Mit der Richtlinie sollen die Arbeitsbedingungen bei Verwendung von Algorithmen durch digitale Arbeitsplattformen transparenter gemacht werden. Automatisierte Systeme sollen nach den Vorgaben der Richtlinie von qualifiziertem Personal überwacht werden. Die Richtlinie verfolgt das Ziel, die Arbeitsbedingungen von Plattformbeschäftigten zu verbessern und die personenbezogenen Daten von Personen, die Plattformarbeit leisten, zu schützen.

Nachfolgend erhalten Sie den Link zur vorläufigen Einigung:

https://data.consilium.europa.eu/doc/document/ST-7212-2024-ADD-1/de/pdf (zuletzt abgerufen am 21.03.2024).

Datenschutzrecht: Handreichung zum Drittstaatentransfer:

Nach dem Angemessenheitsbeschluss der Europäischen Kommission vom 10. Juli 2023 wird ein Transfer an selbstzertifizierte US-Organisationen, die auf einer durch das US- Handelsministerium geführten Liste genannt sind, ermöglicht. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg Prof. Dr. Tobias Keber hat hierzu am 28. Februar 2024 eine Handreichung zu Kapitel V der DSGVO veröffentlicht.

Hier erhalten Sie den Link zur Handreichung:

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/Drittstaatentransfer-_online.pdf (zuletzt abgerufen am 21.03.2024).

Medienrecht: Anti-SLAPP-Richtlinie:

Die Anti-SLAPP-Richtlinie, die dem Schutz der freien Meinungsäußerung von Journalisten, Verlegern, Medienorganisationen, Menschenrechtsverteidigern sowie Organisationen der Zivilgesellschaft dienen soll, wurde am 19. März 2024 durch den Rat der EU angenommen. Natürliche und juristische Personen, die von sogenannten strategischen Klagen gegen öffentliche Beteiligung („strategic lawsuits against public participation“, SLAPP) betroffen sind, können bei Gericht beantragen, dass eine offensichtlich unbegründete Klage zum frühestmöglichen Zeitpunkt abzuweisen ist. Nach ihrer Veröffentlichung im Amtsblatt der EU wird sie am zwanzigsten Tag danach in Kraft treten und muss innerhalb von zwei Jahren in nationales Recht durch die Mitgliedstaaten umgesetzt werden.

Hier erhalten Sie den Link zur Richtlinie:

https://data.consilium.europa.eu/doc/document/PE-88-2023-INIT/de/pdf (zuletzt abgerufen am 21.03.2024).

Kurzbeitrag: Wie gewonnen, so zerronnen

Abgelehnter Bewerber verlangt Schadensersatz nach Auskunftsbegehren

von Ole-Christian Tech

Ein Kläger erringt vor dem Arbeitsgericht Hannover einen echten Pyrrhussieg. Das Gericht zeigt, warum die Sorge vor DSGVO Klagewelle womöglich unbegründet ist.

I. Was ist geschehen?

Der Kläger hatte sich erfolglos bei der Beklagten um einen Job beworben. Als diese den Kläger begründunglos ablehnte, stellte der Kläger am 7. Juli 2023 einen umfassenden Auskunftsanspruch nach Art. 15 Datenschutzgrundverordnung (DSGVO), um in Erfahrung zu bringen, welche personenbezogenen Daten zu welchem Zweck verarbeitet wurden.[1]

Etwa drei Wochen später, am 20. Juli 2023, beantwortete die Beklagte das Auskunftsbegehren und teilte dem Kläger unter anderem mit, welche Datenkategorien für die Durchführung des Bewerbungsverfahrens von ihrem HR Businesspartner gespeichert und verarbeitet wurden.

Am Folgetag, dem 28. Juli 2023, bemängelte der Kläger dann gegenüber der Beklagten die Unvollständigkeit der Auskunft, da er nicht nachvollziehen könne, wie lange die Speicherung seiner Daten erfolgt. Dies ist nach Art 15 Abs. 1 lit. d DSGVO jedoch Bestandteil einer Auskunft: „(…) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer“.

Erst am 11. August 2023 erklärte die Beklagte dann, die Löschung der Daten erfolge sechs Monate nach Eingang der Bewerbung und fügte außerdem den internen Bearbeitungsvermerk bei.[2]

Der Kläger zog daraufhin vor das Arbeitsgericht Hannover und machte einen Schadensersatzanspruch wegen immaterieller Schäden nach Art. 82 Abs. 1 DSGVO geltend. Diesen begründet er mit einem erlittenen Kontrollverlust über seine personenbezogenen Daten und einem „massiven Genervt sein “ aufgrund der späten Auskunft.

Gleichzeitig führt der Kläger weitere derartige Schadensersatzprozesse gegen verschiedene Beklagte, zum Teil vor demselben Gericht.

II. Die Entscheidung des Gerichts

Das Gericht sprach dem Kläger einen Schadensersatzanspruch zu.

Unter Verweis auf die Leitentscheidung des EuGHs vom 14. Dezember 2023, Rs. C-456/222, zum Ersatz immaterieller Schäden bestätigte die Kammer, dass eine Erheblichkeitsschwelle nicht erreicht werden müsse und daher bereits negative Gefühle wie Ärger oder „massives Genervt sein“ ausreichen, um den Tatbestand des Art. 82 Abs. 1 DSGVO zu erfüllen.[3] Der Kläger habe jedoch keinen Kontrollverlust über seine personenbezogenen Daten erlitten, da außer der längeren Wartezeit auf eine vollständige Auskunft keine Nachteile eingetreten seien.

---

1 Zum Auskunftsanspruch nach Art. 15 DSGVO siehe vertiefend Tech Doppelgänger Delights: How to prevent the perfect impersonation (Or Not) in DFN-Infobrief Recht 4/2023 und Palenberg Wer genau seid Ihr und wenn ja, wie viele? In DFN-Infobrief Recht 5/2023.

2 Die Speicherfrist umfasst für Bewerberdaten regelmäßig sechs Monate, da dies die Frist ist, innerhalb der abgelehnte Bewerber Klage wegen rechtswidriger Diskriminierung nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) erheben können. Um sich gegen diese Ansprüche zu verteidigen, benötigen Arbeitgeber die Bewerberdaten.

3 Siehe hierzu auch Müller in DFN-Infobrief Recht 4/2023.

Auch handele der Kläger nach Auffassung des Gerichts nicht rechtsmissbräuchlich, vielmehr sei es sein „gutes Recht“, seine Rechte nach der DSGVO unter Kostendruck auch parallel in zahlreichen anderen Verfahren geltend zu machen.

III. Die Krux der Entscheidung

Dennoch wird der Kläger das Ergebnis kaum als Erfolg verbuchen können.

Das Arbeitsgericht folgte zwar weitgehend seiner Rechtsauffassung, sprach ihm aber nur einen Anspruch in Höhe von 250 Euro statt der ursprünglich geforderten 5.000 Euro zu.

Außerdem setzte das Gericht den Streitwert auf 2.000 Euro fest und verurteilte den Kläger zur Zahlung von 95 Prozent der Kosten und den Beklagten zu 5 Prozent.

Vor den Arbeitsgerichten der ersten Instanz hat jede Partei die eigenen Kosten zu tragen. Hierbei ergeben sich bei einem Streitwert von bis zu 2.000 Euro Anwaltskosten in Höhe von 517,65 Euro.

Zwar sind die Gerichtskostengebühren im Arbeitsrecht etwas geringer als vor den ordentlichen Gerichten der Zivilgerichtsbarkeit, dennoch ergeben sich bereits Gerichtskosten in Höhe von 196 Euro, zuzüglich der Anwaltskosten von 517,65 Euro.[4]

Sollte der Kläger das Verfahren also in Gewinnerzielungsabsicht angestrengt haben, so hat er jedenfalls wirtschaftlich verloren. Sollte es ihm hingegen nur um die Bestätigung seiner Rechtsauffassung gegangen sein, so war ihm dies offenbar einen erheblichen Preis wert.

Ob er seine ebenfalls bereits anhängigen Klagen gegen Banken, Versicherungen und andere Unternehmen unter diesen Umständen noch weiterverfolgen wird, ist jedenfalls fraglich. Das Ergebnis erinnert jedenfalls ein wenig an König Pyrrhos von Epiros, der nach der sieg- aber auch verlustreichen Schlacht bei Asculum gesagt haben soll: „Noch einen solchen Sieg über die Römer, - dann sind wir vollständig verloren!“.

IV. Ausblick

Unter diesen Umständen werden Kläger von massenhaften Schadensersatzbegehren absehen. Die vielfach geäußerte Befürchtung der Verantwortlichen, von „DSGVO-Hoppern“ massenhaft in Anspruch genommen zu werden, könnte sich daher mittelfristig im Hinblick auf das Prozesskostenrecht als unbegründet erweisen. Die weitere Entwicklung bleibt abzuwarten.

4 Vgl. https://www.arbg-hamm.nrw.de/infos/kosten/gkr1/index.php. Verfahrensgebühr, Terminsgebühr und Auslagen: 435,-- € + 82,65 € USt = 517,65 €.zzgl. Gerichtskosten: 196,-- €.

Impressum

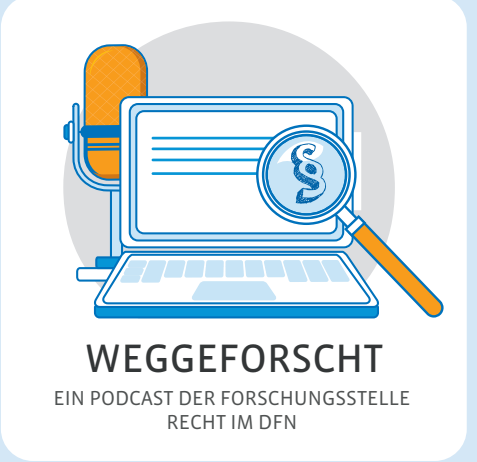
Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster
Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de



Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn