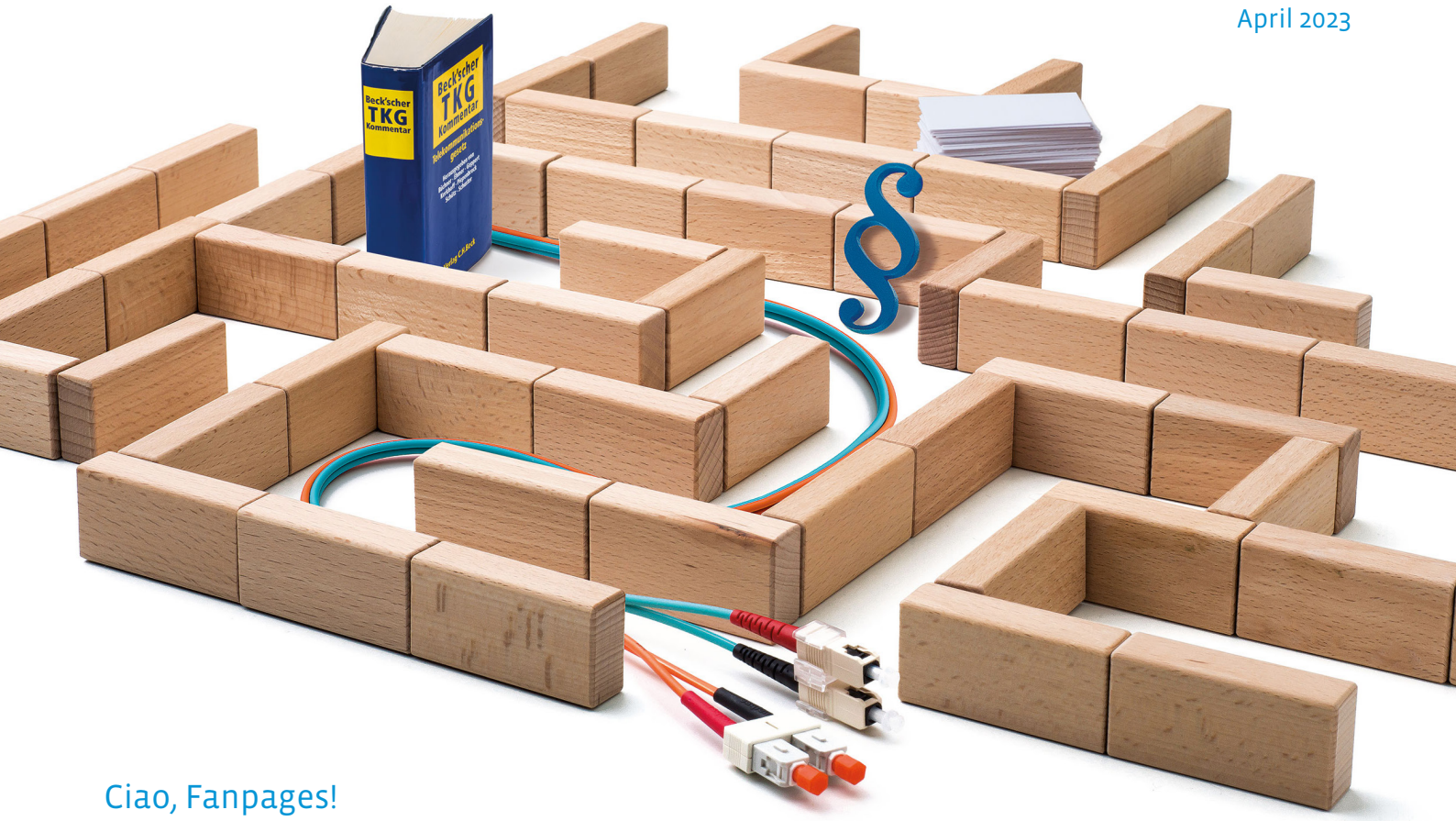
NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

4 / 2023
April 2023



Ciao, Fanpages!

BfDI untersagt Facebook-Präsenz der Bundesregierung

von Justin Rennert

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat dem Presse- und Informationsamt der Bundesregierung den Betrieb der Facebook-Seite der Bundesregierung untersagt. Die Entscheidung hat nicht nur unmittelbare Auswirkungen für die Bundesministerien und obersten Bundesbehörden, sondern auch erhebliche Bedeutung für alle anderen öffentlichen Stellen, die eigene Facebook-Seiten betreiben.

I. Hintergrund und Vorgeschichte

Das Presse- und Informationsamt der Bundesregierung betreibt seit Januar 2015 die Facebook-Seite der Bundesregierung. Auf dieser Seite informiert es über aktuelle politische Vorhaben und Vorgänge innerhalb der Bundesregierung. Mit Bescheid vom 17. Februar 2023 hat der BfDI dem Bundespresseamt den Betrieb der Seite nun untersagt. Als Begründung führte der BfDI an, dass auf der Fanpage Nutzerdaten erhoben und an den Facebook-Mutterkonzern Meta übermittelt würden, ohne dass hierfür eine wirksame Rechtsgrundlage vorhanden sei. Für die Datenverarbeitung sei die Bundesregierung mit Meta gemeinsam verantwortlich und habe somit die Einhaltung der datenschutzrechtlichen Vorschriften jederzeit sicherzustellen und nachzuweisen. Ein solcher Nachweis sei der Bundesregierung in dem dem Bescheid vorausgegangenen Verwaltungsverfahren nicht gelungen. Als letzte Konsequenz bliebe dem BfDI nun nur noch die Anordnung der Deaktivierung.

Die Entscheidung des BfDI hat eine lange Vorgeschichte. In Betrieb genommen hatte die Bundesregierung die Facebook-Seite (auch „Fanpage“ genannt) im Januar 2015. Im Jahr 2018 hatte der Europäische Gerichtshof (EuGH) sein erstes Urteil zu Facebook-Fanpages gefällt.[1] Danach sei für die Verarbeitung der Nutzerdaten nicht nur Facebook verantwortlich, sondern gem. Art. 26 DSGVO auch der Betreiber der Facebook-Seite. In Reaktion darauf wies der der BfDI im Mai 2019 alle Bundesministerien und obersten Bundesbehörden darauf hin, dass der Betrieb einer Facebook-Seite rechtlich nur möglich sei, wenn der Betreiber eine Vereinbarung zur gemeinsamen Verantwortlichkeit mit dem Facebook-Mutterkonzern schließe. Zum Abschluss einer derartigen Vereinbarung kam es in der Folge aber nicht. Die Facebook Ireland Ltd. war nach einer längeren Auseinandersetzung mit der Bundesregierung lediglich bereit, ein sogenanntes Addendum zu den Nutzungsbedingungen zur Verfügung zu stellen. In diesem legte Facebook aus Sicht des BfDI aber nicht hinreichend genau offen, welche Nutzerdaten zu welchem Zweck verarbeitet werden.

Im Juni 2021 informierte der BfDI die obersten Bundesbehörden und Bundesministerien darüber, dass das Addendum aus seiner Sicht nicht den Anforderungen des Art. 26 Datenschutz-Grundverordnung (DSGVO) genüge. Der Bundesbeauftragte empfahl den Behörden die Abschaltung aller Fanpages bis zum Ende des Jahres 2021, was einer Schonfrist gleichkam.

Im Mai 2022 gab der BfDI dem Bundespresseamt Gelegenheit zur Stellungnahme im Rahmen eines formalen Verwaltungsverfahrens. Spätestens zu diesem Zeitpunkt war klar, dass der BfDI es nicht bei einer bloßen Mahnung belassen würde und die Anordnung der Deaktivierung unmittelbar bevorsteht. Rückenwind hatte der BfDI zuvor von der gemeinsamen Datenschutzkonferenz

1 Baur, „So nicht, mein Facebook-Freund!“ in DFN-Infobrief Recht 06/19.

von Bund und Ländern erhalten. Diese hatte im März 2022 ein Kurzgutachten veröffentlicht, das die Rechtsauffassung des BfDI bestätigte: Fanpage-Betreiber und Meta seien gemeinsam für die Datenverarbeitung verantwortlich, wobei für die Datenverarbeitung zudem keine hinreichende Rechtsgrundlage bestünde. Die Datenverarbeitung sei deswegen rechtswidrig.

Zwar deaktivierte Facebook während des Verwaltungsverfahrens auf Wunsch des Bundespresseamts seine Statistik-Funktionen für die Seite der Bundesregierung, dies änderte jedoch nichts an der Rechtsauffassung des BfDI. Am 17. Februar veröffentlichte dieser nun seinen Bescheid, der seitdem auf der Webseite der Behörde öffentlich abrufbar ist.[2]

II. Datenverarbeitungen bei Betrieb einer Facebook-Seite

Der BfDI begründet seine Entscheidung unter anderem damit, dass das Bundespresseamt nicht darlegen könne, welche personenbezogenen Nutzerdaten bei Betrieb einer Facebook-Seite zu welchem Zweck erhoben würden. Und hierin liegt auch die besondere Problematik des Falles: Welche Nutzerdaten der Seitenbesucher verarbeitet Facebook überhaupt? Die Antwort auf diese Frage kennt nur Facebook selbst. Wenn aber Facebook und der Seitenbetreiber gemeinsam verantwortlich sind, dann muss auch der Seitenbetreiber nachweisen können, welche Daten zu welchem Zweck aufgrund welcher Rechtsgrundlage erhoben werden. Andernfalls verletzt er seine aus Art. 5 Abs. 2 DSGVO folgende Rechenschaftspflicht. Weil Facebook trotz Rückfragen der Bundesregierung nicht offenlegte, welche Nutzerdaten es zu welchem Zweck verarbeitete und dies auch in dem oben erwähnten Addendum nicht transparent machte, konnte das Bundespresseamt seiner Rechenschaftspflicht mithin gar nicht mehr gerecht werden.

Klar ist, dass Facebook sowohl die personenbezogenen Daten solcher Seitenbesucher verarbeitet, die ein Konto auf der Plattform haben, als auch die Daten solcher Nutzer, die überhaupt nicht auf Facebook registriert sind und die Fanpage als externe Nutzer besuchen. Im Falle der registrierten Nutzer gehören zu den verarbeiteten Daten in aller Regel der Klarname (es sei denn der Nutzer hat sich unter einem Pseudonym angemeldet) sowie eventuelle Likes und Kommentare unter den Postings auf der Fanpage. Im Falle der nicht registrierten Nutzer verarbeitet Facebook zwar nicht den Klarnamen, aber jedenfalls die IP-Adresse der Besucher. Insbesondere aus Kommentaren und Likes lassen sich politische Präferenzen der Nutzer ableiten. Die Beeinflussung der amerikanischen Präsidentenwahl im Jahre 2016 durch das Unternehmen Cambridge Analytica hat gezeigt, wie effektiv Facebook-Nutzerdaten für politische Zwecke eingesetzt werden können. Angesichts zahlreicher weiterer Fälle von Wahlbeeinflussung über Social-Media-Targeting in den letzten Jahren überrascht es nicht, dass der BfDI mit Blick auf die Facebook-Präsenz der Bundesregierung Vorsicht walten lässt.

Darüber hinaus besteht allerdings Unklarheit darüber, welche Nutzerdaten Facebook noch sammelt. Allenfalls eine Ahnung davon gibt ein Blick auf den Cookie-Speicher des eigenen Browsers. Über den xs-Cookie, einen sogenannten Session-Cookie, kann Facebook beispielsweise eine große Menge der während eines Seitenbesuches vorgenommenen Nutzeraktionen speichern. Mithilfe des fr-Cookies kann Facebook die Relevanz der angezeigten Werbeanzeigen messen. Der datr-Cookie weist auch nicht registrierten Nutzern eine eindeutige ID zu. So kann Facebook einen Nutzer wiedererkennen, der beim Besuch der Seite der Bundesregierung erstmals mit den Facebook-Servern kommuniziert hat – und zwar auch dann, wenn er andere Facebook-Angebote nutzt und sich gar nicht mehr auf der Seite aufhält. Möglicherweise funktioniert dies sogar dienstübergreifend, sodass der Facebook-Mutterkonzern Meta einen nicht registrierten Nutzer, der lediglich einmal die Fanpage der Bundesregierung aufgerufen hat, auch dann wiedererkennen könnte, wenn dieser das ebenfalls zu Meta gehördende Instagram aufruft.

Solange Meta gegenüber Seitenbetreibern nicht offenlegt, welche Daten es genau erhebt und verarbeitet und zu welchem Zweck dies geschieht, wird der BfDI den Betrieb von Fanpages daher weiterhin als rechtswidrig beurteilen. Meta ist allerdings nicht daran gelegen, die Verarbeitungsvorgänge transparent zu machen – dies würde einen Teil des eigenen Geschäftsmodells offenlegen. Konsequenterweise müssen nach der Entscheidung des BfDI nun alle anderen Bundesministerien und obersten Bundesbehörden ihre Facebook-Seiten deaktivieren. Es bleibt abzuwarten, ob die Deaktivierung dieser Seiten hinreichenden Druck auf Meta ausübt, die Verarbeitungsvorgänge offenzulegen.

---

2 Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1 – zuletzt abgerufen am 14.03.2023.

III. Die Begründung des BfDI im Einzelnen

Neben einer Verletzung der Rechenschaftspflicht stützt der BfDI seine Entscheidung auf zwei weitere Erwägungen: Das Bundespresseamt verstoße zum einen gegen die DSGVO, weil für die Verarbeitung der Nutzerdaten keine wirksame Rechtsgrundlage bestünde. Zudem verstoße das Bundespresseamt außerdem gegen das 2021 in Kraft getretene TTDSG, weil Facebook ohne hinreichende Rechtsgrundlage Cookies auf den Rechnern der Endnutzer speichere.

1. Verstoß gegen das TTDSG

Seit Inkrafttreten des TTDSG ist das Setzen von Cookies auf den Rechnern der Nutzer stets einwilligungsbedürftig. Cookies sind seither also nur noch mit Nutzereinwilligung zulässig, unabhängig davon, ob mithilfe des Cookies auch personenbezogene Daten verarbeitet werden. Eine Einwilligung muss allerdings die Anforderungen der DSGVO erfüllen: Der Nutzer muss die Einwilligung also vor allem freiwillig und in informierter Weise abgeben. Wie oben gezeigt, setzt Meta sowohl bei registrierten Nutzern als auch bei nicht registrierten Nutzern diverse Cookies. Auch hierfür seien Meta und das Bundespresseamt nach Auffassung des BfDI gemeinsam verantwortlich. Nach Ansicht des BfDI erfolge die Einwilligung der Nutzer weder freiwillig noch informiert.

Meta holt die Nutzereinwilligung mithilfe eines Einwilligungsbanners ein, das den eigentlichen Seiteninhalt beim ersten Besuch der Seite überlagert. Dabei bleiben Nutzern zwei Auswahlmöglichkeiten: Sie können entweder „nur erforderliche Cookies erlauben“ oder „erforderliche und optionale Cookies erlauben“, wobei der Button für die erste Option mattgrau erscheint und der Button für die letztere Option mit strahlender blauer Farbe unterlegt ist. Dies suggeriere, dass Meta bei einem Klick auf „nur erforderliche Cookies erlauben“ tatsächlich nur solche Cookies setzt, die technisch für die Funktion der Seite unbedingt notwendig sind. Nach Auffassung des BfDI setzt Meta jedoch auch bei Auswahl dieser Option weiterhin Cookies, auf die technisch auch verzichtet werden könnte. Ein Klick auf „nur erforderliche Cookies erlauben“ bewirke vielmehr nur, dass Meta auf Drittanbieter-Cookies verzichte. § 25 des TTDSG verlange aber, dass bei einem Einwilligungsbanner schon auf der ersten Ebene ein Button für Nutzer zur Verfügung steht, mit dem alle außer den technisch unbedingt notwendigen Cookies abgelehnt werden können. Andernfalls könne die Einwilligung nicht mehr freiwillig erfolgen. Der BfDI rügt zudem die Nutzung sogenannter „deceptive design patterns“.[3] Durch die blaue Hinterlegung des Buttons „erforderliche und optionale Cookies erlauben“ sollten Nutzer subtil zur Wahl dieser Auswahlmöglichkeit bewegt werden. Die Einwilligung erfolge daher insgesamt nicht freiwillig.

Zudem erfolge die Einwilligung nicht informiert. Meta habe schon auf der ersten Ebene des Einwilligungsbanners darzulegen, zu welchem Zweck es die Cookies einsetzt und dass es gegebenenfalls Nutzerprofil erstellt. Eine solche Information unterbliebe aber.

2. Fehlende Rechtsgrundlage für die Datenverarbeitung

Das Bundespresseamt verstoße zudem gegen die DSGVO, weil für die Datenverarbeitung keine wirksame Rechtsgrundlage bestünde. Das Bundespresseamt könne die Datenverarbeitung weder auf eine wirksame Einwilligung der Nutzer stützten noch darauf, dass die Datenverarbeitung im öffentlichen Interesse liege. Auch die Einwilligung in die Datenverarbeitung erfolge wegen der Gestaltung des Einwilligungsbanners nicht freiwillig und informiert (s.o.). Die Datenverarbeitung liege auch nicht im öffentlichen Interesse. Zwar sei die Öffentlichkeitsarbeit von Behörden über soziale Netzwerke durchaus ein legitimes Anliegen und könne deswegen nach der DSGVO erlaubt sein, jedoch dürfe die Datenverarbeitung dann auch ausschließlich zu Zwecken der Öffentlichkeitsarbeit erfolgen. Die Datenverarbeitung auf Fanpages erfolge jedoch auch zu Zwecken, die lediglich Meta nutze und Metas Geschäftsmodell der Anzeigenwerbung verbessere.

IV. Fazit

Die Entscheidung des BfDI hat erhebliche Auswirkungen auf alle Behörden des Bundes und der Länder und damit insbesondere für Hochschulen. Für die Bundesbehörden ist nun klar, dass ein Weiterbetrieb der eigenen Facebook-Seiten eine Untersagung durch den BfDI zur Folge hätte. Denn der BfDI führt die

3 Zu „Dark Patterns“ und „Deceptive Design Patterns“: Palenberg, „Google brings light into the dark (pattern)“ in DFN-Infobrief Recht 02/23.

datenschutzrechtliche Aufsicht über sämtliche Behörden des Bundes, nicht nur über die Bundesregierung. Der BfDI begründet seine Entscheidung mit dem Kurzgutachten der Datenschutzkonferenz. In dieser sind auch sämtliche Landesdatenschutzbeauftragten vertreten. Diese führen die datenschutzrechtliche Aufsicht über die Landesbehörden. Es ist damit zu rechnen, dass die Landesdatenschutzbeauftragten künftig auch den Landesbehörden den Betrieb von Facebook-Seiten untersagen. Hiervon wären dann auch die meisten Hochschulen erfasst. Hochschulen sollten daher schon jetzt proaktiv in den Kontakt mit den Landesdatenschutzbeauftragten treten oder die eigenen Facebook-Seiten deaktivieren. Als Alternative bietet sich derzeit das dezentrale Netzwerk Mastodon an. Hier ist die Behörde alleinige datenschutzrechtliche Verantwortliche und kann über Mittel und Zwecke der Verarbeitung allein entscheiden. Diverse Behörden haben im vergangenen Jahr eine eigene Präsenz auf Mastodon aufgebaut.[4]

4 Ausführlich hierzu: Rennert, „Musk? Oh no. Mastodon!“ in DFN-Infobrief Recht 03/2023.

CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?

Die NIS-2-Richtlinie ist am 16. Januar 2023 in Kraft getreten und muss nun vom Gesetzgeber umgesetzt werden

von Nicolas John

Cyberkriminalität ist schon lange kein Novum mehr. Jährlich nehmen digitale Angriffe immer weiter zu und setzen Behörden und Unternehmen zunehmend unter Druck.[1] Auch die technischen Raffinessen der Angreifer entwickeln sich Jahr für Jahr immer weiter. Aus diesen Gründen sah sich der europäische Richtliniengeber berufen, zunächst mit der Netz- und Informationssicherheitsrichtlinie[2] (NIS-Richtlinie) in der Europäischen Union (EU) ein höheres Niveau an IT-Sicherheit zu schaffen. Doch die Umsetzung zeigte, dass es damit nicht genug ist. Es wurde Zeit für ein juristisches Update, die nun in Kraft getretene NIS-2-Richtlinie. Grund genug, um sich in diesem Beitrag einen Überblick über die Richtlinien und Umsetzungen zu verschaffen, die kommenden Änderungen unter die Lupe zu nehmen und damit einen kleinen Ritt durch das europäische Cybersicherheitsrecht zu wagen.

I. NIS-Richtlinie

Im Fokus des europäischen Gesetzgebers steht die Pflicht der Mitgliedsstaaten, eine nationalen Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen und eine sog. Kooperationsgruppe zu schaffen, welche die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten erleichtern soll. Außerdem soll für Notfälle ein Netzwerk an Computer-Notfallteams (CSIRTs) eingerichtet werden, welche die effiziente Zusammenarbeit zwischen den EU-Mitgliedsstaaten fördern und das Vertrauen stärken soll. Dies soll auch mithilfe der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) umgesetzt werden.

Darüber hinaus nimmt die NIS-Richtlinie auch Betreiber verschiedener „wesentlicher Dienste“ aus kritischen Versorgungssektoren in Anspruch. Gemeint sind damit IT-Dienste, welche bei einem Sicherheitsvorfall das öffentliche Leben erheblich einschränken würden und deren Aufrechterhaltung daher unerlässlich ist. Hierzu gehören die Energieversorgung, der Verkehrssektor, das Bankenwesen, Finanzmarktstrukturen, Gesundheitsdienstleister, die Trinkwasserlieferung und -versorgung sowie bestimmte Bereiche der digitalen Infrastruktur (v.a. Knotenpunktbetreiber, DNS-Diensteanbieter und TLD-Name-Registries). Neben den Betreibern der wesentlichen Dienste werden auch Anbieter digitaler Dienste wie Online-Marktplätze, Online-Suchmaschinen oder Cloud-Computing-Dienste von der NIS-Richtlinie umfasst. Dagegen sind Anbieter sozialer Netzwerke von dem Anwendungsbereich nicht

1 Zum Beispiel die vergangenen Emotet-Angriffe, hierzu Uphues, Der Feind in meinem Netz – Teil 1, DFN-Infobrief Recht 1/2020; Uphues, Der Feind in meinem Netz – Teil 2, DFN-Infobrief Recht 2/2020.

2 Richtlinie (EU) 2016/1148 zum Sicherheitsniveau von Netz- und Informationssystemen (NIS-Richtlinie), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=DE (zuletzt abgerufen am 16.3.2023).

erfasst. Auch kleine Unternehmen sollen nach den Richtlinienvorgaben nicht von den Regelungen erfasst werden.

Diese Betreiber und Anbieter sollen verschiedenen Sicherheitsanforderungen und Meldepflichten unterfallen. So schreibt die Richtlinie in Art. 14 den Betreibern der wesentlichen Dienste vor, dass sie unter Berücksichtigung des Stands der Technik „geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen [müssen], um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen". Im Falle eines Sicherheitsvorfalles, welcher erhebliche Auswirkungen auf die Verfügbarkeit des bereitgestellten Dienstes hat, haben die Betreiber unverzüglich eine Meldung bei der zuständigen Behörde[3] vorzunehmen.

Für die Anbieter digitaler Dienste verlangt die NIS-Richtlinie ähnliche Verpflichtungen. Art. 16 NIS-Richtlinie schreibt diesen ebenfalls die Vornahme geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen vor, um die Sicherheit der Dienste zu gewähren. Darüber hinaus unterfallen die Anbieter ebenfalls einer Meldepflicht, wenn es zu einem Sicherheitsvorfall kommt.

Um diese Anforderungen an die Betreiber und Anbieter zu koordinieren und zu überwachen, sollen die Mitgliedsstaaten entsprechende nationale Behörden und Anlaufstellen benennen.

Die NIS-Richtlinie trat 2016 in Kraft.

II. Umsetzung in Deutschland

Europäische Richtlinien haben in den Mitgliedsstaaten keine unmittelbare Rechtswirkung. Vielmehr bedarf es eines Umsetzungsakts durch den nationalen Gesetzgeber, welcher die Vorgaben einer Richtlinie in nationales Recht formuliert und welches dann unmittelbar Geltung findet. Die NIS-Richtlinie strebt dabei eine sog. „Mindestharmonisierung" an. Das bedeutet, dass die Mitgliedsstaaten zwar die Vorgaben der Richtlinie umsetzen müssen, aber darüber hinausgehende Regelungen, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll, durchaus möglich und zulässig sind.[4]

Europaweit soll so ein rechtlicher Mindeststandard geschaffen werden, der nationalrechtlich aber unterschiedlich ausgestaltet werden kann. Die NIS-Richtlinie musste bis Mitte 2018 von den Mitgliedsstaaten umgesetzt werden.

Der deutsche Gesetzgeber hatte schon vor Inkrafttreten der NIS-Richtlinie mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 eine Vielzahl der Vorgaben aus der NIS-Richtlinie erfüllt. Insbesondere die Pflichten von Unternehmen im Bereich kritischer Infrastrukturen, ihre informationstechnischen Systeme durch angemessene organisatorische und technische Vorkehrungen abzusichern und Meldepflichten der Unternehmen im Falle von Angriffen oder Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte der deutsche Gesetzgeber schon vor Inkrafttreten der NIS-Richtlinie reguliert.

Doch nicht alle Vorgaben aus der NIS-Richtlinie waren durch das damalige IT-Sicherheitsgesetz umgesetzt worden, es fehlten vor allem noch die Regelungen zu den Anbietern von digitalen Diensten. Die fehlenden Anpassungen wurden daher mit dem Umsetzungsgesetz der NIS-Richtlinie im Jahr 2017 vorgenommen, welche ab Mai 2018 Geltung in Deutschland fanden.

III. Änderungen der NIS-2-Richtlinie

Doch es zeigte sich schon bald nach Ablauf der Umsetzungsfrist, dass auf europäischer Ebene noch weiterer Anpassungsbedarf besteht. Die Richtlinie wurde in den Mitgliedstaaten sehr unterschiedlich umgesetzt. Insbesondere die „wesentlichen Dienste" wurden unterschiedlich definiert, wodurch die Adressaten der Pflichten in den Mitgliedstaaten stark divergierten. Auch die fehlende Überwachung der Umsetzung der Pflichten stellt in der Praxis einen Schwachpunkt der NIS-Richtlinie dar. Außerdem musste mit Blick auf die weiter wachsenden digitalen Bedrohungen festgestellt werden, dass das von der NIS-Richtlinie festgelegte Niveau der Cyberresilienz zu niedrig ist.

Um diese und einige weitere Schwachpunkte der NIS-Richtlinie auszubessern und auf die Zunahmen der weiter entwickelten Cyberangriffe zu reagieren, legte die Europäische Kommission einen Vorschlag zur Änderung der NIS-Richtlinie vor, welcher

3 In Deutschland ist hierfür das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig (s. II.).

4 Art. 3 NIS-Richtlinie.

nach der Einigung mit dem Europäischen Parlament und des Rates in der NIS-2-Richtlinie[5] mündete. Mit diesen Regelungen soll nun die Cybersicherheit in Europa modernisiert und auch im Anwendungsbereich erweitert werden.[6]

Die Änderungen betreffen daher verschiedene Bereiche. Insbesondere der Anwendungsbereich hat weitreichende Änderungen erfahren. So unterscheidet der europäische Richtliniengeber nun nicht mehr zwischen „wesentlichen" und „digitalen" Diensten, sondern nun zwischen „wesentlichen" und „wichtigen" Diensten.[7] Während aber trotz dieser begrifflichen Anpassung weiterhin alle bisherigen Adressaten von der Einordnung erfasst bleiben, kommen darüber hinaus nun neue Adressaten hinzu.

Zu den wesentlichen Diensten gehören Dienste, welche unter die im Anhang I aufgezählten „Sektoren mit hoher Kritikalität" fallen. So gehört nun auch der Sektor „Weltraum" zu den hochkritischen Sektoren, welcher Einrichtungen bezeichnet, die vom Boden aus weltraumbezogene Dienste erbringen. Aber auch der ursprüngliche Sektor der digitalen Infrastruktur wurde erheblich erweitert und ordnet nun z.B. Dienste des Cloud-Computing den besonders kritischen Infrastrukturen zu und erweitert den Sektor darüber hinaus um Anbieter von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Vertrauensdiensteanbietern und um Anbieter öffentlicher elektronischer Kommunikationsnetze bzw. dienste. Daneben gehören die Verwaltung von Informations- und Kommunikationstechnik-Diensten (IKT-Dienste) und auch die öffentliche Verwaltung nun ebenfalls zu den Sektoren mit hoher Kritikalität.

Wichtige Einrichtungen sind dagegen solche, die unter die in Anhang I oder II genannten Dienste fallen und aufgrund ihrer Größe nicht als wesentliche Einrichtung eingeordnet werden (zu dieser „size-cap-rule" unten gleich mehr). Anhang II der Richtlinie benennt die „sonstigen kritischen Sektoren". Während der europäische Richtliniengeber im Rahmen der digitalen Dienste noch immer Anbieter von Online-Marktplätzen und Suchmaschinen erfasst, zählen nun auch Anbieter von Plattformen für Dienste sozialer Netzwerke zu den erfassten Sektoren. Außerdem gehören auch Post- und Kurierdienste, die Abfallbewirtschaftung, Unternehmensbereiche mit Bezug zu chemischen Mitteln oder Lebensmitteln, das verarbeitende bzw. herstellende Gewerbe in bestimmten Bereichen wie z.B. Medizinprodukten und die Forschung zu den sonstigen kritischen Sektoren.

Mit der Erweiterung und Detaillierung dieses Adressatenkreises macht der europäische Richtliniengeber seine Ankündigung wahr, den Anwendungsbereich erheblich zu erweitern um eine breite Verbesserung der Cybersicherheit und resilienz in Europa zu erreichen.

Neu ist auch die oben schon erwähnte sog. „size-cap-rule". Diese legt nun als allgemeine Regel fest, dass große und mittlere Unternehmen, die in einem der oben genannten Sektoren tätig sind, von den Regelungen erfasst werden. Diese allgemeine Regelung korrigiert demnach den Schwachpunkt der ursprünglichen NIS-Richtlinie, welche es den Mitgliedsstaaten überließ, die Kriterien festzulegen, wann ein Unternehmen unter die Regelungen unterfiel. Nach der Definition einer in der Richtlinie benannten Empfehlung der Kommission haben mittlere Unternehmen weniger als 250 Mitarbeitende und einen Jahresumsatz von unter 50 Mio. Euro, bzw. eine Jahresbilanz von maximal 43 Mio. Euro. Kleine Unternehmen, welche nicht unter die Adressaten fallen sollen, haben maximal 50 Mitarbeitende und einen Jahresumsatz bzw. eine bilanz von unter 10 Mio. Euro.[8] Mit dieser Regelung werden die unterschiedlichen Umsetzungen der Mitgliedsstaaten verstärkt angeglichen. Dennoch lässt der Richtliniengeber weiterhin Ausnahmen in bestimmten Bereichen zu.

Erneuert wurden nun auch die Pflichten der betroffenen Einrichtungen. Die erfassten wesentlichen und wichtigen Einrichtungen müssen weiterhin ihre Präventionsmaßnahmen i.S.v. technischen und organisatorischen Maßnahmen wie z.B. Backups oder Verschlüsselungstechnologien vornehmen und dabei nationale und internationale Standards einhalten. Von diesen Pflichten sind in der NIS-2-Richtlinie nun auch ausdrücklich Lieferketten umfasst.

Weiterhin gelten umfangreiche Meldevorgaben im Falle von erheblichen Sicherheitsvorfällen. Dabei gilt ein Sicherheitsvorfall als erheblich, wenn er entweder „schwerwiegende

5 Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L1535&from=DE (zuletzt abgerufen am 16.3.2023).

6 Der Richtliniengeber stellt die Probleme der NIS-Richtlinie ausführlich in seinen Erwägungsgründen dar, vgl. ErwG 2 ff. NIS-2-Richtlinie.

7 S. Art. 3 NIS-2-Richtlinie.

8 Vgl. Empfehlung der Kommission 2003/361/EG.

Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann“.[9] Bezüglich dieser Meldepflichten macht der Richtliniengeber nun detailliertere Vorgaben als noch in der NIS-Richtlinie. So gibt der europäische Gesetzgeber ein gestuftes Meldevorgehen vor, nach dem nach spätestens 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfalls eine Frühwarnung abzugeben ist und nach spätestens 72 Stunden nach Kenntnisnahme des Sicherheitsvorfalls eine erste Bewertung einschließlich des Schweregrads und seiner Auswirkungen vorgenommen werden muss. Spätestens einen Monat nach Übermittlung der Bewertung des Falls muss außerdem ein Abschlussbericht vorgelegt werden.

Auch die Mitgliedsstaaten werden mehr in die Pflicht genommen. Insbesondere die Umsetzung der Cybersicherheitsstrategie und die Anforderungen an die nationalen Aufsichtsbehörden werden in der NIS-2-Richtlinie weiter vertieft. Außerdem gehört es nun zu den Aufgaben der Computer-Notfall-Teams, auf Anfrage proaktiv Schwachstellenscans vorzunehmen. Zudem soll die ENISA eine Schwachstellendatenbank aufbauen, um den Mitgliedsstaaten schnelleren Zugang zu den erforderlichen Informationen zu verschaffen. Neu sind auch mitgliedsstaatliche Peer-Reviews zur Cybersicherheit.

Verschärft wurden auch die Aufsichts- und Durchsetzungsbefugnisse der nationalen Behörden. Demnach sind neben Warnungen auch Zwangsgelder oder der Ausschluss von Leitungspersonen betroffener Einrichtungen möglich. Außerdem sind Maßnahmen wie Vor-Ort-Kontrollen, Stichproben, Sicherheitsaudits oder die Anforderung von Daten oder Zugängen möglich. Zudem wurden in der Richtlinie umfangreiche Vorgaben zu den Geldbußen festgelegt. So soll der nationale Gesetzgeber bei einem Verstoß einer wesentlichen Einrichtung gegen ihre Pflichten mindestens 10 Mio. Euro oder mindestens 2 % des Vorjahresumsatzes des betroffenen Unternehmens als Höchstbetrag in seiner Umsetzung festsetzen. Bei Verstößen von wichtigen Einrichtungen sollen die Höchstbeträge mindestens 7 Mio. Euro oder 1,4 % des Vorjahresumsatzes im nationalen Umsetzungsgesetz betragen.

Die neue NIS-2-Richtlinie ist am 16. Januar 2023 in Kraft getreten. Die Mitgliedsstaaten haben nun bis Oktober 2024 Zeit, die Vorgaben in nationales Recht umzusetzen.

9 Art. 23 Abs. 3 NIS-2-Richtlinie.

IV. Umsetzungsbedarf in Deutschland

Während die europäischen Institutionen die Überarbeitung der NIS-Richtlinie in die Wege leiteten, war der deutsche Gesetzgeber ebenfalls nicht untätig. Schon vor Inkrafttreten der NIS-2-Richtlinie wurde das IT-Sicherheitsgesetz überarbeitet und trat in seiner neuen Form 2021 in Kraft.

Die Änderungen des sog. „IT-Sicherheitsgesetzes 2.0“ betrafen vor allem die Pflichten von Betreibenden kritischer Infrastrukturen (KRITIS-Betreiber) wie z.B. Energie- oder Telekommunikationsunternehmen und Unternehmen im besonderen öffentlichen Interesse (UNIBÖFI), z.B. Unternehmen der Rüstungs- oder Chemieindustrie aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Der deutsche Gesetzgeber hatte schon in diesem Gesetzgebungsakt festgelegt, dass auch Zulieferer in den Anwendungsbereich der neuen Regelungen fallen können.

UNIBÖFIs müssen nach diesen Regelungen eine Selbsterklärung über ihre Maßnahmen zum Schutz der IT-Sicherheit vornehmen und sich beim BSI registrieren. In diesem Gesetzesakt wurde aber auch der Begriff der KRITIS-Betreiber um beispielsweise die Abfallentsorgung erweitert. Außerdem müssen sich KRITIS-Betreiber ebenfalls beim BSI registrieren, den Einsatz bestimmter IT-Produkte anzeigen und Programme für die Erkennung von Cyberangriffen verwenden. Im Falle eines Sicherheitsvorfalls müssen beide Kategorien der Betreiber dem BSI den Vorfall melden und entsprechende Daten zur Verfügung stellen.

Politisch umstritten war insbesondere die Regelung über die Verwendung sog. „kritischer Komponenten“, welche der Gesetzgeber bestimmen kann. Grund für die Diskussionen war der Umgang mit Bauteilen des chinesischen IT-Unternehmens „Huawei“. Nach dem BSIG kann der Einsatz solcher Komponenten verboten werden, wenn die Befürchtung besteht, dass die Verwendung die öffentliche Sicherheit und Ordnung beeinträchtigen kann. Dies kann z.B. der Fall sein, wenn der Hersteller von der Regierung eines Drittstaates kontrolliert wird. Der Einsatz dieser kritischeren Komponenten muss von dem Betreiber vor der Verwendung beim BSI angezeigt werden.

Durch diese umfangreiche Modernisierung der deutschen Sicherheitsgesetze erfüllt der Gesetzgeber schon Teile der NIS-2-Richtlinie und geht partiell wieder darüber hinaus. Allerdings fehlen auch noch Umsetzungsvorgaben, beispielsweise einige

der in der Richtlinie benannten Sektoren wie die Raumfahrt, die öffentliche Verwaltung oder die Forschung. Soweit die Vorgaben der Richtlinie im deutschen Recht noch nicht umgesetzt sind, wird der Gesetzgeber mit einem „IT-Sicherheitsgesetz 3.0“ die erforderlichen Änderungen vor Ablauf der Umsetzungsfrist vornehmen müssen.

V. Auswirkungen in der Praxis und Fazit

Schon jetzt sind viele Unternehmen in Deutschland von den Pflichten aus der NIS-Richtlinie und den erweiterten Vorgaben des IT-Sicherheitsgesetzes 2.0 betroffen.[10] Doch dass die Umsetzung der Vorgaben in den Unternehmen dringend erforderlich ist, zeigen die regelmäßigen Cyberangriffe auf verschiedenste Einrichtungen. Die Erhöhung des Schutzniveaus in der Cybersicherheit ist daher von großer Bedeutung.

Aus diesen Gründen wird auch die vollständige Umsetzung der NIS-2-Richtlinie als zu erwartendes IT-Sicherheitsgesetz 3.0 vor allem für Unternehmen, aber auch für entsprechende öffentliche Einrichtungen große Herausforderungen bedeuten. Zwar sieht die NIS-2-Richtlinie für Einrichtungen der öffentlichen Verwaltung Einschränkungen vor,[11] allerdings wird dem deutschen Gesetzgeber ein großer Spielraum eingeräumt, welche Einrichtungen der öffentlichen Verwaltung schließlich unter den Anwendungsbereich des Umsetzungsgesetzes fallen sollen.[12]

Nicht alle Bereiche der Forschung werden sich ganz neu mit den Anforderungen an die Cybersicherheit konfrontiert sehen. Schon jetzt fallen z.B. Universitätskliniken als Gesundheitseinrichtungen unter den Katalog der derzeit geltenden BSI-Kritis-Verordnung. Dennoch wird für viele Forschungseinrichtungen und Hochschulen erstmalig neben dem Sektor der öffentlichen Verwaltung insbesondere der neue Sektor der Forschung von Relevanz sein. Forschungseinrichtungen werden in der NIS-2-Richtlinie als Einrichtung definiert, „deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt.“ Letztendlich bleibt hierbei abzuwarten, welche Einrichtungen vom IT-Sicherheitsgesetz 3.0 am Ende tatsächlich unter den Sektoren der öffentlichen Verwaltung oder der Forschung erfasst werden. Auch in Bezug auf Bildungseinrichtungen lässt die Richtlinie den Mitgliedsstaaten Freiheiten. Insoweit obliegt es auch der Entscheidung des deutschen Gesetzgebers, Bildungseinrichtungen in den Anwendungsbereich einzubeziehen, insbesondere, wenn sie kritische Forschungstätigkeiten durchführen.[13]

Der Forschungsbereich wird in der Richtlinie auch noch anderweitig relevant: denn die Richtlinie sieht im Rahmen der Vorgaben zur nationalen Cybersicherheitsstrategie vor, dass Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit umfasst werden müssen.[14] Außerdem müssen Hochschul- und Forschungseinrichtungen bei der Entwicklung, der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur unterstützt werden.[15]

Letztendlich stellt die NIS-2-Richtlinie eine sehr viel stärkere Konkretisierung und Erweiterung der bisherigen Vorgaben der NIS-Richtlinie dar. Der europäische Gesetzgeber zeigt seinen Willen, die Cybersicherheit in Europa zu vereinheitlichen und durch eine enge Zusammenarbeit der Mitgliedsstaaten zu verbessern. Ob ihm das schlussendlich gelingt, hängt von den nun zu erwartenden Umsetzungsgesetzen der Mitgliedsstaaten ab.

10 Die erfassten Einrichtungen sind in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) benannt.

11 Vgl. Art. 3 Abs. 1 lit. d, Art. 2 Abs. 2 lit. f NIS-2-Richtlinie.

12 Art. 2 Abs. 2 lit. f, Abs. 5 lit. a NIS-2-Richtlinie.

13 Art. 2 Abs. 5 lit. b NIS-2-Richtlinie.

14 Art. 7 Abs. 1 lit. f NIS-2-Richtlinie.

15 Art. 7 Abs. 1 lit. g NIS-2-Richtlinie.

Doppelgänger Delights: How to prevent the perfect impersonation (Or Not)

Rechtliche und praktische Hürden bei der Identifizierung des Auskunftsanspruchstellers

Von Ole-Christian Tech

Die Reichweite des Auskunftsanspruchs der betroffenen Person nach Art. 15 Datenschutzgrundverordnung (DSGVO) war zuletzt vielfach Gegenstand der Diskussion in Praxis und Rechtsprechung, welche rechtlichen und praktischen Fallstricke sich jedoch im Alltag bei der Bearbeitung von Anfragen der betroffenen Person ergeben, wird dabei nicht immer ausreichend beleuchtet.

Denn ob Call ID-, E-Mail-, oder URL-Spoofing, das Risiko von impersonation steigt, wenn personenbezogene Daten die verantwortliche Stelle verlassen. Hierzu bedarf es einer sicheren Identifizierung des Anspruchsstellers als betroffene Person.

I. Der Status Quo:

Art. 15 DSGVO verlangt von dem Verantwortlichen, dass er auf Anfrage der betroffenen Person bestimmte Informationen über die Verarbeitung ihrer Daten bereitstellt (sog. Passive Informationspflicht). Dieses Recht auf Auskunft ergänzt die Pflichten des Verantwortlichen, aktiv Informationen gemäß Art. 13 und Art. 14 DSGVO bereitzustellen. In Absatz 1 und Absatz 2 ist ein allgemeines Recht auf Auskunft definiert, das sich auf die von dem Verantwortlichen verarbeiteten Daten und bestimmte Metainformationen bezieht. Außerdem hat die betroffene Person gemäß Absatz 3 das Recht auf eine Kopie ihrer Daten.[1]

Aber wie sieht die rechtssichere Umsetzung in der Praxis aus? Wird das Auskunftsbegehren nicht oder zu spät beantwortet, ist das ein Verstoß gegen Art. 15 DSGVO. Werden die angefragten personenbezogenen Daten aber einem Unberechtigten zugänglich gemacht, stellt dies als Verarbeitung ohne Rechtsgrundlage einen Verstoß gegen Art. 6 Abs. 1 DSGVO dar.
Wird z.B. ein Datenschutzbeauftragter, IT-Mitarbeiter oder Sachbearbeiter mit Bearbeitung des Auskunftsanspruchs betraut, stellen sich zahlreiche Fragen: Kann er sicher sein, dass die anfragende Person auch tatsächlich der Betroffene ist? Wie viele personenbezogenen Daten darf und muss er von dem Anspruchssteller verlangen um ihn zu identifizieren?

Diese Fragen sollen anhand folgender Szenarien näher beleuchtet werden.

II. Szenario 1 „Data-Breach“

Eine Situation wie sie jederzeit und überall in datenverarbeitenden Organisationen vorkommen kann: Der Verantwortliche gibt personenbezogene Daten-oftmals versehentlich- an Unberechtigte heraus. Der Standardfall hierzu wäre der offene E-Mailverteiler.

Was jedoch, wenn der Verantwortliche gezielt getäuscht wird, indem ein Doppelgänger des Berechtigten sich als dieser ausgibt und ein Auskunftsbegehren stellt?

1 Siehe bereits Voget, Daten-Blackout! in DFN-Infobrief Recht 03/2023.

III. Szenario 2 „Verweigerung des Auskunftsbegehrens“

Wann darf ein Begehren verweigert werden?

Wenn der Verantwortliche nicht in der Lage ist, die betroffene Person zu identifizieren, dann ist er nach Art. 11 Abs. 2 Satz 2 DSGVO nicht zu einer Auskunft verpflichtet. Dies gilt jedoch nur dann, wenn der Verantwortliche tatsächlich nachweisen kann, dass es ihm unmöglich ist die Person zu identifizieren. Wenn der Betroffene dann von sich aus weitere Informationen bereitstellt, die eine Identifizierung ermöglichen, muss der Verantwortliche diese entgegennehmen und zur Identifizierung und Bearbeitung des Auskunftsanspruchs verwenden, schließlich hat der Betroffene stets die Datenhoheit.[2]

Nach Art. 12 Abs. 6 DSGVO kann der Verantwortliche bei begründeten Zweifel an der Identität der natürlichen Person, die den Antrag gemäß Art 15 DSGVO stellt zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Die Formulierung „bei begründeten Zweifeln“ und „erforderliche Informationen“ zeigen auch hier, dass der Verantwortliche keine unangemessen hohen Anforderungen an die Identifizierung stellen darf, um etwa von unliebsamen Auskunftsbegehren abzuschrecken, da sonst ein Verstoß gegen Art. 12 Abs. 1 Satz 1 DSGVO iVm. Art. 15 DSGVO droht.

IV. Szenario 3 „Exzessive Verifizierung“

Die Identitätsüberprüfung ist exzessiv, wenn der Verantwortliche für die Identifikation unnötige oder irrelevante Informationen abfragt. Dies kann einer bloßen Neugier des Verantwortlichen geschuldet sein, wird aber in der Regel an Unwissenheit oder Fahrlässigkeit des Verantwortlichen liegen, was dann zu starren und unangepassten Leitfäden für die Bearbeitung von Auskunftsbegehren führt.

Wenn sich das Auskunftsbegehren etwa gegen den Betreiber einer Plattform richtet, auf dem der Betroffene nur mit Pseudonym registriert ist, kann ein amtliches Ausweisdokument nichts zur Identifizierung des Betroffenen beitragen. Eine Anforderung eines solchen Dokuments durch den Verantwortlichen kann sich daher nicht auf Art. 12 Abs. 6 DSGVO stützen und wäre exzessiv.

Welche Arten der Identifizierung in der Praxis Anwendung finden und wie diese rechtssicher umgesetzt werden können, soll die folgende Auswahl verdeutlichen.

V. Eine Auswahl an Möglichkeiten der Identifizierung

1. Cookies

Diese Art der Identifizierung bietet sich besonders dort an, wo dem Verantwortlichen keine Kontaktdaten wie etwa eine E-Mailadresse vorliegen. In der Praxis ist dies regelmäßig bei Onlinewerbeanbietern der Fall, da Cookies hier oftmals der einzige Indikator für den Geräteinhaber und damit den Betroffenen sind.

2. Login-Daten

Hierbei handelt es sich um eine der am häufigsten verwendeten Methoden der Identifizierung. Der Betroffene meldet sich mit seinen Login-Daten auf der Plattform (dem Intranet, sozialen Netzwerk, Selbstverwaltungsbereich etc.) an und stellt dann auf einer hierfür konzipierten Seite den Auskunftsanspruch an den Verantwortlichen. Diese Art der Identifizierung ist nicht nur verhältnismäßig sicher, sondern kommt auch ohne weitergehende personenbezogene Daten des Betroffenen aus und ist im Übrigen auch bereits vom Gesetzgeber anerkannt wie Erwägungsgrund 63 Satz 4 zur DSGVO zeigt, in dem es heißt: *„Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.“*

Zudem lässt sich diese Art der Identifizierung modular erweitern, um ein höheres Sicherheitsniveau zu erreichen, etwa durch eine 2-Faktor Authentifizierung mittels Authentifikator App oder SMS TAN.

2 Das ergibt sich aus Erwägungsgrund 57 DSGVO.

3. Hinterlegte E-Mailadresse

Auch dieser Ansatz wird häufig in der Praxis verwendet. Der Betroffene weist hiermit in der Sache nach, dass er Zugriff auf das Postfach der bei dem Verantwortlichen hinterlegten Mailadresse hat. Diese Art der Identifikation ist ähnlich sicher wie die via Login-Daten.

4. Betroffenenspezifische Informationen

Betroffenenspezifische Informationen umfassen alle Angaben, die zur eindeutigen Identifizierung des Betroffenen dienen können wie z.B. Rechnungsnummern oder Antworten auf Sicherheitsfragen. Das Sicherheitsniveau dieser Methode hängt maßgeblich von der Art der angeforderten Informationen ab. So sollte davon abgesehen werden, nicht änderbare Informationen zur Identifizierung zu verwenden (z.B. den Geburtsort), da im Fall eines Bekanntwerdens dieser Informationen aus einem Datenleck an anderer Stelle diese Angaben beliebig lange von Doppelgängern für missbräuchliche Auskunftsbegehren verwendet werden können.

Bei dieser Identifizierung sollte noch auf das besondere Risiko sog. Daisy Chains[3] hingewiesen werden. Hierbei verwendet ein Doppelgänger ihm bekannte personenbezogene Daten, um sich bei einem Verantwortlichen als vermeintlicher Betroffener zu identifizieren und ein Auskunftsbegehren zu stellen, bei dem er dann weitergehende personenbezogene Daten erlangt. Diese verwendet er dann beim nächsten Verantwortlichen und arbeitet sich so entlang der Kette (Daisy Chain) immer weiter vor und erlangt jedes Mal weitere, ggf. sensiblere personenbezogene Daten.

Auf diese Weise wird der einmalige Data Breach sozusagen „gehebelt". Diese Problematik lässt sich unterbinden, indem neben der Adresse, von der die Anfrage stammt zugleich auf eine hinterlegte andere Kontaktmöglichkeit des Betroffenen geantwortet wird. Wenn der Doppelgänger also eine kompromittierte oder frei erfundene Mailadresse des Betroffenen verwendet, ergeht so eine Antwort auch an den Betroffenen, die ihn im Idealfall alarmiert, sodass die Kette durchbrochen werden kann bevor sensible personenbezogene Daten herausgegeben werden.

5. Ausweisdokumente

Ebenfalls praxisrelevant ist die Identifizierung durch amtliche Ausweise wie den Personalausweis. In der Regel wird ein Scan des Personalweises per Mail verlangt, wobei damit in der Sache der Besitz dieses Dokuments nachgewiesen wird. Wie sicher diese Methode ist, wird sehr unterschiedlich bewertet. In der Literatur wird oft kritisiert, dass bei einem Scan die Qualität der Aufnahme häufig zu schlecht wäre, wichtige Erkennungsmerkmale eines echten Ausweisdokuments wie Wasserzeichen seien nicht erkennbar und der Verantwortliche oft nicht versiert genug im Umgang mit Echtheitsprüfungen von Ausweisdokumenten, sodass ein erhebliches Risiko bestünde, dass die Vorlage eines gefälschten Ausweises durch den Doppelgänger unerkannt bleibt.

Für Deutschland hat sich der Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bisher für eine Identifizierung durch amtliche Ausweise ausgesprochen, allerdings mit der Einschränkung, dass nur Daten wie Name, Anschrift, Geburtsdatum und Gültigkeitsdauer auf der Abbildung enthalten sind und alle anderen Daten wie Ausweisnummer, Lichtbild, persönliche Merkmale oder die Staatsangehörigkeit geschwärzt bzw. unkenntlich gemacht werden.[4]

Aufgrund des hohen Missbrauchspotentials von Ausweisdokumenten sollte mit dieser Art der Identifikation jedenfalls sparsam umgegangen werden, um nicht ein unverhältnismäßiges Risiko einzugehen.

6. Kontrollanrufe

Eine eher selten genutzte Art der Identifizierung ist der Kontrollanruf. Dieser ist regelmäßig sicher, wobei es Ausnahmen geben kann, wenn Telefonanschlüsse gemeinsam genutzt werden. Ein (zugegeben eher veraltetes) Beispiel wäre etwa der gemeinsam genutzte Festnetzanschluss in der studentischen Wohngemeinschaft.

Zu beachten ist jedoch, dass diese Methode nur dann sicher ist, wenn der Kontrollanruf von dem Verantwortlichen auf eine hinterlegte Telefonnummer aus erfolgt. Andersherum würde ein

3 engl. ‚Gänseblümchenkette'.

4 Siehe hierzu https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html , zuletzt abgerufen am 09.02.2023.

Anruf vom (vermeintlichen) Betroffenen sonst das Risiko des Telefonnummer-Spoofings bergen.

7. Videoidentifikation

Die Videoidentifikation vereint die Vorteile verschiedener bereits genannter Methoden. Sie ist einerseits eine Ausweiskontrolle, die zahlreiche Probleme der oben beschriebenen Möglichkeiten (schlechte Sichtbarkeit von Wasserzeichen etc.) umgeht und zugleich ein Kontrollanruf, der auch hier das Risiko bei gemeinsam genutzten Telefonanschlüssen umgeht.

Er ist jedoch für den Verantwortlichen und den Betroffenen relativ aufwändig und erfordert zudem Personal, das mit der Prüfung von Ausweisdokumenten vertraut ist.

VI. Handlungsempfehlung und Bedeutung für Hochschulen

Hochschulen und Forschungseinrichtungen sind als Verantwortliche oftmals selbst Adressaten der Ansprüche auf Auskunft ihrer Beschäftigten (als Arbeitgeber), Studenten (als Bildungseinrichtung) oder z.B. Studienteilnehmer (als Forschungseinrichtung). Dabei ist der rechtmäßige Umgang mit personenbezogenen Daten immanent und damit Verstöße gegen die DSGVO und damit verbundene Bußgelder bzw. Schadenersatzansprüche ein ernstzunehmendes Risiko.

Welche Anforderungen sind nun konkret an den Verantwortlichen zu stellen? Die unbefriedigende Antwort hierzu lautet: Es kommt drauf an. Die DSGVO ist von verschiedenen Grundsätzen geprägt, die hier miteinander je nach Einzelfall in Einklang gebracht werden müssen. Art. 5 Abs. 1 lit. c) DSGVO etwa verlangt die Datenminimierung und Art. 5 Abs. 1 lit. d) DSGVO die Speicherbegrenzung. Diese Grundsätze schützen vor allem gegen „exzessive Verifizierung“. Art. 5 Abs. 1 lit. d) DSGVO hingegen verlangt geeignete technische und organisatorische Maßnahmen, um angemessene Sicherheit vor unbefugter oder unrechtmäßiger Verarbeitung (also auch: Offenlegung) zu schaffen, wie in Szenario 1 aufgezeigt.

Im Ergebnis geht es also wieder einmal um die Verhältnismäßigkeit. Es ist erforderlich, einen dynamischen Rahmen je nach Umfeld, Größe und involvierten Daten anzuwenden. Identifizierung mittels Ausweisdokumenten kann für einfache Newsletter Anbieter bereits exzessiv sein, während eine Verifizierung per E-Mailadresse bei sensiblen Gesundheitsdaten fahrlässig sein kann.

Kurzbeitrag: Kleines Versehen, großer Schaden

OLG Hamm zu Schadensersatzansprüchen wegen rechtswidriger Offenlegung von personenbezogenen Gesundheitsdaten unter Verstoß gegen Art. 9 DSGVO

von Johannes Müller

Das Oberlandesgericht (OLG) Hamm musste sich in seinem Urteil (Az. 11 U 88/22) mit einem Datenschutzverstoß aufgrund eines versehentlichen E-Mail-Versands von personenbezogenen Daten beschäftigen. Hierbei hat es zu einigen dogmatischen Fragestellungen rund um datenschutzrechtliche Schadensersatzansprüche Stellung bezogen.

I. Datenverstoß durchs Impfzentrum

Dem Urteil liegt folgender Sachverhalt zugrunde: Ein Impfzentrum musste aufgrund einer Änderung der Öffnungszeiten die Termine von 1.200 Personen verschieben. Die hierzu erforderlichen Daten exportierten Mitarbeiter des Impfzentrums aus einer Excel-Liste der Kassenärztlichen Vereinigung Nordrhein. Versehentlich versandten sie die Excel-Liste als Anhang an die 1.200 Empfänger mit. Diese enthielt personenbezogene Daten von rund 13.000 Personen. Die Daten setzten sich zusammen aus den Namen, den Geburtsdaten, den Anschriften der zu impfenden Personen und Angaben zum vorgesehen Impfstoff und zur Frage, ob es sich um die erste oder zweite Impfung handelt. Teilweise enthielt die Liste auch Telefonnummern und E-Mail-Adressen. Der Kläger war Empfänger einer solchen Mail und auch selbst Betroffener. Von ihm wurde auch die Telefonnummer und E-Mail-Adresse veröffentlicht. Er verlangte vom dem Impfzentrum hierfür Schadensersatz.

II. Urteil des OLG Hamm

Das Gericht setzt sich zunächst mit einem Schadensersatzanspruch aus Art. 82 DSGVO auseinander. Dieser setzt eine Verletzung der DSGVO voraus, die laut dem OLG in dreierlei Hinsicht vorliege. Zuerst fehle für die Verarbeitung, also das Verschicken der Excel-Liste mit personenbezogenen Daten, die notwendige Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Zudem habe der Verantwortliche durch den Versand gegen die Anforderungen der angemessenen Sicherheit der personenbezogenen Daten verstoßen und damit Art. 5 Abs. 1 lit. f DSGVO verletzt. Zuletzt habe die Excel-Tabelle auch Angaben über bereits erfolgte Impfungen und den gewählten Impfstoff enthalten. Daher seien auch entgegen Art. 9 Abs. 1 DSGVO Gesundheitsdaten verarbeitet worden. Das fahrlässige Verhalten der zuständigen Mitarbeiter könne den Betreibern des Impfzentrums zugerechnet werden.

Zudem beschäftigt sich das Gericht mit den weiteren Voraussetzungen des Art. 82 DSGVO neben dem Vorliegen eines Datenschutzverstoßes. Hier stellen sich schwierige Fragen zum immateriellen Schadensersatz bei DSGVO-Verletzungen.[1] Zunächst lehnt das Gericht eine Erheblichkeitsschwelle für einen immateriellen Schadensersatz ab, auch eine schwerwiegende Persönlichkeitsrechtsverletzung müsse nicht vorliegen. Es genüge bereits der Verlust der Kontrolle über die personenbezogenen Daten. Unerheblich sei zudem, dass der Kläger selbst in den sozialen Medien seine Impfungen öffentlich gemacht hatte, denn diese Informationen sei nur einem vom Kläger ausgewählten Personenkreis zugänglich. Die Daten in der Excel-Tabelle seien zudem deutlich umfassender. Zuletzt bestätigt das OLG die von

1 Vgl. hierzu Uphues, Steh zu deinen Fehlern oder es kommt dir teuer zu stehen, DFN-Infobrief Recht 04/2021; Müller, Morgen Kinder werden wir klagen, DFN-Infobrief Recht 12/2022; Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

der Vorinstanz vorgenommene Festsetzung des Schadens auf 100€. Es wägt hierzu umfassend alle Umstände des Einzelfalls ab: Zwar handele es sich um einen umfassenden Datensatz, der an viele Personen gesendet worden sei. Andererseits seien diese Daten aber auch der Sozialsphäre des Klägers zuzuordnen, die Beklagte habe eine öffentliche Aufgabe erfüllt und nicht gewinnorientiert gehandelt, es liege lediglich Fahrlässigkeit seitens der Mitarbeiter vor und die Beklagte habe alles unternommen, um möglichst viele E-Mails zurückzurufen. Angesichts dessen, dass insgesamt 13.000 Personen schadenersatzberechtigt sind, entfalte eine Summe von 100€ auch eine hinreichende Abschreckungswirkung.

III. Relevanz für Hochschulen und andere wissenschaftliche Einrichtungen

Das Urteil kann als Beispiel dafür dienen, wie ein kleiner faux pas in den Betriebsabläufen erhebliche datenschutzrechtliche Konsequenzen für den Verarbeiter entfalten kann. Als Sanktion von Datenschutzverletzungen kommen Schadensersatzansprüchen eine zunehmend größere Bedeutung zu. Ob sich hierbei die Ansicht des OLG Hamm durchsetzen wird, dass keine erhöhten Voraussetzungen an die Annahme immaterieller Schäden zu stellen sind, kann jedoch bezweifelt werden. Der Generalanwalt hat sich zuletzt gegenteilig geäußert.[2] Dennoch stellt das Urteil etwaige Haftungsrisiken für Datenschutzverstöße unter Beweis. Zwar mag die Summe von 100€ nicht besonders hoch wirken. Berücksichtigt man aber die enorm hohe Anzahl der Anspruchsberechtigten, ergibt sich eine mögliche erhebliche finanzielle Belastung. Wichtig ist auch, dass sich der Verantwortliche nicht aus seiner Schadensersatzpflicht befreien kann, indem er darauf verweist, er habe seine Mitarbeiter hinreichend instruiert und überwacht. Das Verschulden der Mitarbeiter wird dem Verantwortlichen zugerechnet. Auch Hochschulen und anderen wissenschaftlichen Einrichtungen ist damit anzuraten, das eigene Personal mit größter Vorsicht darin zu unterweisen, wie mit personenbezogenen Daten umzugehen ist. Nur so lassen sich Fälle wie der vorliegende effektiv vermeiden.

2 Müller, Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

Impressum

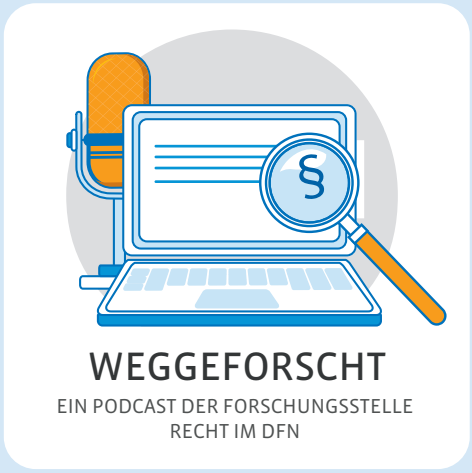
Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

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 WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, 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