infobrief recht DFN

4 / 2020
April 2020

Zu Risiken und Nebenwirkungen fragen Sie Ihren Arzt oder Verantwortlichen

Zur datenschutzrechtlichen Relevanz von Teletherapie

Admin-C – Sag beim Abschied leise Servus

Zur haftungsrechtlichen Verantwortung des Admin-C nach dem Inkrafttreten der DSGVO

Möge die Firewall mit dir sein

Zum Datenschutz bei der Einrichtung von (Viren-) Schutzsystemen im betrieblichen Netzwerk

Zu Risiken und Nebenwirkungen fragen Sie Ihren Arzt oder Verantwortlichen

Zur datenschutzrechtlichen Relevanz von Teletherapie

von Owen Mc Grath

Durch die momentane Bedrohung des Coronavirus ist der Einsatz von technischen Hilfsmitteln in der medizinischen Behandlung zur Vermeidung von unmittelbarem Patientenkontakt von zentraler Bedeutung. Trotz der prekären Umstände ist das Datenschutzrecht, welches bereits im Grundgesetz durch das Institut der „informationellen Selbstbestimmung“ (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) Anknüpfung findet, bei solchen Vorgängen nicht außer Acht zu lassen.

I. Einordnung

Als Teil der Telemedizin bezeichnet Teletherapie die Behandlung von Patienten unter Einsatz von Fernkommunikationsmitteln. Der Begriff setzt sich zusammen aus den Wörtern Telematik und Therapie. Was früher gelegentlich durch Telefongespräche erledigt wurde, geschieht heutzutage primär durch den Einsatz von Videotelefondiensten. Umfasst von der Teletherapie sind die Teleberatung, Teleoperation, Televisite, Telebetreuung, Telenachsorge, Telebehandlungspflege und das Telemonitoring. Es können beispielsweise Bewegungs- oder Sprachübungen unter ärztlicher Überwachung durch Verwendung von Webcams durchgeführt werden. Trotz der vielseitigen Einsatzmöglichkeiten kann Teletherapie eine unmittelbare Behandlung in vielen Bereichen nicht ersetzen. In der Radiologie zum Beispiel ist eine Untersuchung in der Praxis oder Klinik unter Einsatz von Geräten von zentraler Bedeutung und auf die Ferne so nicht durchzuführen.

Der Teletherapie vorgeschaltete telemedizinische Maßnahmen werden als Telediagnostik bezeichnet. Weiterhin umfasst die Telemedizin die Bereiche der Telerehabilitation und Teleprävention. Allen Bereichen ist der Einsatz von Fernkommunikationsmitteln zur Überwindung von zeitlichen und räumlichen Grenzen gleich. Dieser Einsatz bietet die Vorteile der Zeit- und Aufwandsersparnis. An- sowie Abfahrtswege und -mühen entfallen. Eine regelmäßigere Versorgung der Patienten wird erleichtert.

Akut führt auch die Gefahr einer Virusinfektion zum vermehrten Einsatz von Fernkommunikationsmitteln in der medizinischen Behandlung von Patienten. Sowohl der Schutz vor Ansteckung der Therapeuten als auch der Patienten wird durch den Einsatz von Teletherapie gewährleistet.

Telemedizin und Teletherapie im speziellen führen zwangsläufig zu einer Verarbeitung von personenbezogenen Daten und insbesondere auch Gesundheitsdaten (sog. sensible Daten).

Jede Verarbeitung von personenbezogenen Daten stellt einen datenschutzrechtlich relevanten Vorgang dar. Für den Bereich der Teletherapie ist im Folgenden die Vereinbarkeit mit dem Datenschutzrecht zu klären.

II. Grundsätzliche Anforderungen des Datenschutzrechts

Für jede Verarbeitung personenbezogener Daten sind bestimmte Grundsätze zu beachten. Diese sind in Art. 5 Datenschutz-Grundverordnung (DSGVO) geregelt. Zu den Grundsätzen zählen die Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit der Verarbeitung. Ferner sind insbesondere auch die Informationspflichten (Art. 13, 14 DSGVO) und Rechte der Betroffenen (Art. 15 ff. DSGVO) zu beachten. Diese Grundlagen verpflichten beispielsweise schon zum Einsatz

von verschlüsselten Verbindungen im Bereich der Teletherapie. Die zentralsten Grundsätze werden im Folgenden erörtert.

III. Die Verarbeitung von Gesundheitsdaten

Nach dem Grundsatz der Rechtmäßigkeit der Verarbeitung muss ein Erlaubnistatbestand zur Verarbeitung der personenbezogenen Daten vorliegen (Art. 6 DSGVO). Erlaubt sein kann eine Verarbeitung beispielsweise dann, wenn das Einverständnis des Betroffenen vorliegt (Art. 6 Abs. 1 S. 1 lit. a DSGVO) und die weiteren Bedingungen für eine wirksame Einwilligung vorliegen (Art. 7 DSGVO). Weitere Besonderheiten ergeben sich aber vor allem auch bei der Verarbeitung von Gesundheitsdaten. Diese werden im Erwägungsgrund 35 zur DSGVO näher beschrieben und definiert als Daten, „die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen".

Gesundheitsdaten zählen zu den sensiblen Daten im Sinne des Art. 9 DSGVO. Eine Verarbeitung von sensiblen Daten ist nach Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Ausnahmen von diesem Verbot werden in Art. 9 Abs. 2 DSGVO normiert.

Im Rahmen von Teletherapie werden vornehmlich personenbezogene Daten in Form von Gesundheitsdaten erhoben und verarbeitet. Die Verarbeitung muss zur Rechtsmäßigkeit also nicht bloß dem Standard des Art. 6 Abs. 1 DSGVO genügen, sondern auch dem strengeren Maßstab des Art. 9 Abs. 2 DSGVO.

Abseits der EU-weit geltenden Regelungen der DSGVO können auch gesetzliche Regelungen auf Bundesebene (durch das Bundesdatenschutzgesetz (BDSG)), sofern eine sog. Öffnungsklausel in der DSGVO besteht, Ausnahmen und Erlaubnistatbestände normieren. Solche Öffnungsklauseln finden sich unter anderem in Art. 9 Abs. 2 lit. b, g, i und h i.V.m. Abs. 3 DSGVO. Der deutsche Gesetzgeber hat von diesen Klauseln in § 22 BDSG Gebrauch gemacht. Eine Verarbeitung sensibler Daten kann demnach durch die Erfüllung der Anforderungen des § 22 BDSG gerechtfertigt werden.

Die Behandlung eines Patienten mit Mitteln der Teletherapie durch einen Arzt oder anderweitig medizinisch geschultes Personal und damit die Verarbeitung von Gesundheitsdaten wird regelmäßig schon durch eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO gedeckt sein.

Abseits dessen erlaubt § 22 Abs. 1 Nr. 1 lit. b BDSG zumindest die Verarbeitung sensibler Daten „von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen", wenn jene Verarbeitung „zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist".

Der Einsatz von Teletherapie zu den genannten gesundheitlichen Zwecken bedarf bei der Durchführung durch die einschlägigen Personen also keiner ausdrücklichen Einwilligung zur Rechtfertigung der Verarbeitung personenbezogener sensibler Daten.

Problematisch ist allerdings der Einsatz von Plattformen, welche beispielsweise Videotelefonie ermöglichen, wenn jene Unternehmen angehören, die nicht den therapierenden Gesundheitseinrichtungen zuzuordnen sind. Hierbei kommt es zu einer Datenverarbeitung, welche nicht durch § 22 Abs. 1 Nr. 1 lit. b BDSG gedeckt ist. Die Plattformbetreiber werden regelmäßig kein ärztliches Personal oder sonstige Personen im Sinne des § 22 Abs. 1 Nr. 1 lit. b BDSG sein und die Verarbeitung auch nicht zu den genannten Zwecken ausführen. Der Einsatz dieser Plattformen und eine hiermit einhergehende Verarbeitung von Gesundheitsdaten ist wohl nur durch die Einholung der ausdrücklichen Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO zu rechtfertigen.

Um die mit strengen Anforderungen und großem Aufwand verbundene Einholung der Einwilligung nicht vornehmen zu müssen, bietet es sich an, eigene Dienste in den Gesundheitseinrichtungen zu implementieren und zu verwenden. Eine Datenverarbeitung von dritter Seite würde dann entsprechend entfallen.

IV. Der Verantwortliche

Besondere Aufmerksamkeit ist weiterhin der Rolle des Verantwortlichen im Datenschutzrecht zu widmen. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“. Nach Art. 24 DSGVO ist der Verantwortliche zuständig für die Einhaltung der datenschutzrechtlichen Vorgaben. Im Bereich der Teletherapie ist die Rolle des Verantwortlichen nicht unproblematisch zuzuordnen.

Schon die Frage, welche Person bei der Anwendung von telemedizinischen Maßnahmen in komplexen Praxis- und Krankenhausgeflechten Verantwortlicher ist, ist nicht klar zu beantworten. Hinzu kommt die Problematik der häufig in der Teletherapie vorhandenen Arbeitsteilung. Unterschiedliche Stufen und Teile der Therapie werden von verschiedenen Personen durchgeführt. Die Verantwortlichkeit müsste hier im Grunde aufgeteilt werden. Auch bei der Einschaltung eines externen Plattformbetreibers (bspw. für Videotelefonie) liegt eine Datenverarbeitung von verschiedenen Stellen vor. In solchen Konstruktionen bietet sich die Vereinbarung einer sog. gemeinsamen Verantwortlichkeit nach Art. 26 DSGVO an. Sollte es nämlich erst nachträglich zu der Einstufung der gemeinsamen Verantwortlichkeit kommen, sieht sich einer der Verarbeitenden unerwarteten Pflichten und Ansprüchen ausgesetzt.

Eine gemeinsame Verantwortlichkeit liegt nach Art. 26 Abs. 1 S. 1 DSGVO vor, wenn „zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest[legen]“. Der Gerichtshof der Europäischen Union (EuGH) legt den Begriff der gemeinsamen Verantwortlichkeit weit aus. Schon die Einbeziehung mehrerer Akteure in verschiedenen Phasen und in unterschiedlichem Ausmaß reicht in dem aktuellen FashionID-Urteil des EuGH zur gemeinsamen Verantwortlichkeit aus.[1] Es kommt daher schnell zu einer Einstufung einer Verarbeitung personenbezogener Daten durch mehr als eine Stelle als gemeinsame Verantwortlichkeit. Art. 26 Abs. 1 S. 2 f. DSGVO erlegt gemeinsam Verantwortlichen die Pflicht auf, ihre Verantwortlichkeit in einer eindeutigen Vereinbarung zu regeln. Eine solche Vereinbarung hat ferner den Vorteil, dass die Einzelheiten der datenschutzrechtlichen Verantwortlichkeit klar geregelt sind.

Eindeutige Vereinbarungen zu der Verantwortlichkeit und ggf. die Vereinbarung einer gemeinsamen Verantwortlichkeit können also im Rahmen der Teletherapie klare Verhältnisse schaffen und unerwartete Ansprüche vermeiden.

V. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Viele Unikliniken sind das Zentrum für medizinische Entwicklung und den Fortschritt von Behandlungsmethoden. Besonders hier zählt der Einsatz von Telemedizin bereits zur Praxis.

Die Bedrohung durch Viruserkrankungen, wie sie momentan mit Covid-19 vorherrscht, lässt Teletherapie noch attraktiver erscheinen. Nicht nur verringert sich das Ansteckungsrisiko, sondern auch der Zeitaufwand für einzelne Behandlungen sinkt. So wird der medizinische Sektor entlastet und es werden weitere Kapazitäten zur Bekämpfung der wesentlich drängenderen Virusproblematik geschaffen.

Wird den oben genannten Bedenken durch Befolgung der dargelegten Rahmenbedingungen begegnet, kann auch aus datenschutzrechtlicher Sicht grundsätzlich grünes Licht für Maßnahmen der Teletherapie erteilt werden. Dabei gilt es allerdings teilweise für die einzelnen Einrichtungen noch Landeskrankenhausdatenschutzgesetze oder Landeskrankenhausgesetze zu beachten, die spezifischere oder ergänzende Regelungen zum Umgang mit Datenschutz enthalten.

1 Die Aufarbeitung dieses Urteils in Baur, Stecker rein – Verantwortlicher sein!, DFN-Infobrief Recht 10/2019.

Admin-C – Sag beim Abschied leise Servus

Zur haftungsrechtlichen Verantwortung des Admin-C nach dem Inkrafttreten der DSGVO

von Maximilian Wellmann

Mit der Einführung der Datenschutz-Grundverordnung hat sich das Haftungsregime zum Admin-C grundlegend geändert. Die DSGVO ist hier Treiber einer Entwicklung, die die DENIC eG im vorauseilenden Gehorsam dazu veranlasst hat, ihre Domainrichtlinie zu novellieren. Bisher noch recht stiefmütterlich behandelt, lohnt es sich in der Folge, diese für das Domainmanagement spannende Entwicklung unter Einbeziehung der jüngsten Rechtsprechung nachzuzeichnen und auf die haftungsrechtlichen Implikationen für den Admin-C sowie den Domaininhaber einzugehen.

I. Hintergrund

Im Internet sind Websites entweder über die IP-Adresse des Webservers oder über die Domain der Website zu erreichen. Das Domain Name System (DNS) wurde eingeführt, um die Zahlenreihenfolge der IP-Adresse (z.B. 194.95.245.140) in ein Format zu transferieren, dass für den Menschen leichter wahrnehmbar ist (z.B. www.dfn.de). Jeder Domain ist dabei mindestens eine IP-Adresse zugeordnet. Für jede Top-Level Domain (z.B. .com.; .net; .de) gibt es eine Organisation, die für den Betrieb der Nameserver und die Vergabe von Domains unterhalb der Top-Level Domain verantwortlich ist. Für die Vergabe und Koordinierung von Top-Level Domains ist die Internet Corporation for Assigned Numbers (ICANN) zuständig, die ihrerseits die Verantwortung für die Verwaltung der einzelnen Top-Level Domains an verschiedene Unternehmen, sog. Registries überträgt. Für die „.de“ Domains ist dies die DENIC (Deutsches Network Information Center). Die Vergabe der Domains findet allerdings nicht direkt über die Registry statt, sondern über sog. Registrare, die für den Websitebetreiber die Registrierung der Domain erwirken. Die Registrare sind kommerzielle, von den Registries akkreditierte Anbieter, die mit dem Websitebetreiber in ein Vertragsverhältnis treten. Auf Grundlage dieses Vertrages erwirkt der Registrar bei der Registry, zum Beispiel der DENIC, die Registrierung der Domain. Das geschieht durch die Eintragung der Domain in einen von der Registry betriebenen Nameserver (sog. Konnektierung). Bisher war es bei der Registrierung einer Domain unumgänglich, bestimmte personenbezogene Informationen des Domaininhabers, des Admin-C und des Tech-C an die Registry und die zuständigen Registrare zu übermitteln.

Diese Daten wurden dann zentral in einer Datenbank des Registry abgelegt, dem sog. Whois-Eintrag (engl. „who is“). Mithilfe des Whois-Eintrags können von einem Datenbanksystem Informationen zu Internet-Domains und IP-Adressen sowie deren Inhabern abgefragt werden. Der Eintrag bestand nach der alten Domainrichtlinie der DENIC aus den persönlichen Kontaktdaten des Domaininhabers, des administrativen Ansprechpartners (Admin-C), des technischen Kontakts (Tech-C) sowie des Zonenverwalters (Zone-C) und konnte öffentlich eingesehen werden.

II. Domainrichtlinie und Domainbedingungen seit dem 25. Mai 2018

Mit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 hat sich die dargestellte Praxis für die Top-Level Domain „.de“ grundlegend geändert. Die DENIC hat sich bereits im März 2018 dazu entschlossen ihre Domainrichtlinien und Domainbedingungen grundlegend zu ändern und an die Erfordernisse der DSGVO anzupassen. Daraus ergeben sich einerseits für das Haftungsregime des Admin-C, als auch andererseits für die Abfrage des Whois-Eintrags durch Dritte grundlegende Änderungen.

Wie auch für den Domaininhaber wurden für den Admin-C in der Vergangenheit Name, Postanschrift, Telefonnummer und E-Mail-Adresse erhoben. Dem Admin-C kam hierbei eine Doppelrolle zu. Einerseits war er im vertraglichen Innenverhältnis zur DENIC berechtigt, sämtliche die Domain betreffenden Entscheidungen eigenverantwortlich zu treffen. Andererseits trat er auch im Außenverhältnis als die Person auf, der in Bezug auf die Domain eine eigenständige Entscheidungskompetenz zukam.

Ausgehend vom datenschutzrechtlichen Geboten der Zweckbindung und der Datenminimierung (vgl. Art. 5 Abs. 1 lit. b), c) DSGVO) hat sich die DENIC bei der Novellierung der Domainrichtlinie entschieden, die Regelungen zum Admin-C, zum Tech-C und Zone-C ersatzlos zu streichen. Eine entsprechende Datenerhebung findet damit logischerweise nicht mehr statt. Demgegenüber werden aber weiterhin domainbezogene technische Daten, wie die Angaben zu Nameservern und Informationen zu DNS-Keys erhoben, um die Funktionsfähigkeit der Domains sicherzustellen. Dabei handelt es sich aber nicht um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Um jedoch rechtliche und technische Anfragen in Bezug auf die Domain bearbeiten zu können, sind zusätzlich zu den persönlichen Pflichtangaben des Domaininhabers zwei nicht personalisierte E-Mail-Adressen abzufragen, eine für allgemeine und technische Anfragen (General Request) und eine zur Anzeige missbräuchlicher Nutzung der Domain (Abuse). Für die Adressen ist der jeweilige Registrar verantwortlich, der damit gewährleistet, dass der Domaininhaber wie bisher bei potentiellen Rechtsverletzungen oder technischen Problemen erreichbar ist.

Änderungen ergeben sich zudem bei der Abfrage des Whois-Eintrags durch Dritte. Hier sind nur noch die technischen Informationen der Nameserver (Domain registriert/nicht registriert) sowie die zwei Mailadressen zur spezifizierten Kontaktaufnahmen abrufbar. Ein öffentliches Anzeigen weiterer personenbezogener Daten findet nicht mehr statt. Dritte können damit weitergehende personenbezogene Informationen zum Domaininhaber nur noch bei Vorliegen eines berechtigten Interesses, eines vollstreckbaren Titels oder auf Grundlage einer gesetzlichen Bestimmung erhalten.

III. Haftung des Domaininhabers und des Admin-C

Aus der Nutzung einer Domain können Rechte Dritter verletzt werden. In Betracht kommt hier vor allem eine Haftung für Namens- (§ 12 BGB), Kennzeichenrechts-, (§§ 5, 15 MarkenG) oder Wettbewerbsrechtsverletzungen (§ 4 Nr. 4 UWG). Denkbar sind darüber hinaus auch Verstöße gegen das Urheberrecht. Haftungsrechtliche Sonderkonstellationen bestehen in sog. Treuhandkonstellationen, in denen dem Domaininhaber keine originären Rechte an der Domain als verwendetes Kennzeichen zustehen und bei der Verpachtung von Domains.

Für den Domaininhaber ändert sich durch die Implementierung der neuen Domainrichtlinie seitens der DENIC nichts. Er haftet wie schon zuvor unmittelbar für Rechtsverletzungen. Das heißt, er kann Adressat von Unterlassungs- und Schadensersatzansprüchen in Folge der oben bezeichneten Rechtsverletzungen werden. Domaininhaber kann dabei neben einer natürlichen Person auch eine juristische Person des öffentlichen Rechts, wie eine Hochschule oder Forschungseinrichtung, sein.

Änderungen ergeben sich aber für den Admin-C. In der Vergangenheit war dabei umstritten, ob dieser auch persönlich für Rechtsverletzungen haftet. Grund hierfür ist, dass der Admin-C rechtsgeschäftlich bestellter Vertreter des Domaininhabers ist und so gegenüber der DENIC die rechtliche Befugnis hat, auf den Inhalt der Eintragung einzuwirken. Der Admin-C haftet aber nicht unmittelbar als Täter oder Teilnehmer, da ihm in der Regel kein vorsätzliches oder fahrlässiges Handeln zur Last gelegt werden kann. Fraglich war in der juristischen Diskussion allenfalls, ob eine Störerhaftung in Betracht komme. Für die persönliche Haftung des Admin-C war dabei zwischen Namens- und Kennzeichenverletzungen, die durch die Eintragung der Domain selbst entstehen sowie unter der Domain eingestellte, rechtswidrige Inhalte zu differenzieren. Der Bundesgerichtshof (BGH) (u.a. Urteil vom 9.11.2011 – Az.: I ZR 150/09) hat im Hinblick auf die erste Konstellation Grundsätze der Störerhaftung konturiert und dabei eine allgemeine Prüfpflicht in Bezug auf rechtswidrige Inhalte und eine allgemeine Filterpflicht des Admin-C verneint. Eine persönliche Haftung des Admin-C könne aber dann ausgelöst werden, wenn dieser willentlich und adäquat-kausal an Störungen mitgewirkt habe, bei denen er rechtlich in der Lage war, diese zu beseitigen. Hinzutreten müsse zudem die Verletzung einer zumutbaren Prü-

fungspflicht. Zur zweiten Fallkonstellation war bis dato noch keine höchstrichterliche Entscheidung ergangen.

Als Folge der diffizilen Haftungslage rund um den Admin-C war in der Vergangenheit eine im Innenverhältnis zwischen Arbeitnehmer (Admin-C) und Arbeitgeber vereinbarte Haftungsfreistellungserklärung zu empfehlen, um das persönliche Haftungsrisiko des Admin-C auszuschließen.

Mit der neuen Domainrichtlinie der DENIC ist fraglich, ob eine Haftungsverantwortlichkeit des Admin-C besteht, nunmehr obsolet geworden. Die entsprechenden Datensätze werden durch die DENIC nicht mehr erhoben. Demzufolge kommt es im Innenverhältnis zwischen Arbeitnehmer und Arbeitgeber nicht mehr auf die Frage einer Haftungsfreistellungserklärung an, was in der Konsequenz dazu führt, dass eine Haftung für etwaige Rechtsverletzungen nur noch für den Domaininhaber in Betracht zu ziehen ist.

IV. Beschluss des Landgerichts Bonn

Der Wegfall der Datenerhebung zum Admin-C führt zu dem Problem, dass die entsprechenden Daten nach der bisher geübten Praxis nicht mehr an die ICANN übermittelt werden. Die ICANN hat daraufhin vor dem Landgericht (LG) Bonn (Beschluss vom 29.05.2018, Az.: 10 O 171/18) im Wege einer einstweiligen Verfügung beantragt, einem von ihr akkreditierten Registrar zu untersagen, Second-Level-Domains anzubieten und zu registrieren, ohne die Daten zum Admin-C und Tech-C zu erheben. Das LG Bonn wies die Beschwerde ab und führte zur Begründung aus, dass die Datenerhebung vor dem Hintergrund des Art. 5 Abs. 1 lit. b), c) DSGVO dem Grundsatz der Zweckgebundenheit und der Datenminimierung unterliege. Zwar bedeute die Erhebung zusätzlicher Daten eine erleichterte und verlässlichere Identifizierung der für die Domain verantwortlichen Personen, doch sei dieser Funktion schon durch den einzelnen Datensatz zur Identifizierung des Domaininhabers genüge getan. Zur Verfolgung strafrechtlich oder sonst wie zu ahnender Verstöße sei nicht ersichtlich, warum neben dem Hauptverantwortlichen (dem Domaininhaber) noch weitere Ansprechpartner zur Verfügung stehen müssten. Hinzukomme, dass für alle drei Datensätze (Domaininhaber, Admin-C und Tech-C) bisher dieselben Personendaten Verwendung finden konnten. Die Registrierung einer Domain scheiterte mithin nicht daran, dass dieselben Daten verwendet wurden. Die Entscheidung über die Angabe weiterer abweichender Datensätze zum Admin-C lag also schon vor Inkrafttreten der DSGVO beim Registrierungswilligen und war damit faktisch freiwillig. Dies muss nach Auffassung des LG Bonn so bleiben, da ein Registrierungswilliger nicht dazu gezwungen werden könne, Angaben zum Admin-C oder Tech-C zu machen. Im weiteren Prozessverlauf hat das Oberlandesgericht (OLG) Köln (Beschluss vom 03.09.2018, Az.: 19 W 32/18) als nächsthöhere Instanz, diese Rechtsansicht bestätigt und dabei ebenfalls den Grundsatz der Datenminimierung bekräftigt.

V. Fazit

Alles neu macht der Mai. So kann zutreffend die Einführung der DSGVO im Mai 2018 in Bezug auf die haftungsrechtliche Beurteilung von Domains ausfallen. Entgegen den landläufig zu beobachtenden Auslegungsproblemen, die mit der Einführung der DSGVO einhergehen, hat die DSGVO im Bereich des Domainmanagements (zumindest für die Top-Level Domain „.de“) mittelbar zu einer deutlichen Vereinfachung des Haftungsregimes geführt. Die Novellierung der Domainrichtlinie seitens der DENIC lässt Mitarbeiter von Hochschulen und Forschungseinrichtungen, die bisher als Admin-C fungierten, aufatmen, da sich für sie nun nicht mehr die Frage nach einer persönlichen Haftungsverantwortung stellt. Zwar war bereits vor dem Inkrafttreten der DSGVO eine Kennzeichenrechtsverletzung Dritter durch Hochschuldomains, die sich allein aus Buchstabenkürzeln und Ortsnamen zusammensetzen unwahrscheinlich, für Projektseiten oder fachspezifische Portale ist eine Haftung des Admin-C nunmehr aber endgültig vom Tisch. Auch für die Hochschulen und Forschungseinrichtungen als Arbeitgeber ist die Neuregelung eine Erleichterung, da es nun nicht mehr notwendig ist, mit dem Admin-C Haftungsfreistellungserklärungen abzuschließen, die den Mitarbeiter vor einer persönlichen Haftung schützen.

Die Rechtsprechung scheint in der Beurteilung der neuen Domainrichtlinie an der Seite der DENIC, betont sie doch die Grundsätze der Datenminimierung und Zweckbindung. In ihren absoluten Rechten verletzte Dritte werden durch den Beschluss des LG Bonn aber nicht rechtlos gestellt. Ihnen verbleibt vielmehr die Möglichkeit über die zwei nicht personalisierten E-Mail-Adressen gegen den Domaininhaber vorzugehen. Für Hochschulen und Forschungseinrichtungen, die als Körperschaften des öffentlichen Rechts grundsätzlich auch

Domaininhaber sein können, bedeutet dies also weiterhin eine haftungsrechtliche Verantwortung, der sie sich stellen müssen.

Möge die Firewall mit dir sein

Zum Datenschutz bei der Einrichtung von (Viren-) Schutzsystemen im betrieblichen Netzwerk

von Nicolas John

Schon seit mehreren Monaten sorgen Emotet-Angriffe auf Netzwerke für Unruhe in der digitalen Welt.[1] Ganze Stadtverwaltungen und Universitäten werden angegriffen und im Erfolgsfall lahmgelegt. Als Systemadministrator ist es daher unerlässlich, entsprechende Schutzsysteme gegen Virenangriffe einzurichten. Dennoch ist auch in diesem Bereich eine grenzenlose Kontrolle und Überwachung des Datenverkehrs nicht zulässig – die Datenschutzvorschriften wollen hier ebenfalls ausreichend beachtet sein.

I. Hintergrund und Ausgangssituation

Netzwerkadministratoren sehen sich tagtäglich der Gefahr ausgesetzt, dass das betriebliche Netzwerk durch einen Angriff mit einem Virus, Wurm oder sonstiger schädlicher Software infiziert werden kann. Die Folgen eines erfolgreichen Angriffs sind dabei kaum zu überschauen: Die Angreifer können beispielsweise durch eine geschaffene Sicherheitslücke unbemerkt sensible Daten herunterladen, die Mitarbeiter und Nutzer des Netzwerks überwachen und dadurch Zugangsdaten abfangen oder sämtliche vorhandenen Daten auf dem betrieblichen Server verschlüsseln, um danach ein Lösegeld für die Entschlüsselung zu fordern. Daher erscheint es selbstverständlich, dass gegen potenzielle Angriffe entsprechende digitale Schutzvorrichtungen etwa in Form von Firewalls, Virenscannern oder Intrusion Prevention Systemen (IPS) eingerichtet werden müssen. Je nach ihrer Funktionsweise greifen diese Schutzsysteme tief in den Datenverkehr des zu schützenden Netzwerks ein.

Doch die umfassende Überwachung des Netzwerkes ist nicht grenzenlos zulässig.[2] Durch den Eingriff werden die Daten der Mitarbeiter oder Nutzer des Netzwerks analysiert, protokolliert und gespeichert. Dabei ist zu unterschieden, ob die private Internetnutzung (teilweise) gestattet ist oder nicht. Hier sind unterschiedliche Maßstäbe im Sinne der Datenschutzvorschriften an die Behandlung und Untersuchung der Datenströme anzulegen. Somit ist vorab im Betriebsnetzwerk immer zu untersuchen, ob eine Erlaubnis zur Privatnutzung vorhanden ist oder aufgrund betrieblicher Übung die Nutzung gestattet sein könnte.[3] Diese tatsächlichen Gegebenheiten sind maßgebend für die rechtliche Einschätzung einer Kontrolle des Nutzungsverhaltens der Arbeitnehmer. Die Abwägung zwischen dem Schutz des Netzwerks mitsamt seinen gespeicherten Daten auf der einen Seite und dem allgemeinen Persönlichkeitsrecht der Arbeitnehmer und Nutzer des Netzwerks auf der anderen Seite ist daher unter vielen Gesichtspunkten gewissenhaft vorzunehmen.

1 Zur Arbeitsweise von Emotet sowie den Meldepflichten bei Betroffenheit: 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 Vertiefend zur Arbeitnehmerüberwachung m.w.N.: Baur, Spiel mit offenen Karten, DFN-Infobrief Recht 12/2017.

3 Zur privaten Internetnutzung am Arbeitsplatz: Tiessen, All work and no play, DFN Infobrief Recht 11/2019.

II. Überblick über die aktuelle rechtliche Lage

Für die aufgeworfene Problematik bei erlaubter privater Internetnutzung im Netzwerk ist zunächst klarzustellen, dass es zum jetzigen Zeitpunkt seit Erlass der Datenschutzgrundverordnung (DSGVO) keine aktuelle Rechtsprechung zu dieser Thematik gibt. Dies führt zu einer Vielzahl unterschiedlicher Ansichten in der Literatur, auf die nachfolgend eingegangen wird. Da eine höchstrichterliche Entscheidung aussteht, sollte der Arbeitgeber oder Netzwerkadministrator vorsichtig sein, soweit er - wenn auch zu Sicherungszwecken - Eingriffsmaßnahmen durchführen möchte. Insbesondere sind der Zweck des Eingriffs sowie die Eingriffstiefe für die rechtliche Einschätzung maßgebend. Hierzu sind die Hintergründe, Gesamtumstände und Einzelheiten, die einen Eingriff erforderlich machen, relevant.

Eine über den Zweck der Angriffserkennung hinausgehende Nutzung und Kenntnisnahme der Inhalte wird nach einer Ansicht der Literatur aufgrund des geschützten berechtigten Privatverkehrs vollumfänglich gesperrt, wenn nicht erkennbar ist, ob es sich um privaten oder dienstlichen Verkehr handelt. Insbesondere ist das in Art. 10 Grundgesetz (GG) verankerte Fernmeldegeheimnis zu beachten. § 88 Telekommunikationsgesetz (TKG) schützt das Fernmeldegeheimnis ebenfalls und konkretisiert die Rolle des Dienstanbieters. Den Telekommunikationsanbietern wird dadurch verboten, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder der näheren Umstände der Telekommunikation zu verschaffen. Ob § 88 Abs. 2 TKG jedoch nach Einführung der DSGVO weiterhin zur Anwendung kommt ist umstritten.

Fest steht, dass die Straftatbestände der §§ 202a, 206 und 303a Strafgesetzbuch (StGB) anwendbar bleiben. So kann die unbefugte Einsichtnahme in die privaten Daten des Arbeitnehmers strafbar sein, wenn der Zweck der Einsichtnahme nicht der Beseitigung von vorhandenen systemgefährdenden Viren oder Trojanern dient. Ebenfalls kann die Unterdrückung oder gar Löschung privater E-Mails ohne Rückfrage (zum Beispiel durch einen automatischen Spam-Filter) und ohne Rechtfertigungsgrund strafrechtliche Konsequenzen nach sich ziehen.[4] Es ist somit bei der Abwägung, inwieweit ein Eingriff in die Daten erforderlich ist, stets darauf zu achten, nur das absolut erforderliche Maß für den Systemschutz anzuwenden.

III. DSGVO, TKG, BDSG, LDSG?

Bei berechtigter Nutzung des Internets am Arbeitsplatz für private Zwecke ist derzeit mangels Rechtsprechung noch umstritten, ob sich die datenschutzrechtliche Beurteilung nach den speziellen Regelungen über das Fernmeldegeheimnis und den Datenschutz in §§ 88, 91 ff. TKG oder nach den allgemeinen Vorschriften von Art. 6 DSGVO, § 26 Bundesdatenschutzgesetz (BDSG) richtet.
Grundsätzlich ist der Anwendungsbereich der DSGVO aufgrund der Verarbeitung personenbezogener Daten i.S.d. Art. 4 Nr. 1 DSGVO bei der Verwendung von Angriffserkennungssoftware eröffnet. Bei einer Datenverarbeitung im Beschäftigungsverhältnis eröffnet Art. 88 DSGVO den weiteren Anwendungsbereich des § 26 BDSG, aber nur bei Datenverarbeitungen im „Beschäftigungskontext“. Wie weit der Begriff des Beschäftigungskontextes auszulegen ist, ist bislang durch die Rechtsprechung ebenfalls nicht abschließend geklärt. Überwiegend kann derzeit aber davon ausgegangen werden, dass die Implementierung von Angriffserkennungssoftware eine erlaubnispflichtige Verarbeitung i.S.d. Art. 6 Abs. 1 DSGVO darstellt.

In Bezug auf die Verwendung von Firewalls und Malwareerkennungssoftware wird die Implementierung des Angriffserkennungssystems in das Netzwerk von der Mehrheit als berechtigtes Interesse des Arbeitgebers nach Art. 6 Abs. 1 lit. f DSGVO gesehen. Auch Erwägungsgrund 49 der DSGVO bejaht das berechtigte Interesse, wenn die Verhinderung des Zugangs Unbefugter zu den elektronischen Kommunikationsnetzen und die Abwehr der Verbreitung schädlicher Programmcodes Ziel des Verarbeiters der personenbezogenen Daten ist. Diese Ansicht wird ebenfalls von Art. 32 DSGVO gestützt, wonach der Arbeitgeber für die Sicherheit der Datenverarbeitung zu sorgen hat. Dennoch muss immer im Einzelfall eine Abwägung hinsichtlich des Umfangs der Verarbeitung vorgenommen werden, denn jeder Eingriff in die Daten des

4 Zum zulässigen Umgang mit Spam-Mails: Sydow, Die Guten ins Töpfchen, die Schlechten ins Kröpfchen, DFN-Infobrief Recht 4/2017.

Benutzers stellt eine Verletzung des allgemeinen Persönlichkeitsrechts dar. Die Verarbeitung der Daten ist daher auch im Bereich der Angriffserkennungssoftware immer auf das absolut Notwendigste zu beschränken.

Eine andere Auffassung in der Literatur vertritt die Ansicht, dass auch § 26 BDSG (oder bei Hochschulbezug eventuell vorhandene vorrangig geltende Landesdatenschutzgesetze) aufgrund Art. 88 DSGVO anwendbar ist und ein Beschäftigungskontext bei berechtigter Privatnutzung vorliegt. Dies führt zu einer Erforderlichkeitsprüfung und -abwägung der Verarbeitung bezüglich der Durchführung des Arbeitsverhältnisses. Legitime Zwecke können hierbei technische Bedingungen des Verkehrs sein, etwa die Bewahrung des Computersystems vor Schaden. Eine Abwägung des Umfangs der Kontrollen ist jedoch auch hier im Hinblick auf das allgemeine Persönlichkeitsrecht des Arbeitnehmers für den Einzelfall vorzunehmen. Soweit der Schutz des Fernmeldegeheimnisses für die Kommunikation der Arbeitnehmer und Nutzer geprüft wird, ist ein großer Teil der Literatur und die Datenschutzaufsichtsbehörden der Ansicht, dass der Arbeitgeber als Diensteanbieter dem Fernmeldegeheimnis des § 88 TKG unterliegt. Zwar hat das OVG Münster nach zwischenzeitlicher Vorlage zum Europäischen Gerichtshof (EuGH) in einer aktuellen Entscheidung (Urteil vom 5.2.2020, Az. 13 B 1494/19) entschieden, dass E-Mail-Dienste wie GMail von Google nicht als Telekommunikationsdienste anzusehen sind. Jedoch betrifft dies nur den Fall, dass der Anbieter die Signalübertragung nicht sicherstellt. Da der Arbeitgeber mit seinem Netzwerk die erforderliche Signalübertragung für den funktionierenden Datenaustausch aber gerade bereitstellt und dafür verantwortlich ist, ändert dieses Urteil voraussichtlich nichts im Umgang mit den Daten während des Übertragungsvorganges. Insoweit ist eine mögliche Anwendbarkeit des TKG nicht ausgeschlossen.

Firewalls oder IPS-Systeme sind als unselbstständige Bestandteile des Dienstes zu betrachten, daher kommt das Datenschutzrecht zur Anwendung, welches für den angebotenen Dienst gilt. Auch hier finden sich im Rahmen des TKG Rechtfertigungs- und Erlaubnisnormen in den §§ 88 Abs. 3 Satz 1, 100, 109 TKG. Insoweit darf der Diensteanbieter zunächst gemäß §§ 100, 109 TKG automatische Angriffserkennungssysteme einsetzen, soweit dort keine Inhaltsdaten des Verkehrs verwendet werden, um auffällige Datenpakete zu erkennen. Jedoch kann § 88 Abs. 3 Satz 1 TKG darüber hinaus im Einzelfall als Erlaubnisnorm herangezogen werden, wenn die Kenntnisnahme der Inhaltsdaten im Einzelfall zum Schutz der technischen Systeme erforderlich ist. Im Ergebnis führt dies ebenfalls zu einer Einzelfallabwägung, inwieweit die Verwendung von Inhaltsdaten erforderlich ist. Soweit diese zum Schutz der technischen Systeme erforderlich sind, kann der Einsatz solcher Virenprogramme zulässig sein.

Bei allen vorgenannten Auffassungen ist zu beachten, dass die jeweilige Abwägung unter dem Aspekt des Schutzes des Netzwerks hinsichtlich des Einsatzes von Angriffserkennungssystemen vorzunehmen ist. Eine darüberhinausgehende Einsichtnahme in offensichtlich privaten Verkehr ist eher ausgeschlossen.

IV. Einwilligung oder Betriebs-/Dienstvereinbarung?

Selbstverständlich steht es dem Verarbeiter frei, eine Einwilligung von dem Betroffenen in die Datenverarbeitung zu Zwecken des Virenschutzes im Sinne der DSGVO einzuholen. Diese kann zwar einige der beschriebenen Unsicherheiten beseitigen, ist aber nicht immer zielführend. Da die Einwilligung freiwillig erfolgen muss und jederzeit widerrufen werden kann, bietet sie im Blick auf den dauerhaften Schutz des Netzwerks nur eine bedingte Sicherheit für eine effektive Gefahrenabwehr.[5]

Bezüglich Regelungsmöglichkeiten durch Betriebs- bzw. Dienstvereinbarungen hinsichtlich des Einsatzes von Angriffserkennungssoftware mangelt es zu diesem Zeitpunkt ebenfalls noch an höchstrichterlicher Rechtsprechung. Grundsätzlich hat ein Betriebs- bzw. Personalrat zwar Mitbestimmungsrechte bezüglich Einrichtungen, die in der Lage sind das Verhalten des Arbeitnehmers zu überwachen. Dazu genügt schon die objektive Möglichkeit der Überwachung. Ob davon Gebrauch gemacht wird, ist irrelevant. Daher genügen schon Aufzeichnungen wie Protokolle oder Verläufe um dies zu bejahen. Deshalb vertritt die Literatur die Auffassung, dass Office Software, Standard-Internetprogramme und Security Incident and Event Management-Systeme (SIEM-Systeme) als technische Überwachungseinrichtung einzustufen sind. Soweit diese Überwachungsmöglichkeit besteht,

5 Vertiefend zur Einwilligung: Fischer, Ja, ich will!, DFN-Infobrief Recht 3/2020; Mörike, Anweisung vom Chef: Willige ein!, DFN-Infobrief Recht 2/2019.

eröffnet Art. 88 DSGVO (im Beschäftigungskontext) neben § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) (bzw. bei Personalräten § 75 Abs. 2 Nr. 17 Bundespersonalvertretungsgesetz (BPersVG) oder entsprechende Landesnormen bei Hochschulbezug) die Möglichkeit einer andersartigen Regelung des Datenschutzes durch Kollektivvereinbarungen. Dabei ist jedoch zu beachten, dass die entsprechende Betriebsvereinbarung keine wesentliche Abweichung von dem Schutzstandard der DSGVO vornehmen darf. Nach momentan gängiger Praxis ist die Rechtfertigung der Verarbeitung der Arbeitnehmerdaten durch eine entsprechende Betriebsvereinbarung aber grundsätzlich möglich. § 26 Abs. 4 Satz 2 BDSG verweist dabei auf Art. 88 Abs. 2 DSGVO. Sie müssen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person beinhalten. Insbesondere hinsichtlich der Transparenz der Verarbeitung, der Übermittlung personenbezogener Daten innerhalb eines Unternehmensverbunds und Überwachungssysteme am Arbeitsplatz müssen die Interessen des Arbeitnehmers gewahrt werden.

IV. Fazit und Konsequenzen für die Hochschulpraxis

Aufgrund des fortschreitenden digitalen Ausbaus der Hochschulen und Forschungseinrichtungen ist die Einrichtung von Angriffserkennungssystemen auch hier unerlässlich. Da im wissenschaftlichen Bereich eine Unterscheidung zwischen privater und dienstlicher Nutzung oftmals nur schwer möglich ist, wird die private Internetnutzung meistens in den Forschungseinrichtungen erlaubt sein. Insoweit muss hier die Abwägung - auch im Hinblick auf mögliche Straftatbestände - äußerst gewissenhaft und umfassend vorgenommen werden. Dabei muss klar sein, dass die Verarbeitung privater Daten am Arbeitsplatz momentan sehr umstritten ist und es nach derzeitigem Stand keine Gerichtsentscheidungen hinsichtlich der „richtigen“ Sicherung des Netzwerks durch Schutzsoftware gibt. Daher sind bei dem Abwägungsvorgang sämtliche Faktoren einzubeziehen und unter strengen Gesichtspunkten in Bezug auf die Erforderlichkeit einzubringen. Dennoch können umfassende, notwendige Schutzmaßnahmen getroffen und eingerichtet werden, soweit eine einfachere, gleich effektive Lösung nicht in Sicht ist. Im Übrigen wird man in diesem Bereich die zukünftige Rechtsprechung abwarten und beobachten müssen, um datenschutzrechtliche Entwicklungen frühzeitig zu erkennen und technisch angepasst im eigenen System entsprechend zu implementieren.

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