www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

August 2020

Bild: iStock.com/AndreyPopov

Kein DSB muss fürchten, so schnell seine Sachen packen zu müssen. Denn für die Abberufung muss ein wichtiger Grund vorliegen.

Zuverlässigkeit und Fachkunde

Abberufung eines DSB wegen Pflichtverletzungen

Angenommen, der DSB übersieht etwas beim Datenschutz. Kann das eine schuldhafte Pflichtverletzung sein, die seine Abberufung rechtfertigt? Und angenommen, er macht bei seinen Aufgaben außerhalb des Datenschutzes einen Fehler. Kann das zur Abberufung als DSB führen?

Die meisten Datenschutzbeauftragten (DSB) nehmen mindestens eine weitere Funktion im Unternehmen wahr. Beides zugleich ist oft kaum zu schaffen. Doch was passiert, wenn in einem der Bereiche Fehler unterlaufen? Welche Folgen hat das für die Stellung des DSB? Eine Entscheidung des Landesarbeitsgerichts Mecklenburg-Vorpommern führt mitten hinein in diese Themenkreise.

Parteien des Rechtsstreits

Der Kläger, ein Volljurist, ist Angestellter im öffentlichen Dienst. Beklagte ist seine Arbeitgeberin, eine Universität. Sie betreibt ein Universitätsklinikum mit mehr als 4.100 Beschäftigten. Dieses Klinikum ist Teil einer Unternehmensgruppe, zu der weitere elf Gesellschaften mit insgesamt rund 900 Beschäftigten gehören.

Bestellung des Klägers zum DSB

Der Kläger war nicht von Anfang an DSB. Vielmehr begann er als Personaldezernent. Zum DSB des Universitätsklinikums bestellte ihn die Beklagte erst über sieben Jahre später. Dies wurde in einem ersten Änderungsvertrag zum Arbeitsvertrag festgehalten. Der Änderungsvertrag enthielt keine Regelung zu den Arbeitszeitanteilen für die verschiedenen Funktionen.

Regelung der Arbeitszeitanteile

Neun Monate später kam es zu einem zweiten Änderungsvertrag. Er legte fest, dass der Kläger zu 25 % seiner Arbeitszeit als Justiziar tätig sein sollte. 75 % seiner Arbeitszeit sollte er für Aufgaben des behördlichen Datenschutzbeauftragten sowie des Konzernbeauftragten für den Datenschutz verwenden.

Vorausgegangen war eine Anfrage des Klägers beim zuständigen Landes- →

Editorial

Ricarda Veidt, Chefredakteurin

Eingebauter Datenschutz

Liebe Leserin, lieber Leser! Ich weiß ja nicht, wie es Ihnen so geht. Aber bei mir hält sich die Begeisterung in Grenzen, wenn ich mir ein neues technisches Gerät anschaffen muss. Jüngstes Beispiel: Der zehn Jahre alte Fernseher macht offensichtlich langsam schlapp. Sehr bedauerlich, denn es kostet ja nicht unerheblich Zeit und Geld, sich einen neuen zu beschaffen.

Also im ersten Schritt darüber informiert, was es so am Markt gibt. Erste Erkenntnis: Himmel, wie groß müssen denn die deutschen Wohnzimmer sein, in die diese Riesenfernseher passen? (Nebenbei bemerkt: Wir brauchen auch einen Ersatz für das noch ältere durchgesessene Sofa – hier das gleiche Bild: fast nur noch Liegelandschaften, die mindestens eine Loft-Wohnung erfordern.)

Zweite Erkenntnis: Die Themen „Privacy by Design" und „Transparenz" sind bei den Herstellern wohl noch nicht wirklich angekommen. Das kritisiert aktuell auch ein recht neuer Akteur auf dem Gebiet des Datenschutzes: das Bundeskartellamt (siehe https://ogy.de/untersuchung-smart-tv). Ob es etwas nutzt? Wir werden sehen.

Bleiben Sie gesund!
Ihre Ricarda Veidt

beauftragten für den Datenschutz. Dieser teilte mit, die Tätigkeit als Datenschutzbeauftragter an der Universitätsmedizin sei als Vollzeitbeschäftigung einzustufen. Das berücksichtigte die Änderung zumindest teilweise.

Bestellung zum DSB für weitere Unternehmen

Zusätzlich ist der Kläger noch Datenschutzbeauftragter von insgesamt zehn GmbHs, die zur Unternehmensgruppe gehören. Dabei handelt es sich beispielsweise um mehrere medizinische Versorgungszentren, ein Kreiskrankenhaus und ein Palliativnetzwerk.

Umsetzung der DSGVO als Streitpunkt

Zum Konflikt zwischen Kläger und Beklagter kam es, als die Geltung der Datenschutz-Grundverordnung (DSGVO) ab 25. Mai 2018 unmittelbar bevorstand. Die Ereignisse entwickelten sich dabei wie folgt:

- Am 30.1.2018 führte die Beklagte mit dem Kläger ein Gespräch zum Stand der DSGVO-Umsetzung im eigenen Haus und bei den Tochtergesellschaften.
- Mit Schreiben vom 31.1.2018 nahm der Kläger dazu Stellung. Dabei berichtete er über die aktuellen Gesetzgebungsverfahren im Land Mecklenburg-Vorpommern zur Anpassung des Landesdatenschutzrechts an die Vorgaben der DSGVO.
- Dabei ging er insbesondere auf die Entwürfe für ein neues Landesdatenschutzgesetz und ein neues Landeskrankenhausgesetz ein.
- Ergänzend verwies er auf einen Aufsatz zur Datenschutz-Grundverordnung, den er für die Zeitschrift „f&w führen und wirtschaften im Krankenhaus", Ausgabe 2/2017, verfasst hatte.

Arbeitsverweigerung des Klägers?

Ein rotes Tuch für die Beklagte war der letzte Satz im Schreiben des Klägers: „Die konkrete Umsetzung der Datenschutzgesetze des Landes kann durch die Datenschutzverantwortlichen denklogisch erst nach Inkrafttreten der Gesetze erfolgen." Die Beklagte zog aus dieser Formulierung den Schluss, der Kläger sei nicht gewillt, seinen Verpflichtungen als Datenschutzbeauftragter nachzukommen.

Abberufung als DSB

Das führte zu einer ganzen Serie von Schreiben im Februar 2018, die die Bestellung des Klägers zum Datenschutzbeauftragten jeweils mit sofortiger Wirkung widerriefen:

- Mit je eigenen Schreiben widerriefen zehn Tochtergesellschaften der Beklagten die Bestellung des Klägers zum Datenschutzbeauftragten.
- Ebenso widerrief die Beklagte die Bestellung des Klägers zum Konzerndatenschutzbeauftragten.
- Darüber hinaus widerrief die Beklagte die Bestellung des Klägers zum Datenschutzbeauftragten bei der Beklagten selbst.

ONLINE-TIPP

Das Urteil des Landesarbeitsgerichts Mecklenburg-Vorpommern vom 25. Februar 2020 – 5 Sa 108/19 ist abrufbar unter https://ogy.de/5-Sa-108-19 (Umfang: 13 Seiten mit 83 Randnummern).

Bestellung eines neuen DSB

In der Folgezeit stritten Kläger und Beklagter darüber, ob die Widerrufe seiner Bestellung wirksam sind oder nicht. Ohne das Ergebnis der Auseinandersetzung abzuwarten, bestellte die Beklagte einen neuen, externen Datenschutzbeauftragten. Er nahm seine Tätigkeit auf.

Rüge der Datenschutzaufsicht

Der Streit eskalierte weiter, als der zuständige Landesbeauftragte für den Datenschutz einen Verstoß des Universitätsklinikums gegen Datenschutzbestimmungen rügte. Dabei ging es um ein Dienstplansystem, das bereits seit mehreren Jahren in Betrieb war. Dort waren zahlreiche Daten hinterlegt, die alle Mitarbeiter einer Station einsehen konnten. Dazu gehörten auch die Krankmeldungen sämtlicher Stationsmitarbeiter.

Der Landesbeauftragte hielt dies für nicht erforderlich und damit für unzulässig. Er forderte verschiedene Maßnahmen, um die Situation zu ändern, u.a. die Erstellung eines Rechte- und Rollenkonzepts. Andernfalls stellte er ein Bußgeld in Aussicht.

Erneute Abberufung als DSB

Daraufhin widerrief die Beklagte die Bestellung des Klägers zum Konzern- und zum Datenschutzbeauftragten vorsorglich erneut. Am gleichen Tag erklärten auch die zehn Tochtergesellschaften nochmals den Widerruf der Bestellung.

Die Beklagte warf dem Kläger vor, er habe zu keiner Zeit auf die datenschutzrechtlichen Probleme bei dem Dienstplansystem hingewiesen. Das habe erst der neu bestellte externe DSB getan.

Freistellung von der Arbeit und Hausverbot

Zu weiterem Disput führte ein Vorgang, den der Kläger in seiner Eigenschaft als Personaldezernent bearbeitet hatte. Dabei ging es um eine Versorgungszusage für einen früheren Kaufmännischen Vorstand. Die Beklagte warf dem Kläger vor, diese Versorgungszusage rechtswidrig vorgenommen zu haben. Er habe dabei mit dem Begünstigten „kollusiv zusammengewirkt", also mit ihm unter einer Decke gesteckt und gemeinsam mit ihm der Beklagten bewusst geschadet. Deshalb stellte die Beklagte den Kläger unwiderruflich von der Arbeit frei und erteilte ihm Hausverbot.

Strafanzeige wegen angeblicher Untreue

Eine weitere Stufe der Eskalation bestand darin, dass die Beklagte gegen den Kläger eine Strafanzeige erstattete. Dies begründete sie damit, dass er die Beiträge der Beklagten zu seiner eigenen Altersversorgung rechtswidrig erhöht habe. Darin liege eine strafbare Untreue.

Klage zum Arbeitsgericht

Der Kläger erhob Klage zum zuständigen Arbeitsgericht. Er begründet die Klage damit, dass sämtliche Widerrufe seiner Bestellung zum DSB unwirksam seien. Es liege kein wichtiger Grund für einen Widerruf der Bestellungen vor. Seine Pflichten als Datenschutzbeauftragter habe er nicht verletzt.

Sieg beim Arbeitsgericht

Das Arbeitsgericht gab der Klage statt. Es stellte fest, dass der Widerruf der Bestellungen des Klägers zum DSB sowie zum Konzern-DSB unwirksam seien. Das akzeptierte die Beklagte nicht. Sie legte Berufung zum Landesarbeitsgericht ein.

Sieg auch beim Landesarbeitsgericht

Im Ergebnis entschied das Landesarbeitsgericht zugunsten des Klägers. Der Kernsatz seiner Entscheidung lautet: „Der Kläger besitzt sowohl die erforderliche Sachkunde als auch die erforderliche Zuverlässigkeit zur Erfüllung der dem behördlichen Datenschutzbeauftragten obliegenden Aufgaben." Um zu diesem Ergebnis zu gelangen, musste das Gericht umfassende Überlegungen anstellen.

Maßgebliche Rechtsvorschriften

Zunächst stellt sich die Frage, anhand welcher Rechtsvorschriften zu prüfen →

ist, ob die Bestellung zum DSB wirksam widerrufen wurde. Die erste „Widerrufswelle“ erfolgte durch Schreiben vom 19., 20. und 27.2.2018. Die zweite „Widerrufswelle“ ereignete sich dann am 27.8.2018. Zwischen diesen beiden „Wellen“ liegt der 25.5.2018. Seitdem gilt die DSGVO.

Vorgaben der DSGVO

Die DSGVO legt als Qualifikationsvoraussetzungen fest, dass der DSB „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt [wird], das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt“. Zusätzlich fordert sie, seine Fähigkeit zu berücksichtigen, die gesetzlichen Aufgaben eines DSB zu erfüllen (siehe Art. 37 Abs. 5 DSGVO). Seit 25. Mai 2018 ist ausschließlich von diesen Voraussetzungen der DSGVO auszugehen.

Vorgaben des früheren Landesrechts

Die vorher maßgebliche Regelung des Datenschutzgesetzes Mecklenburg-Vorpommern formulierte die Voraussetzungen anders. Sie legte fest, dass zum DSB nur bestellt werden darf, wer die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt (siehe § 20 Abs. 1 Satz 3 Datenschutzgesetz Mecklenburg-Vorpommern in der damaligen Fassung).

PRAXIS-TIPP

Ein DSB müsse eine Vielzahl von Aufgaben wahrnehmen. Das erfordere es, Schwerpunkte zu setzen. „Die Kontrollpflichten werden nur dann vernachlässigt, wenn der DSB die ihm hierfür zur Verfügung stehende Arbeitszeit nicht ausschöpft, obwohl die Aufgaben noch nicht erledigt sind.“ So das Gericht wörtlich. Mit anderen Worten: Dass ein Landesdatenschutzbeauftragter etwas beanstandet, belegt für sich allein noch keine Pflichtverletzung des DSB. Vielmehr müssten weitere Aspekte hinzukommen. Beispiel: Der DSB hatte Hinweise auf die Rechtswidrigkeit eines Verfahrens, wird aber nicht aktiv, obwohl er die Zeit hierfür hatte.

Parallele Anforderungen

Nach Auffassung des Gerichts ergibt sich aus den abweichenden Formulierungen in der Sache kein Unterschied. Zwar erwähne die DSGVO die persönliche Zuverlässigkeit nicht gesondert. Daraus ergebe sich jedoch keine Abweichung. Denn ohne eine solche persönliche Zuverlässigkeit könnte ein DSB seine gesetzlichen Aufgaben gemäß Art. 39 DSGVO nicht erfüllen.

Ausgehend von dieser Sichtweise prüft das Gericht die beiden „Widerrufswellen“ nach denselben Maßstäben. Dabei geht es so vor, dass es sich zunächst mit der Sachkunde des Klägers befasst und dann mit seiner persönlichen Zuverlässigkeit.

Sachkunde des Klägers

Die Sachkunde des Klägers steht für das Gericht außer Frage. Als Volljurist sei er ohne Weiteres in der Lage, sich mit dem Datenschutzrecht vertraut zu machen und es praktisch anzuwenden. Dass er die Einzelheiten des neuen Datenschutzrechts kenne, zeige seine Veröffentlichung in einer Zeitschrift. Hinsichtlich technischer Fragen könne sich der Kläger bei seinem Stellvertreter informieren. Dieser Stellvertreter ist Informatiker.

Das Gericht fordert ausdrücklich nicht, dass ein DSB für alle Teilbereiche des Datenschutzes über eine volle eigene Qualifikation verfügt. Vielmehr genüge es, wenn er für Teilbereiche auf fachkundige Mitarbeiter zurückgreifen könne.

Zuverlässigkeit des Klägers

Auch an der persönlichen Zuverlässigkeit des Klägers hat das Gericht keine Zweifel. Seines Erachtens hat der DSB seine Pflichten nicht verletzt, obwohl er gegen das elektronische Dienstplansystem keine Einwendungen erhoben hat.

Pflichtverletzungen außerhalb des Datenschutzes

Allerdings könnte sich eine relevante Pflichtverletzung noch daraus ergeben, dass der DSB in seiner Eigenschaft als Personaldezernent dem früheren Kaufmännischen Vorstand angeblich eine rechtswidrige Versorgungszusage zugeschanzt hatte. Hier unterscheidet das Gericht:

- Vom Grundsatz her kann sich eine solche Pflichtverletzung durchaus auf die Zuverlässigkeit eines DSB auswirken, obwohl sie inhaltlich mit dem Datenschutz nichts zu tun hat. Jedenfalls bei einem internen DSB lasse sich seine Stellung als DSB nicht vollständig von dem Arbeitsverhältnis trennen, das dieser Stellung zugrunde liegt. Beispiele solcher Pflichtverletzungen seien etwa Diebstähle oder Unterschlagungen.
- Im konkreten Fall sieht das Gericht allerdings keine Anhaltspunkte für eine Pflichtverletzung. Denn die Rechtsauffassung des Klägers zu der Versorgungszusage sei jedenfalls vertretbar gewesen.

Ergebnis: Abberufung als DSB ist unwirksam

Unter dem Strich gelangt das Gericht zu der Auffassung, dass keine Pflichtverletzung des Klägers vorliegt. Damit verfüge er über die notwendige Zuverlässigkeit. Außerdem sei auch die erforderliche Fachkunde vorhanden.

Somit scheidet ein Widerruf seiner Bestellungen zum DSB aus. Sie würde nämlich voraussetzen, dass ein wichtiger Grund für eine Abberufung vorliegt. Dieser Grund müsste so schwerwiegend sein, dass er bei einem Arbeitsverhältnis die fristlose Kündigung rechtfertigen würde. Davon kann jedoch keine Rede sein, wenn dem Kläger überhaupt keine Pflichtverletzung vorzuwerfen ist. Und genau das ist die Auffassung des Gerichts im konkreten Fall.

Zu diesem Urteil des Landesarbeitsgerichts ist bereits Revision eingelegt zum Bundesarbeitsgericht. Das Aktenzeichen dort lautet 10 AZN 441/20.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken (Bayern). Er befasst sich seit vielen Jahren mit Fragen des Datenschutzes.

Bild: iStock.com/peterschreiber.media

In der Praxis sind Schadenersatzansprüche und die Drohung, solche geltend zu machen, zunehmend ein Thema

Sanktionen

Schadenersatzansprüche: Das unterschätzte Risiko der DSGVO

Schadenersatzansprüche sind zunehmend ein Thema. Das Arbeitsgericht Düsseldorf hat z.B. aktuell die Kriterien zur Bußgeldbemessung herangezogen, um einen immateriellen Schaden zu bewerten. Sensibilisieren Sie die Geschäftsleitung auch für dieses Risiko.

Die Datenschutz-Grundverordnung (DSGVO) hält einige Überraschungen bereit. Ein bisher unterschätztes Risiko sind z.B. die Schadenersatzansprüche. Eine zentrale Frage in der aktuellen Entwicklung ist, wer was beweisen muss. Außerdem muss sich zeigen, ob der Geschädigte eher einen Ausgleich für seinen Schaden erhält oder ob es vielmehr darum gehen wird, den Verursacher zu bestrafen.

Grundlagen eines Schadenersatzanspruchs

Die DSGVO regelt den Schadenersatzanspruch in Art. 82 DSGVO. Schadenersatzansprüche sind nicht neu. §§ 7, 8 des alten Bundesdatenschutzgesetzes (BDSG a.F.) sahen Schadenersatzansprüche ebenso vor wie das deutsche Zivilrecht im Bürgerlichen Gesetzbuch sowohl für eine Verletzung von Vertragspflichten (z.B. Arbeitsvertrag) als auch als sogenannter deliktischer Anspruch (§§ 823 ff. BGB; z.B. Verletzung des Persönlichkeitsrechts).

Weder nach DSGVO noch nach BGB ist also zwingend eine Vertragsbeziehung zwischen den Geschädigten und dem Schädiger erforderlich. Art. 82 DSGVO ist eine datenschutzrechtliche Spezialregelung, die gegenüber §§ 823 ff. BGB Vorteile für den Anspruchsteller vorsieht.

Voraussetzungen eines Schadenersatzanspruchs

Um Anspruch auf Schadenersatz zu haben, sind verschiedene Elemente Voraussetzung. Art. 82 Abs. 1 DSGVO formuliert das so: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter."

Anspruchsberechtigte

Nach Art. 82 Abs. 1 DSGVO ist also „jede Person" anspruchsberechtigt. Da die DSGVO nur natürliche Personen schützt, ergibt sich zumindest die Einschränkung, dass juristische Personen nicht anspruchsberechtigt sind.

Die Fachliteratur diskutiert, dass nicht nur die betroffene Person (siehe Art. 4 Nr. 1 DSGVO), sondern jede Person berechtigt sein soll, weil Art. 82 DSGVO das so formuliert. Das bedeutet, dass nicht nur die Personen den Anspruch geltend machen können, deren Daten von der Verletzung direkt betroffen sind, sondern auch mittelbar berührte Personen. Abgesehen davon, dass diese Ansicht abzulehnen ist, scheinen sich Anwendungsfälle auch nicht gerade aufzudrängen. Ein Beispiel könnte der Schaden eines familiären Mit-Kreditnehmers sein: Ist der Scoring-Wert falsch, zahlt er dadurch bedingt höhere Zinsen.

Rechtsverletzung

Grundlegende Voraussetzung für einen Anspruch ist, dass gegen eine Regelung der DSGVO verstoßen wurde. Hier kommt jede Regelung der DSGVO in Betracht. Gerade auch die in der Praxis ungeliebten Pflichten wie Löschregelungen, Privacy by Design and Default, Datenschutz-Folgenabschätzung, Dokumentations- und Organisationspflichten.

Schaden

Kein Schadenersatzanspruch ohne Schaden! Dem Anspruchsteller muss ein →

Schaden entstanden sein. Das sind zum einen materielle Schäden. Häufig sind das zumindest die Kosten der Rechtsverfolgung. Die DSGVO stellt aber klar, dass zum anderen auch immaterielle Schäden erfasst sind – Stichwort: Schmerzensgeld.

Die deutsche Rechtsprechung ist derzeit zurückhaltend bei der Höhe von Schmerzensgeld. Nach deutschem Zivilrecht ist auch schon der Anwendungsbereich von Schmerzensgeld inhaltlich begrenzt. Hier ist mit Ausweitungen gegenüber der bisherigen deutschen Rechtspraxis zu rechnen. Denn der Schadenersatz nach Art. 82 DSGVO sollte EU-weit einheitlich ausgelegt und angewendet werden und nicht alle EU-Mitgliedstaaten sind so restriktiv wie die deutsche Rechtspraxis.

Kausalität zwischen Rechtsverletzung und Schaden

Allein eine Rechtsverletzung und ein Schaden führen nicht zum Schadenersatz. Genau die konkrete Rechtsverletzung muss zusätzlich auch den konkreten Schaden verursacht haben. Das bringt in Art. 82 Abs. 1 DSGVO der Begriff „wegen" zum Ausdruck. Welche Anforderungen der ursächliche Zusammenhang erfüllen muss, ist noch nicht abschließend geklärt. Genügt die reine (Mit-)Ursächlichkeit? Oder ist auch die im deutschen Recht anerkannte Adäquanz erforderlich – sprich: Der Schaden liegt nicht außerhalb jeder Erwartbarkeit?

Nicht erforderlich ist nach der DSGVO, dass die verletzte Regelung vor dem konkreten Schaden schützen sollte. Im deutschen Deliktsrecht ist das unter dem Stichwort „Schutzzweck der Norm" dagegen eine weitere Voraussetzung für einen Schadenersatzanspruch.

Verschulden

Nach deutschem Rechtsverständnis setzt ein Schadenersatzanspruch ein Verschulden desjenigen, der mit dem Anspruch konfrontiert wird (Inanspruchgenommener), in Bezug auf die Rechtsverletzung voraus. In Bezug auf den Schadenersatzanspruch von Art. 82 DSGVO ist das umstritten, weil er das Verschulden nicht ausdrücklich anspricht.

Allerdings sieht Art. 82 Abs. 3 DSGVO vor, den Inanspruchgenommenen von der Haftung zu befreien, „wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist". Vereinfacht läuft das auf Vergleichbares hinaus. Denn auch nach dem deutschen Schadenersatzrecht müsste der Inanspruchgenommene darlegen, dass ihn kein Verschulden trifft.

Allerdings könnte die Formulierung von Art. 82 Abs. 3 DSGVO dazu führen, dass er sich in weiterem Umfang entlasten muss. Insbesondere könnte auch die Frage nach einer ausreichenden Datenschutzorganisation relevant werden.

Umfang eines Schadenersatzanspruchs

Damit ist noch nichts über das Ausmaß des Ersatzanspruchs gesagt. Dieser zweite Teil eines Schadenersatzanspruchs wird auch als „haftungsausfüllender Tatbestand" bezeichnet. Hierzu enthält die DSGVO keine Regelungen. Es gilt somit das deutsche Zivilrecht – also insbesondere §§ 249 ff. BGB.

Die DSGVO sieht den Ersatzanspruch sowohl für materielle als auch für immaterielle Schäden vor. Den immateriellen Schaden kennt man auch unter dem Stichwort „Schmerzensgeld". Materielle Schäden sind – vereinfacht gesagt – die Kosten, die anfallen, um den Zustand ohne das Schadensereignis wiederherzustellen. Häufig

Keine Haftungsprivilegierung mehr

Schadenersatzhaftung des Auftragsverarbeiters

Für den Auftragsverarbeiter ist mit Blick auf die Haftung eine neue Zeitrechnung angebrochen. Denn nach dem alten BDSG war er durch § 11 Abs. 1 Satz 1 vor Schadenersatzansprüchen des Datenschutzrechts geschützt. Art. 79 und Art. 82 DSGVO haben diese „Haftungsprivilegierung" beendet. Der Auftragsverarbeiter kann also seit dem 25.5.2018 direkt in Anspruch genommen werden. Die DSGVO ist noch einen Schritt weitergegangen. Denn nach Art. 82 Abs. 4 DSGVO haftet der Auftragsverarbeiter gegenüber einer betroffenen Person auch für Verstöße des Auftraggebers.

Nach Art. 82 Abs. 2 Satz 2 DSGVO haftet ein Auftragsverarbeiter für den Schaden, den eine Verarbeitung verursacht. Das gilt aber „nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat". Das schränkt seine Haftung zumindest in Teilen ein.
Gerade für die Sicherheit der Verarbeitung nach Art. 32 DSGVO ist zu beachten, dass der Auftragsverarbeiter diese Pflicht nicht nur als Auftrag des Auftraggebers ausführt. Art. 32 Abs. 1 DSGVO verpflichtet ihn auch selbst und direkt. Blindes Vertrauen auf die Haftungsbegrenzung könnte daher trügerisch sein.

Bild: iStock.com/cybrain

sind das zumindest die Kosten der Rechtsverfolgung – also insbesondere des eingeschalteten Rechtsanwalts. In der deutschen Rechtsprechung ist aber anerkannt, dass nicht jede sofortige Einschaltung eines Rechtsanwalts schadenersatzfähig ist, sondern sich der Betroffene zunächst selbst bemühen muss. Ob das auch für die DSGVO gilt, wird noch zu klären sein.

Strafschadenersatz: Der neue Weg, Datenschutz durchzusetzen

Im deutschen Schadenersatzrecht ist der Schadenersatz in Gestalt einer Bestrafung des Verletzers eigentlich nicht anerkannt. Ziel ist bisher stattdessen, einen entstandenen Schaden zu kompensieren, also auszugleichen. Das Arbeitsgericht Düsseldorf schlägt in seinem Urteil vom 5. März 2020 (Az. 9 Ca 6557/18) über einen Anspruch auf Ersatz des immateriellen Schadens wegen nicht vollständiger und verspäteter Auskunftserteilung allerdings einen anderen Weg ein.

Das Gericht stellt darauf ab, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten solle. Verstöße müssten effektiv sanktioniert werden, damit die DSGVO wirken könne. Das werde v.a. durch Schadenersatz in abschreckender Höhe erreicht. Gerichte könnten sich bei der Bemessung des immateriellen Schadenersatzes auch an Art. 83 Abs. 2 DSGVO – also den Bußgeldbemessungskriterien – orientieren. Das tut das Gericht sodann und setzt 5.000 € fest.

Ein solcher Weg birgt erhebliche Risiken:

- Der Schadenersatzanspruch wird zur „Ersatzstrafe" und die Zivilgerichte faktisch zu Sanktionsgerichten.
- Die betroffene Person darf den „Strafschadenersatz" – anders als das etwa bei staatlichen Bußgeldern nach Art. 83 DSGVO der Fall ist – behalten. Das könnte auf Kläger und Klägerinnen motivierend wirken. Bedenkt man, dass bei einem Datenschutzverstoß, der auf strukturellen Problemen fußt, eine Vielzahl von Personen betroffen sein kann, potenziert sich das Risiko.
- Auch ist nicht klar, ob es dann zu Doppel- und Mehrfachbestrafungen desselben Verstoßes käme. Man stelle sich eine unzulässige Aussendung von E-Mail-Werbung vor, und jeder Empfänger macht Strafschadenersatz geltend. Im Ergebnis würde – jedenfalls unter Beachtung der jeweiligen Kosten für Gerichtsverfahren – eine erheblich höhere Strafe „herauskommen" als die, die eine Aufsichtsbehörde verhängt.

Das macht die potenzielle Dimension erkennbar. Sie ergibt sich insbesondere auch deshalb, weil die betroffene Person bei diesem Ansatz überhaupt nichts zum eigenen Schaden vortragen müsste, sondern nur den Rechtsverstoß. Das Zivilgericht würde dann anhand der Bußgeldbemessungskriterien einen angemessenen Strafschadenersatz festlegen.

Auch für Datenschutzverantwortliche im Unternehmen kann das Konsequenzen haben. Denn die Unternehmen könnten auf die Idee kommen, den Datenschutzverantwortlichen wegen der Schadenersatzpflicht in Anspruch zu nehmen.

WICHTIG

Sollte sich dieser Ansatz durchsetzen, schafft das durch die Hintertür die Möglichkeit, im Privatklageweg die Bestrafung von Datenschutzverstößen zu erreichen.

Entscheidend: die Beweislast

In der Praxis von entscheidender Bedeutung ist: Wer muss was beweisen?

Nach deutschem Zivilrecht muss der Anspruchsteller grundsätzlich alle Anspruchsvoraussetzungen mit Ausnahme des Verschuldens beweisen. Der Inanspruchgenommene muss also nur beweisen, dass ihn kein Verschulden trifft. Die Rechtsprechung sieht aber – vereinfacht gesagt – auch Beweiserleichterungen für den Anspruchsteller vor, wenn sich beispielsweise ein Vorgang vollkommen in der Sphäre des Inanspruchgenommenen befindet. Wie sich diese Ansätze der Zivilrechtsprechung auf die DSGVO-Ansprüche auswirken, ist noch nicht final klar.

ACHTUNG!

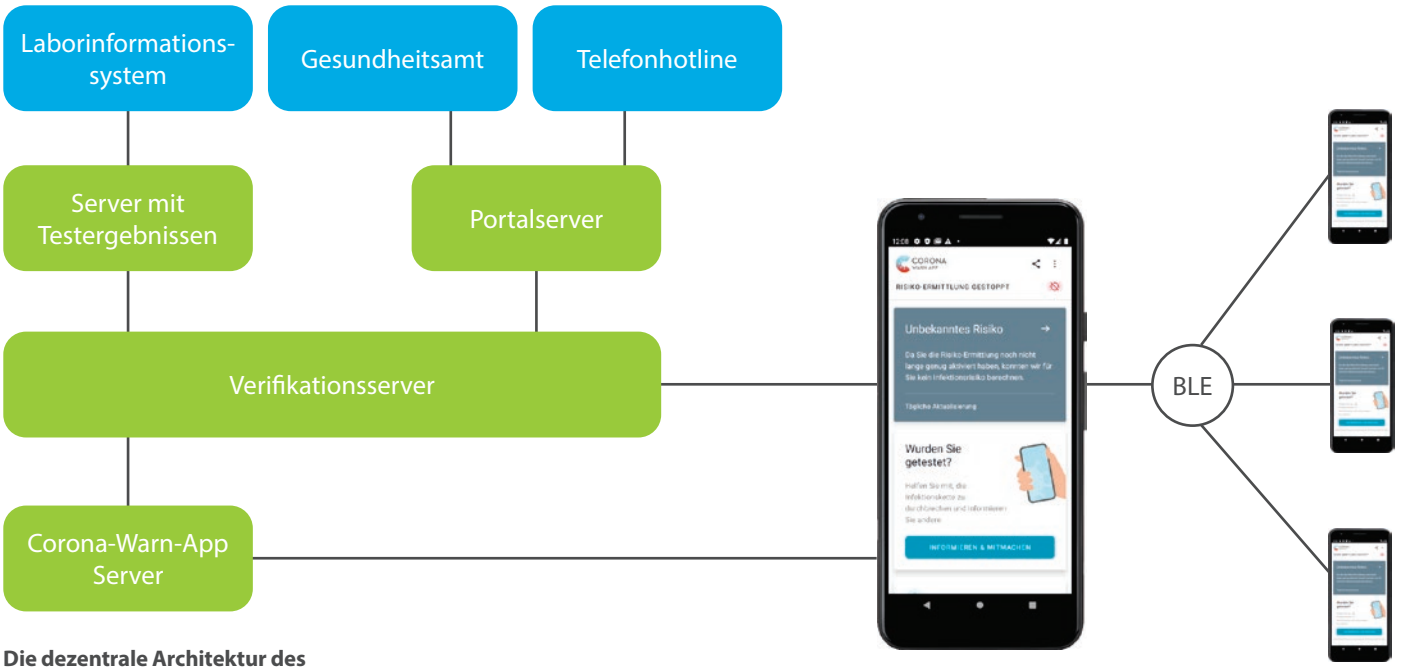
Muss nach deutschen Zivilrecht der Anspruchsteller seinen Schaden und die Kausalität der Rechtsverletzung für diesen Schaden darlegen und beweisen, würde der Ansatz des ArbG Düsseldorf auch hier einschlagen: Denn bestimmte sich der zu zahlende Schadenersatz nicht nach dem Schaden, sondern nach den Bußgeldbemessungskriterien, müsste der Anspruchsteller nichts zum Schaden oder zur Kausalität ausführen.

Bleibt es angesichts von Art. 82 DSGVO dabei? Nach der Systematik der DSGVO müssen Verantwortliche und Auftragsverarbeiter nachweisen, dass sie die DSGVO einhalten und nicht gegen das Recht verstoßen (siehe z.B. Art. 5 Abs. 2 DSGVO). Damit läge die vollständige Beweislast allein beim Verantwortlichen bzw. beim Auftragsverarbeiter. Erste gerichtliche Entscheidungen halten aber am Ansatz des deutschen Zivilrechts fest und sehen nicht die vollständige Beweislast beim Verantwortlichen (und Auftragsverarbeiter). Hier wird die weitere Entwicklung zu beachten sein.

Fazit: Die bessere Ausgangsposition hat der Anspruchsteller

Der Schadenersatzanspruch nach DSGVO ist ein bisher unterschätztes Risiko. Auch wenn noch nicht alle Fragen abschließend geklärt sind, müssen Datenverarbeiter zunehmend damit rechnen. Die beste Gegenmaßnahme ist schlicht, die DSGVO einzuhalten. Aber wenn es schiefgelaufen ist, muss sich der Verantwortliche konsequent und weitsichtig verteidigen. Denn der Anspruchsteller ist – auch wenn nicht die extreme Auslegung greift, dass er selbst nichts darlegen muss – in der komfortableren Ausgangsposition.

Dr. Jens Eckhardt ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht bei Derra, Meyer & Partner Rechtsanwälte in Düsseldorf.



Grafik: Andreas Sachs

Die dezentrale Architektur des deutschen Corona-Tracings ist sehr komplex

Data Protection by Design

Die deutsche Corona-Tracing-App

Das Projekt „Corona-Warn-App" ist ein Paradebeispiel dafür, dass 100 % Funktionalität (= schnelle Nachverfolgung von Infektionskontakten) zugleich mit einem hohen Maß an Datenschutz möglich ist.

Tracing

Der Begriff „Tracing", zu Deutsch „Ablaufverfolgung", war bislang eher aus der IT-Technik für die Protokollierung von Systemereignissen bekannt. Geht es darum, Infektionskontakte nachzuverfolgen, suggeriert der Begriff eine Nähe zum „Tracking". Doch diese Nähe täuscht. Denn die Verfolgung funktioniert ohne die negativen Begleiterscheinungen wie Identifizierbarkeit oder die Bildung von Persönlichkeitsprofilen.

Das neuartige Coronavirus kann ansteckend sein, bevor die infizierte Person auch nur leichteste Symptome entwickelt. Manche Personen haben keine Symptome und werden eher zufällig durch Reihentestungen entdeckt. Das verursacht eine erhöhte Ansteckungsrate.

Baustein zur Eindämmung

Aus diesem Grund ist es wichtig, dass infizierte Menschen sich in Quarantäne begeben. Neben der manuellen Nachverfolgung durch die Gesundheitsämter und ausreichenden Testkapazitäten gilt die Kontakt-Nachverfolgung durch eine App als möglicherweise bedeutender Baustein, um das Infektionsgeschehen einzudämmen (siehe https://ogy.de/studie-uni-oxford).

Tracing-Techniken

Es gibt nach momentanem technischem Stand drei Varianten, um das Kontaktverhalten von großen Teilen der Bevölkerung zu erfassen:

1. Funkzellen

Jedes Smartphone ist permanent in mehrere Funkzellen eingeloggt. Während nur eine dieser Zellen die Daten- oder Sprachverbindung realisiert, lässt sich über einfache geometrische Funktionen anhand der Signalstärke und des Standorts der Masten der Standort eines Nutzers abschätzen. Diese Technik nutzt die Polizei unter strengen rechtlichen Anforderungen mitunter im Rahmen ihrer Aufgaben.

2. Standortdaten

Standortdaten zu erfassen, ist technisch sehr einfach. Jedes Smartphone hat einen integrierten Standortdienst. Er erfasst die Position des Geräts anhand von GPS- und Wifi-Signalen in der Regel auf wenige Meter genau. Innerhalb von Gebäuden kommt diese Technik allerdings an ihre Grenzen. Denn hier ist keine GPS-Koordination vorhanden, und die Positionsbestimmung mit Wifi-Signalen verliert deutlich an Genauigkeit.

Internationale Ansätze

Wie arbeiten andere Warn-Apps?

Auch andere Länder setzen Smartphone-Apps als Baustein ein, um die Corona-Pandemie zu bewältigen. So hat China z.B. die Erfassung von Standortdaten in weit verbreitete Apps integrieren lassen. Diese Apps sind somit auch geeignet, um umfangreiche Bewegungsprofile eines Großteils der Bevölkerung zu erstellen. In Südkorea, das ebenfalls eine App einsetzen wird, sind die Telefonnummern der Smartphones mit den erfassten Kontaktdaten verknüpft. Das ermöglicht zumindest Beziehungsmuster aller App-Nutzer mit unmittelbaren Identifikationsmerkmalen. Österreich dagegen setzt zwar Bluetooth ein, um Kontakte zu erfassen. Es erfasst aber die Telefonnummern, wenn jemand seine eigene Corona-Infektion meldet.

3. Funksignale

Jedes Smartphone hat integrierte Funkchips. Sie realisieren das Funkprotokoll Bluetooth. Die neueste Variante, Bluetooth Low Energy (BLE), bietet neben verbesserten Sicherheitseigenschaften einen geringeren Stromverbrauch. Das Corona-Tracing verwendet BLE recht kreativ: Anhand der Signalstärke wird der Abstand zwischen zwei Smartphones abgeschätzt. Das ist keineswegs trivial. Denn die Signalstärke schwankt und variiert zwischen Hardwaremodulen und Softwaretreiberversionen.

Die deutsche Corona-Warn-App arbeitet mit BLE. Warum hat man sich dafür entschieden? Den datenschutzrechtlichen Grundsatz der Erforderlichkeit definiert die Datenschutz-Grundverordnung (DSGVO) wie folgt: Geeignet, um einen bestimmten Zweck zu erreichen, und es ist kein milderes Mittel (im Sinne eines Grundrechtseingriffs) vorhanden. Bei den drei beschriebenen Tracing-Varianten erfüllt insbesondere mit Blick auf geschlossene Räume die Variante, die Funksignale nutzt, konkret BLE, beide Voraussetzungen am besten.

Direkte Identifizierbarkeit vs. Pseudonymität vs. Anonymität

Die Frage, ob eine Tracing-Erfassung von weiten Teilen der Bevölkerung mit direkt identifizierbaren Merkmalen wie Telefonnummer oder Name bzw. Adresse stattfinden sollte, wurde schon frühzeitig politisch entschieden: Der Datenschutz sollte so weit möglich umgesetzt werden. Die direkte Identifizierbarkeit war damit vom Tisch.

Das führte zu dem Konzept, dass stabile kryptografische Verfahren Zufallskennungen erzeugen. Diese Kennungen werden als Bestandteil eines Kontaktdatensatzes, der auch einen Zeitstempel oder die Signalstärke enthält, gespeichert. Diese Zufallskennung erfüllt die Voraussetzung zur Pseudonymisierung nach DSGVO. Denn die Kennung ist nicht mit einem unmittelbar identifizierbaren Merkmal verknüpft. Es könnte aber verfügbares Zusatzwissen geben, das eine Identifikation ermöglicht.

Es lässt sich jedoch durchaus auch der Begriff der Anonymität begründen. Denn hier fordert die DSGVO, alle Mittel zu berücksichtigen, die der Verantwortliche oder eine andere Person nach allgemeinem Ermessen wahrscheinlich nutzt, um die natürliche Person direkt oder indirekt zu identifizieren. Gerade mit Blick auf den gleich beschriebenen dezentralen Ansatz ist diese Sichtweise nicht allzu abwegig.

Zentral vs. dezentral

Beim Infektions-Tracing geht es darum, Personenkontakte in räumlicher Nähe über einen gewissen Zeitraum zu erfassen. Hat einer dieser Kontakte einen positiven Corona-Test gehabt, informiert das Tracing alle relevanten Personenkontakte über ein mögliches Infektionsrisiko. Dabei sind drei grundlegende Fragen zu klären:

1. Wo werden die zufälligen Personenkennungen erzeugt?
2. Wo werden die Kontaktinformationen (von zwei Smartphones) gespeichert?
3. Wie werden Nutzer über einen risikobehafteten Kontakt informiert?

Beim zentralen Modell erzeugt ein zentraler Server die Kennungen und speichert sie. Die Information über einen Kontakt zu bestä- →

Tracing bei Urlaubsreisen (Interoperabilität)

Wie ist denn der Kontakt in der Kneipe im Urlaubsort zu werten, von dem eher der Ouzo als der Name des Trinkpartners in Erinnerung ist? Sollten auch Apps anderer Länder das Exposure Notification Framework von Apple/Google nutzen, ist eine grenzübergreifende Benachrichtigung technisch kein Problem, sofern der politische Wille vorhanden ist. Sollte das Framework nicht genutzt werden, dann sieht es schon anders aus – machbar ist es aber.

Zentraler Ansatz in Frankreich

In Frankreich hat der zentrale Ansatz den „Segen" der französischen Datenschutzaufsichtsbehörde erhalten; zwar mit gewissen Bauchschmerzen, aber immer noch in Einklang mit der DSGVO.

Die Datenschutzerklärung der Corona-Warn-App ist in einfacher Sprache geschrieben und gut verständlich. So soll es sein.

WICHTIG

Das Aufsetzen auf das Exposure Notification Framework setzt voraus, dass die Firmen Google und Apple vertrauenswürdig sind und sie die Zufallskennungen nicht mit Benutzerkonten oder Werbe-IDs verknüpfen. Bei Android ist es zudem so, dass dieses Framework Bestandteil der „Google Play Services"-App ist. Rein als Open Source betriebene Android-Smartphones mit sogenannten Custom-ROMs werden damit (noch?) nicht unterstützt.

tigten Corona-Personen erfolgt ebenfalls serverseitig an die Geräte, die einen Kontakt zu der Person hatten. Den zentralen Ansatz verfolgte ursprünglich auch Deutschland. Die konkreten Realisierungskonzepte hatten bereits den Grundgedanken Data Protection by Design verfolgt und wären grundsätzlich auch mit der DSGVO in Einklang zu bringen gewesen.

Dass es dann zum dezentralen Modell kam, lag an zwei Faktoren: Die in der Öffentlichkeit geführte Diskussion um die zwei unterschiedlichen Architekturansätze führte dazu, dass besorgte Bürgerinnen und Bürger der Meinung waren, es sollten Bewegungsprofile mit Standortinformationen und direkter Identifizierbarkeit zum Corona-Tracing eingesetzt werden.

Der andere Grund war viel schlichter: Smartphone-Apps auf dem Apple-Betriebssystem unterstützen keine dauerhaft laufenden Hintergrundprogramme mit Zugriff auf die Bluetooth-Schnittstelle. Es musste also eine Lösung für dieses „Problem" her.

Das dezentrale Modell der Corona-Warn-App

Das dezentrale Modell, das in Deutschland die „Corona-Warn-App" umsetzt, besitzt also folgende Eigenschaften:

1. Die Generierung der Zufallskennungen erfolgt auf dem Smartphone ohne Speicherung auf einem zentralen Server.
2. Kontaktinformationen zwischen zwei Smartphones bleiben auf den Geräten und werden nicht an einen zentralen Server zur Speicherung übertragen.
3. Die Information über mögliche Corona-Kontakte erfolgt von einem Smartphone über eine zentrale Stelle an alle Smartphones, die die Tracing-App installiert haben. Ein Abgleich erfolgt ausschließlich lokal auf dem Gerät, genauso wie die Meldung, dass man ein erhöhtes Infektionsrisiko besitzt.

Plattformunterstützung durch Google und Apple

Soll ein Infektions-Tracing über das Bluetooth-Signal erfolgen, sind neben der Frage des Batterieverbrauchs und dauerhaft laufender Hintergrundprozesse umfangreiche Kenntnisse über das Bluetooth-Protokoll, die verwendete Hardware und ggf. Softwaretreiber erforderlich. Aus diesem Grund haben die beiden großen Plattformanbieter für Smartphones, die Firmen Google und Apple, das Exposure Notification Framework (https://www.google.com/covid19/exposurenotifications/) entwickelt. Die Plattform soll es App-Entwicklern ermöglichen, über eine Softwareschnittstelle auf Zufallskennungen zuzugreifen, wenn sie ein dezentrales Architekturmodell realisieren.

Das Framework arbeitet mit einem Risikomodell, das eine externe Parametrisierung unterstützt. Das bedeutet, dass der App-Betreiber gewisse Stellschrauben bezüglich des aktuellen Infektionsgeschehens einstellen kann. In Deutschland ist dies das Robert-Koch-Institut.

Außerdem ist sichergestellt, dass nicht alle anderen Apps auf einem Smartphone auf diese Schnittstelle zugreifen können. Denn das würde Re-Identifikationsrisiken mit sich bringen.

Wie steht es um den Datenschutz durch Technikgestaltung?

Der „Datenschutz durch Technikgestaltung" von Art. 25 Abs. 1 DSGVO fordert,

- den Datenschutz schon in der Planungsphase zu berücksichtigen und
- die Datenschutzgrundsätze von Art. 5 Abs. 1 DSGVO risikoorientiert umzusetzen.

Wie hat nun die Warn-App diese Grundsätze umgesetzt?

1. Transparenz für den Betroffenen

Die Transparenz für den Betroffenen ist durch Datenschutzbestimmungen für die unterschiedlichen Zwecke und die Einholung der Einwilligung zentral in der App integriert. Die Sprache ist einfach gehalten. Eine Mehrsprachigkeit ist angedacht.

2. Datensparsamkeit & Zweckbindung

Die Datensparsamkeit setzt die App durch den dezentralen Ansatz und die lokale Erfassung von sich ändernden Zufallskennungen durch BLE um. Die Zweckbindung stellen die weitgehend pseudonymen/anonymen Zufallskennungen sicher. Die nach Zwecken getrennten Systemeinheiten in der Grundarchitektur unterstützen ebenfalls die Zweckbindung.

3. Richtigkeit der Daten

Bei der Richtigkeit der Daten ist der unsichere Faktor, ob die schwankenden Signalstärken der BLE-Funksingale nicht im Einzelfall eine Risikoexposition mit sich bringen, obwohl in Wirklichkeit z.B. eine Glasscheibe dazwischen war. Die Richtigkeit im Sinne von Authentizität von Corona-Infektionen realisieren abseits der App einzulesende TAN-Nummern (z.B. in QR-Codes) – das setzt allerdings voraus, dass diese TAN-Nummern im Gesamtsystem robust gegen Zufallsangriffe geschützt sind.

4. Speicherbegrenzung

Die Speicherbegrenzung wird derart umgesetzt, dass die Zufallskennungen im Exposure Notification Framework nach 30 Tagen automatisch gelöscht werden. Darüber hinaus kann der Nutzer die eigene Zufallskennungen-Reihe löschen, indem er die App deinstalliert.

5. Integrität und Vertraulichkeit

Den Grundsatz der Integrität und Vertraulichkeit, also die Informationssicherheit der App und der beteiligten Server, sollen folgende Maßnahmen umsetzen:

- saubere Softwareentwicklung
- begleitende Pen-Tests
- Orientierung an Best-Practice-Maßnahmen (z.B. BSI-IT-Grundschutz)
- Source-Codes werden der Öffentlichkeit und damit externen Sicherheitsforschern o.Ä. zur Verfügung gestellt.

Im Ergebnis enthält die Warn-App zumindest alle relevanten Bereiche von Art. 5 Abs. 1 DSGVO. Damit ist dieses Projekt ein sehr gutes Beispiel dafür, dass sich Funktionalität und ein hohes Maß an Datenschutz nicht widersprechen.

Datenschutz-Folgenabschätzung

Dass eine Datenschutz-Folgenabschätzung (DSFA) bei einem solchen Infrastrukturprojekt erforderlich ist, überrascht nicht. Eher schon, dass man auch hierbei dem Transparenzansatz vollumfänglich nachgekommen ist. Die DSFA samt Risikoanalyse sowie technischen und organisatorischen Maßnahmen, um erkannte Risiken einzudämmen, lässt sich frei herunterladen (https://ogy.de/cwa-dsfa; PDF mit 117 Seiten).

Was ist mit einem Zweckänderungsverbot?

Die Rechtsgrundlage für die Corona-Tracing-App ist die datenschutzrechtliche Einwilligung nach Art. 6 Abs. 1 Buchst. a. Dass diese Einwilligung nicht freiwillig sein könnte, Gastronomen beispielsweise den Zugang zu ihren Betrieben von einer „grünen Anzeige“ in der App abhängig machen, haben die Datenschutzaufsichtsbehörden erkannt. In ihrer Pressemitteilung sprechen sie daher bei solchen Fällen klar von einer „zweckwidrigen Verwendung“ (https://ogy.de/dsk-warn-app).

Trotzdem wäre es eine weitere vertrauensbildende Maßnahme gewesen, ein Zweckänderungsverbot der Tracing-Daten gesetzlich zu verankern. Allerdings stellt die beschriebene dezentrale Architektur mit pseudonymen bzw. anonymen Zufallskennungen weitgehend sicher, dass zumindest keine zentrale Massenüberwachung der Bevölkerung möglich wäre.

Fazit: Gutes Beispiel für Privacy by Design und DSFA

Die Gesamtarchitektur der deutschen Corona-Tracing-App besitzt eine gewisse Komplexität – sie tut jedenfalls mehr, als nur flächendeckend personenbezogene GPS-Koordinaten auf einem Server zu sammeln. Sie kann nach aktueller wissenschaftlicher Erkenntnis einen Baustein darstellen, der das Corona-Infektionsgeschehen effektiv eindämmt. Und dies unter Berücksichtigung der technischen Gestaltungsmöglichkeiten des europäischen Datenschutzes.

Die momentan höchsten Risiken, die abseits dieser Betrachtung existieren, liegen in Deutschland darin, dass noch nicht alle Labore daran teilhaben, die TANs digital zu generieren – ein Problem, das an sich leicht zu lösen ist.

Die DSFA zur Corona-Warn-App kann ein Referenzprojekt auch für andere Verantwortliche sein, die bislang der Meinung waren, mit ein bis zwei Seiten Risikoauswertung eine Datenschutz-Folgenabschätzung durchgeführt zu haben.

Andreas Sachs ist Vizepräsident des Bayerischen Landesamts für Datenschutzaufsicht und leitet das Referat, das sich u.a. mit dem technischen Datenschutz beschäftigt.

Konsultation der Aufsichtsbehörde

Die DSFA kommt zu dem Ergebnis, dass es hohe Restrisiken gibt, die sich nicht wirksam eindämmen lassen. Die DSFA ruft an dieser Stelle Art. 36 DSGVO aus (Konsultation der Aufsichtsbehörde). Art. 36 DSGVO sagt nicht, dass ein Verantwortlicher die Verarbeitung nicht starten dürfe, sondern „nur“, dass er die zuständige Datenschutzaufsichtsbehörde konsultieren muss. Die Datenschutzaufsicht kann dann im Einzelfall eine Verarbeitung untersagen, muss dies aber nicht tun. Das lässt sich als weiterer Schritt zu einem hohen Datenschutz-Standard werten. Hier stellt sich eher die Frage, wieso Art. 36 DSGVO in der Praxis bei Unternehmen abseits der Corona-Tracing-App faktisch nicht vorkommt.

Europäische Kommission

Bericht zur Evaluierung der DSGVO

Bild: iStock.com/Esra Sen Kula

Erstmals hat die Europäische Kommission gemäß ihrer Verpflichtung aus Art. 97 Abs. 1 DSGVO einen Bericht vorgelegt, der dazu dienen soll, die Datenschutz-Grundverordnung (DSGVO) zu bewerten und zu überprüfen.

Ziele erreicht

Sätze wie dieser prägen weithin das Bild des Berichts: „Die allgemeine Auffassung ist, dass die DSGVO zwei Jahre nach Beginn ihrer Anwendung ihre Ziele, den Schutz des Rechts des Einzelnen auf den Schutz personenbezogener Daten zu stärken und den freien Verkehr personenbezogener Daten innerhalb der EU zu gewährleisten, erreicht hat." (Seite 4).

Für eine Bewertung, ob die Mechanismen der Zusammenarbeit zwischen den nationalen Aufsichtsbehörden funktionieren, ist es nach Auffassung des Berichts noch zu früh (siehe Seite 5). Häufig würden Beobachter auf Widersprüche zwischen den Auffassungen der nationalen Aufsichtsbehörden und des Europäischen Datenschutzausschusses hinweisen. Auch werde mehr praktische Hilfestellung als bisher erwartet (Seite 6).

Vorteil technikneutraler Ansatz

Der technikneutrale Ansatz der DSGVO erweist sich nach Auffassung der Kommission als ein großer Vorteil (Seite 10 des Berichts). Zum Thema „Evaluation der vorhandenen Angemessenheitsbeschlüsse gemäß Art. 45 DSGVO" will die Kommission gesondert berichten, sobald der Europäische Gerichtshof am 16. Juli 2020 seine Entscheidung in dem Verfahren „Schrems II" (Rechtssache C-311/18) verkündet hat (Seite 11 des Berichts).

Der Bericht vom 24. Juni 2020 umfasst 18 Seiten und ist (bisher nur auf Englisch) abrufbar unter https://ogy.de/bericht-dsgvo.

Cyber-Sicherheit

Selbst-Check für medizinische Einrichtungen

Der Bayerische Landesbeauftragte für den Datenschutz und das Bayerische Landesamt für Datenschutzaufsicht haben gemeinsam „Best-Practice-Prüfkriterien Art. 32 DS-GVO" zum Thema „Cybersicherheit für medizinische Einrichtungen" veröffentlicht. Sie behandeln 16 Themenkreise, u.a. Ransomware, Firewall und Homeoffice.

Umfangreiche Checkliste

Das Papier ist als umfangreiche Checkliste aufgebaut, die je Themenkreis drei bis zehn Einzelaspekte anspricht. Bei jedem Thema finden sich Links zu empfehlenswerten Seiten, die eine Vertiefung ermöglichen.

Der äußere Umfang des Selbst-Checks wirkt mit fünf Seiten eher bescheiden. Inhaltlich deckt er jedoch eine so große Bandbreite von Fragen ab, dass das Durcharbeiten erhebliche Zeit in Anspruch nehmen wird. Das Dokument (Stand: 27. Mai 2020) ist abrufbar unter https://ogy.de/best-practice-medizin.

Baden-Württemberg

Fragebogen zur Videoüberwachung

Ein Fragebogen zur Videoüberwachung, den die Aufsichtsbehörde Baden-Württemberg bei Datenschutzprüfungen verwendet, ist im Internet auf der Plattform FragDenStaat abrufbar. Die Plattform wird durch den Verein Open Knowledge Foundation Deutschland e.V. betrieben. Sie will dazu anregen, bei staatlichen Stellen vorhandenes Wissen durch Anfragen verfügbar zu machen.

Der Fragebogen besteht aus 15 Fragen. Einige wenige Fragen sind im Normalfall rasch zu beantworten, so etwa Frage 2 „Wie viele Kameras sind in Betrieb?" Andere Fragen zu beantworten, macht es erforderlich, Unterlagen zu erstellen. Das gilt z.B. für Frage 3. Sie besteht aus einer kurzen Eingangsfrage, an die sich mehree Aufforderungen anschließen, umfangreiche Dokumente vorzulegen. Sie lautet: „Wo sind die einzelnen Kameras installiert und welche räumlichen Bereiche werden mit ihnen jeweils beobachtet? Bitte legen Sie dazu eine Skizze und Fotos der Örtlichkeit (Bilder der Kameras in ihrem Umfeld) sowie für jede einzelne Kamera ein zuordenbares Bildschirmfoto (Screenshot, Bildschirmkopie, fotoähnliche Abbildung der aktuellen grafischen Wiedergabe der Kamera) des Erfassungsbereichs der Kamera vor, damit nachvollzogen werden kann, was die Kameras abbilden. Bitte geben Sie dabei auch an, ob Arbeitsplätze (Welche Art von Arbeitsplätzen? Kurzzeitig genutzte oder dauerhaft genutzte Arbeitsplätze?) von der Kamera erfasst werden."

Vorlage für schriftliche Prüfung

Die direkte Anrede bei einigen Fragen spricht dafür, dass die Aufsichtsbehörde den Fragenkatalog auch dazu verwendet, um auf schriftlichem Weg eine Art „Prüfung aus der Ferne" durchzuführen. Der Fragebogen ist abrufbar unter https://ogy.de/fragebogen-videoueberwachung. Er trägt kein Datum. Die Aufsichtsbehörde hat ihn mit Schreiben vom 19.6.2020 versandt.

Schutz von Baustellen

Videoüberwachung auf Baustellen

Die Videoüberwachung auf Baustellen erfolgt oft im Wege der Auftragsverarbeitung. Dabei ist ein Sicherheitsunternehmen als Auftragnehmer eines Bauunternehmens tätig (Art. 4 Nr. 8 DSGVO und Art. 28 DSGVO). Für die Rechtmäßigkeit der Verarbeitung und für die Einhaltung der damit verbundenen Pflichten (z.B. Informationspflichten nach Art. 13 DSGVO, insbesondere Anbringen von Hinweisschildern am überwachten Bereich) bleibt dabei der Bauunternehmer als Auftraggeber verantwortlich.

Er ist deshalb auch verpflichtet, der Aufsichtsbehörde auf ihre Anforderung hin Informationen bereitzustellen (Art. 58 Abs. 1 Buchst. a DSVO). Er kann die Aufsichtsbehörde nicht einfach an den Auftragnehmer verweisen.

Zwecke der Videoüberwachung

Als Zwecke für die Videoüberwachung auf Baustellen geben Bauunternehmen meist die Aufklärung von Diebstählen, Einbrüchen und Vandalismus an. Diese Zwecke stellen grundsätzlich berechtigte Interessen im Sinne von Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO dar. Dasselbe gilt für den Zweck, ein unberechtigtes Betreten der Baustelle während der Nachtzeit festzustellen.

Erforderlichkeit

Nach dem Grundsatz der Erforderlichkeit ist die Videoüberwachung nur soweit zulässig, wie sie notwendig ist, um diese Zwecke zu erreichen. Außerdem dürfen Grundrechte und Grundfreiheiten betroffener Personen nicht überwiegen.

- Daraus folgt, dass sich der Erfassungsbereich der Kameras auf die Bereiche beschränken muss, in denen mit Diebstählen, Einbrüchen, Vandalismus oder unberechtigtem Betreten zu rechnen ist.
- Regelmäßig genügt hierfür die Überwachung von Teilen der Baustelle.
- Die Überwachung von Bereichen, die unmittelbar an die Baustelle angrenzen, kommt nur ausnahmsweise in Betracht.

Die Videoüberwachung ist regelmäßig in zeitlicher Hinsicht zu beschränken. Die genannten Gefahren drohen üblicherweise außerhalb der Zeiten, in denen auf der Baustelle gearbeitet wird. Deshalb ist die Videoüberwachung in der Regel auf den Zeitraum außerhalb der Arbeitszeiten zu beschränken. Das dient dem Schutz der Beschäftigten.

Videoüberwachung von Beschäftigten

Die Videoüberwachung von Beschäftigten ist generell besonders problematisch. Das gilt v.a. dort, wo die Beschäftigten der Videoüberwachung nicht nur flüchtig oder vorübergehend ausgesetzt sind, sondern dauernd. Denn die Beschäftigten können sich der Überwachung häufig nicht entziehen, ohne ihre Pflicht zur Arbeit zu verletzen. Eine dauerhafte Überwachung von Mitarbeitern ließe sich deshalb nur mit äußerst gewichtigen Interessen des Arbeitgebers rechtfertigen. Diese Fälle werden sehr selten sein.

Videoüberwachung zur Diebstahlvermeidung

Soll die Videoüberwachung dazu dienen, Diebstähle zu vermeiden, also das Personal vom Diebstahl abzuhalten bzw. des Diebstahls zu überführen, so ist dies ausschließlich in den engen Grenzen von § 26 Abs. 1 Satz 2 BDSG zulässig. Diese Vorschrift ermöglicht bei einem konkreten Verdacht, der sich mit milderen Mitteln nicht aufklären lässt, ausnahmsweise eine Videoüberwachung. Sie muss dann zudem zeitlich und räumlich sehr eng auf die Aufklärung dieses Verdachts ausgerichtet sein. Eine rein vorbeugende, dauerhafte Videoüberwachung von Beschäftigten, um Diebstähle zu verhindern, wäre nicht zulässig.

Quelle: 16. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt für das Jahr 2019, Seiten 76/77. Der Bericht ist abrufbar unter https://ogy.de/tb-2019-sachsen-anhalt.

Bild: iStock.com/adekvat

DSFA

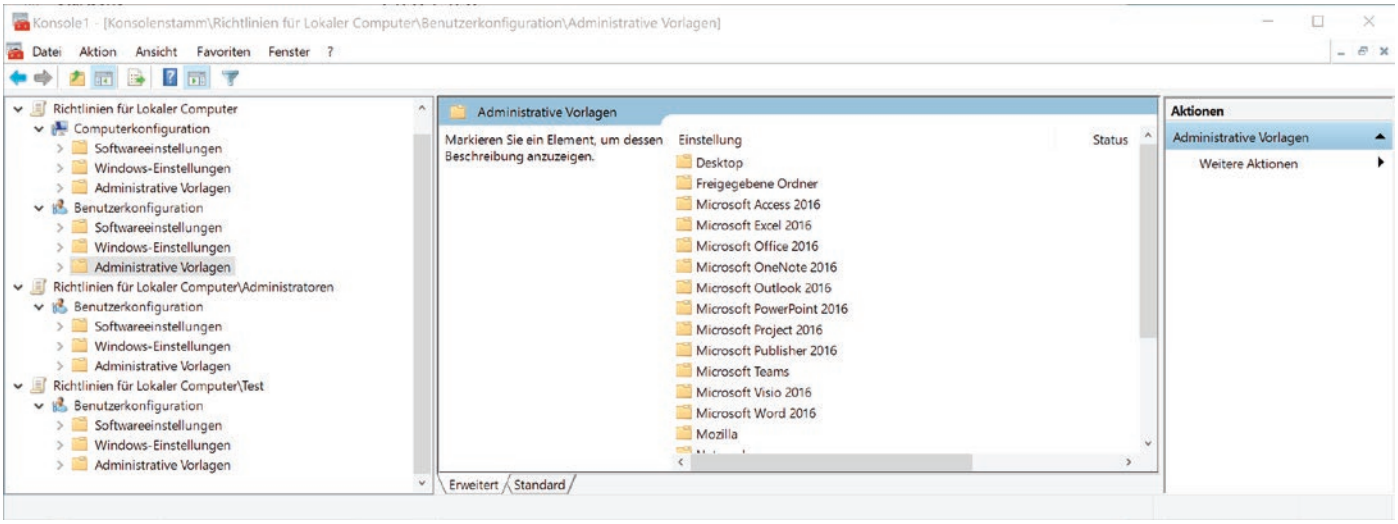
Kostenloser Leitfaden

Die Datenschutz-Folgenabschätzung (DSFA) gehört in vielen Unternehmen zu den noch kaum erledigten Aufgaben des Datenschutzes. Das Fraunhofer-Institut für System- und Innovationsforschung stellt dafür ein kostenloses Handbuch mit dem Titel „Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO“ zur Verfügung.

Gesamtüberblick

Auf der Basis eines Fünf-Phasen-Vorgehens erörtert das Werk schlaglichtartig die wesentlichen Fragen zur Datenschutz-Folgenabschätzung. Im Vordergrund steht dabei der Gesamtüberblick, weniger die Vertiefung komplexer Einzelfragen. Das Handbuch mit dem Stand Februar 2020 hat einen Umfang von 68 Seiten. Es ist abrufbar unter https://ogy.de/fraunhofer-dsfa.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken (Bayern). Er befasst sich seit vielen Jahren mit Fragen des Datenschutzes.



Screen: Rainer W. Gerling

Der Editor für die lokalen Gruppenrichtlinien mit den Vorlagen für die Einstellungen für Microsoft 365 (ehemals Office 365)

Berechtigungskonzept

So lassen sich auch wenige Rechner effizient managen

Wie schaffen es kleinste und kleine Unternehmen, Windows-Rechner einheitlich zu konfigurieren und die Berechtigungen der Rechner und Benutzer im Griff zu haben? Die lokalen Gruppenrichtlinien helfen weiter.

Für manche Unternehmen ist es keine Option, extra eine Windows-Domain einzurichten, um Gruppenrichtlinien (GPO) anwenden zu können und so für Einheitlichkeit im Berechtigungskonzept zu sorgen. Das ist wie mit Kanonen auf Spatzen zu schießen. Zum Glück gibt es aber lokale Gruppenrichtlinien (LGPO).

Wer Datenschutzbeauftragter für ein solches Unternehmen ist, muss vielleicht mehr ins Detail gehen bzw. eine Anleitung mitliefern. Daher stellen wir das Vorgehen bei lokalen Gruppenrichtlinien genau vor.

Die Voraussetzungen für Einstellungen schaffen

Um umfangreiche Einstellungen zu machen, müssen zuerst die Verwaltungsvorlagen installiert werden. Sie liegen im Ordner `%SYSTEMROOT%\PolicyDefinitions`. Wir laden uns die Verwaltungsvorlagen für Microsoft 365 (früher Office 365, https://ogy.de/vorlagen-365) und Windows 10 (https://ogy.de/vorlagen-windows-10) herunter und führen die Programme zum Entpacken aus. Bei den Windows-10-Vorlagen kopieren wir den Inhalt des Verzeichnisses – sowohl die admx-Dateien als auch die Verzeichnisse mit den Sprachdateien – in das Policy-Definitions-Verzeichnis auf allen Rechnern, die wir verwalten wollen.

Bei den Office-Vorlagen kopieren wir den Inhalt des admx-Verzeichnisses entsprechend. Den Inhalt des Admin-Verzeichnisses benötigen wir nicht. Die Excel-Tabelle dokumentiert die Einstellungen. Zum Kopieren sind Administrator-Rechte nötig. Auch für Software von Drittherstellern gibt es entsprechende Templates.

Die Vorlagen z.B. für Mozilla Firefox finden sich unter https://ogy.de/policy-templates-ff und für Google Chrome unter https://ogy.de/policy-templates-chrome.

Die Management-Konsole

Nun starten wir die lokale Microsoft-Management-Konsole. Dazu drücken wir die Windows-Taste und die R-Taste gleichzeitig und geben in die Zeile `mmc` ein. Ein Klick auf den OK-Button, und wir sehen die leere Konsole.

- Über „Datei ⇨ Snap-In hinzufügen/entfernen“ erhalten wir einen Auswahl-Dialog. Hier im linken Fenster den „Gruppenrichtlinienobjekt-Editor“ durch Klick auf den „Hinzufügen“-Button auswählen. Im sich öffnenden Fenster klicken wir auf den „Fertig-Stellen“-Button.
- Wir wiederholen das Ganze, klicken jetzt im aufgehenden Fenster auf den „Durchsuchen“-Button und gehen dann auf den Reiter „Benutzer“. Dort wählen wir „Administratoren“ aus. Nach Klick auf den „OK“-Button auf den „Fertig-Stellen“-Button gehen.
- In einem dritten Durchgang wählen wir auf der Seite „Benutzer“ einen realen Benutzer (z.B. Test) aus.

Dann sehen Sie die Ansicht wie im oben abgebildeten Screenshot.

BEISPIEL

Beispiele für Einstellungen

Es sind Computer-Einstellungen, Einstellungen für alle Benutzer, Einstellungen für die Gruppe der Administratoren und Einstellungen

für den Benutzer „Test“ möglich. Um die lokalen Gruppenrichtlinien bearbeiten zu können, sind Administrator-Rechte erforderlich. Möchten Sie z.B. verhindern, dass Mitarbeiter ausführbare Dateien von USB-Sticks starten? Dann aktivieren Sie unter „Richtlinien für Lokale Computer ⇨ Computerkonfiguration ⇨ Administrative Vorlagen ⇨ System ⇨ Wechselmedienzugriff“ die Option „Wechseldatenträger: Ausführungszugriff verweigern“.

Wollen Sie im Unternehmen „DNS über HTTPS“ (DoH) unterbinden (siehe Datenschutz PRAXIS 09/2019, Seite 16–17), ist das auch möglich. Das geht unter „Richtlinien für Lokale Computer ⇨ Benutzerkonfiguration ⇨ Administrative Vorlagen ⇨ Mozilla ⇨ Firefox“. Wird die Option „Aktiviert“ deaktiviert, ist DoH deaktiviert. Damit der Nutzer DoH nicht wieder aktivieren kann, muss zusätzlich die Option „Gesperrt“ aktiviert sein.

Was ist wo gespeichert?

- Alle Einstellungen, auf die das Betriebssystem und die Programme zugreifen, sind in der Registry gespeichert.
- Die lokalen Gruppenrichtlinien für den Computer und für alle Nutzer sind im Verzeichnis `%SYSTEMROOT%\System32\GroupPolicy` gespeichert.
- Die Vorgaben für Gruppen und Einzel-Nutzer finden sich in `%SYSTEMROOT%\System32\GroupPolicyUsers`.
- Die eigentlichen Richtlinien finden sich in der Datei `registry.pol`, die in den entsprechenden Verzeichnissen steht.

Was gilt?

Windows wendet die Einstellungen in unserem Szenario in dieser Reihenfolge an:

1. Fährt der Rechner hoch, werden die Computer-Richtlinien in die Registry übertragen.
2. Meldet sich der Nutzer an, werden die Richtlinien für alle Nutzer übertragen,
3. danach eine der beiden Richtlinien für die Gruppen Administratoren bzw. Nicht-Administratoren, und zuletzt
4. die Richtlinie für den Einzelnutzer.

Da die Gruppenrichtlinien die vorhandenen Einträge in der Registry überschreiben, „gewinnt“ immer die jeweils letzte Anwendung.

Die Einstellungen verteilen

Die Einstellungen nimmt die IT auf einem Rechner in der Management-Konsole vor. Auf diesem Rechner sollte die IT auch bei restriktiven Einstellungen mögliche Nebenwirkungen testen. Ist man damit fertig, kann die Verteilung beginnen.

Zuerst wird eine Netzwerkfreigabe (ein USB-Stick tut es auch) angelegt, auf den alle Rechner Zugriff haben (in den weiteren Beispielen `f:\lgpo`). An diesem Ort speichert man die LGPO.exe aus der Datei LGPO.ZIP des Microsoft Baseline Security Toolkit 1.0. Dann startet man diese Datei in einer Eingabeaufforderung mit administrativen Rechten (Starten mit „Als Administrator ausführen“): `lgpo /b f:\lgpo /n „Backup LGPO 10.5.2020 “`

Das Backup wird in einem Verzeichnis mit einem kryptischen Namen der Art „{9575E916-4D88-4689-BE35-7D368B-068CFB}“ abgelegt. Dieses Verzeichnis lässt sich jedoch umbenennen. Der Befehl `lgpo /g f:\lgpo\{9575E916-4D88-4689-BE35-7D368B068CFB}` spielt es auf dem gleichen oder einem anderen Rechner wieder ein.

Diese Verteilung funktioniert nur für Richtlinien, die jeweils unterhalb der Zweige „Administrative Vorlagen“ angesiedelt sind. Nur sie sind Registry-basiert.

Individuelle Einstellungen

Im Verzeichnis `GroupPolicyUsers` werden die Policy-Dateien unter der SID (= Security Identifier, ein eindeutiges Sicherheitskennzeichen) der Nutzer bzw. Gruppen gespeichert. Dabei sind die Gruppen „Administratoren (S-1-5-32-544)“ und „Benutzer (S-1-5-32-545)“ noch systemübergreifend einheitlich. Die SID eines Nutzers muss aber nicht überall gleich sein. Mit dem Befehl `wmic useraccount` lässt sich die Zuordnung Benutzername – SID anzeigen.

Die Richtlinie für Administratoren kann transferiert werden mit den beiden Befehlszeilen `copy %SYSTEMROOT%\System32\GroupPolicyUsers\S-1-5-32-544\User\Registry.pol f:\lgpo\grp_admin.pol` und `lgpo /ua f:\lgpo\grp_admin.pol`

Will man die Richtlinie für den Nutzer „Test“ übertragen, muss man im Copy-Befehl die SID und den Dateinamen (z.B. test.pol) ersetzen. Das erneute Einspielen auf einen anderen Rechner geht per `lgpo /u:test f:\lgpo\test.pol`

Die Kommandozeilen-Hilfe von LGPO.exe zeigt weitere Möglichkeiten an.

Fazit: einfach und kostengünstig

Stellt sich das Gefühl ein, bei der Anzahl der Rechner, die zu managen sind, ist der Aufwand doch zu groß, wird es Zeit, darüber nachzudenken, doch eine Windows-Domain einzurichten. Ansonsten sind die lokalen Gruppenrichtlinien (LGPO) eine einfache und kostenfreie Möglichkeit, umfangreiche Konfigurationen auf eine nicht zu große Zahl von Rechnern zu verteilen.

PRAXIS-TIPP

Die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur sicheren und datenschutzkonformen Konfiguration von Microsoft Office lassen sich relativ leicht per Gruppenrichtlinien umsetzen (https://ogy.de/bsi-empfehlungen-microsoft). Auch die Baseline-Sicherheitseinstellungen im Microsoft Baseline Security Toolkit 1.0 sind eine gute Sammlung von Einstellungen (https://ogy.de/compliance-toolkit).

Prof. Dr. Rainer W. Gerling ist Autor und Referent sowie stellvertretender Vorsitzender des Vorstands der GDD e.V. Er lehrt IT-Sicherheit an der Hochschule München.

Beide Bilder: Hailo

KI-Chips wie Hailo lassen sich in Endgeräten verbauen, damit Nutzer auf bestimmte KI-Dienste direkt zugreifen können, ohne einen Cloud-Dienst zu benötigen

Künstliche Intelligenz (KI)

Wie KI-Chips dem Datenschutz helfen können

Bei KI-Verfahren fehlt meist die Transparenz, wie sie personenbezogene Daten verarbeiten. Zudem erfolgt die Datenverarbeitung oft in einem US-Cloud-Dienst. KI-Chips könnten dies ändern, indem sie Teile der KI-basierten Datenverarbeitung direkt auf den Geräten ermöglichen.

In ihrem „Weißbuch Künstliche Intelligenz" (https://ogy.de/weissbuch-ki) hat die Europäische Kommission ihren Vorschlag eines Rahmens für vertrauenswürdige künstliche Intelligenz vorgestellt.

Da KI-Systeme in bestimmten Zusammenhängen komplex sein und erhebliche Risiken bergen könnten, sei es von entscheidender Bedeutung, Vertrauen aufzubauen, so die EU-Kommission. Vor allem KI-Systeme mit hohem Risiko benötigten klare Vorschriften:

- In Fällen mit hohem Risiko, z.B. in den Bereichen Gesundheit, Polizei oder Verkehr, sollten KI-Systeme transparent und rückverfolgbar sein.
- Die Aufsicht durch den Menschen müsse stets gewährleistet sein.
- Behörden sollten die Daten, die die Algorithmen nutzen, ebenso prüfen und zertifizieren können, wie sie es bei Kosmetika, Autos und Spielzeug tun.

Datenschutzgerechte KI braucht die richtige Infrastruktur

Dabei gibt es zwei Herausforderungen:

- Vielen KI-Lösungen mangelt es an Transparenz, eine Prüfung ist kaum möglich.
- Zudem findet die Datenverarbeitung bei vielen KI-Diensten innerhalb von US-Clouds statt.

Die Nationale KI-Strategie der Bundesregierung (https://ogy.de/nationale-ki-strategie) nennt deshalb als zentrales Anliegen den „Aufbau und Betrieb einer zentralen, nationalen, vertrauensvollen allgemein zugänglichen Daten- und Analyseinfrastruktur inklusive des Aufbaus einer zugrundeliegenden Cloud-Plattform mit skalierbarer Speicher- und Rechenkapazität".

Datenschutzgerechte, vertrauenswürdige KI erfordert also transparente Algorithmen und eine zuverlässige Daten- und IT-Infrastruktur. Neben dem geplanten Aufbau von KI-Diensten innerhalb der EU kommen dafür auch sogenannte KI-Chips infrage.

Was sind KI-Chips?

KI-Chips sind spezialisierte Computer-Chips, die lokal auf dem Endgerät oder auf einem Server KI-Dienste erbringen können. Die Daten, die die KI-Services verarbeiten, verlassen das Gerät nicht, so die Idee. Der Vorteil gegenüber einem Dienst, der in einer Cloud läuft, ist offensichtlich.

Die Marktforscher von Deloitte prognostizieren, dass im Jahr 2020 mehr als 750 Millionen KI-Chips verkauft werden. Damit sei aber das Ende der Fahnenstange noch nicht erreicht. Denn KI-Chips haben viele Vorteile, wenn es um Datenschutz, Datenübertragung und Echtzeit-Anwendungen geht, so die Analysten.

Welche Vor- und Nachteile haben KI-Chips?

Die Datenschutzkonferenz (DSK) nennt dazu passend als einen Prüfpunkt zum Datenschutz beim Einsatz von KI-Systemen in personenbezogenen Verarbeitungstätigkeiten:

„Kann die KI-Komponente rein lokal durch den Anwender genutzt werden, oder sind Onlineverbindungen bspw. zum Verantwortlichen oder zum Hersteller

der KI-Komponenten oder zu Dritten, die bspw. als Trainings-Provider agieren, notwendig?“

Wer mit KI-Chips arbeitet, kann die Verarbeitung rein lokal bei sich selbst intern vornehmen. Dabei ist es aber wichtig zu wissen, dass die Möglichkeiten einer chipbasierten KI im Vergleich zu einer cloudbasierten KI (noch) beschränkt sind.

Es kommt also darauf an, welche Dienste der Künstlichen Intelligenz ein KI-Chip genau erbringen kann und welche Cloud-Funktionen zusätzlich erforderlich sind. Das begrenzt den Datenschutzvorteil einer lokalen Verarbeitung.

Künstliche Intelligenz im Unternehmen bewerten

Hinweise der Datenschutzkonferenz zu KI

Die Datenschutzkonferenz (DSK) hat mehrere Entschließungen zu Künstlicher Intelligenz und zur datenschutzgerechten Gestaltung von KI-Lösungen veröffentlicht. Sie sind eine wichtige Hilfe dabei, den Einsatz von KI im Unternehmen zu bewerten:

- Hambacher Erklärung zur künstlichen Intelligenz – Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019 (https://ogy.de/hambacher-erklaerung)
- Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen (https://ogy.de/KI-DSK)
- Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen (https://ogy.de/Positionspapier-KI).

PRAXIS-TIPP

Das richtige Konzept beim Einsatz von KI-Chips aus Datenschutzsicht ist deshalb, möglichst alle personenbezogenen und personenbeziehbaren Daten auf Chip-Ebene zu verarbeiten und nur anonymisierte Daten an cloudbasierte KI-Dienste zu übergeben.

Welche datenschutzrelevanten Funktionen bieten KI-Chips bereits?

Auf dem Markt gibt es schon eine Fülle an KI-Chips. Sie bieten durchaus Funktionen an, die die Nutzer sonst aus KI-Cloud-Diensten beziehen würden und die personenbezogene Daten betreffen können.

Der KI-Chip Hailo (https://www.hailo.ai) z.B. kommt im Bereich teilautonomer Fahrzeuge, intelligenter Kameras, Smartphones, Drohnen sowie Augmented- und Virtual-Reality-Plattformen zum Einsatz. Der Chip erbringt bestimmte KI-Funktionen zur Bildverarbeitung. Sie müssen nicht als Cloud-Dienst bezogen werden.

GreenWave (https://greenwaves-technologies.com) bietet einen KI-Chip, der bei der Erkennung von Personen, bei der Gesichtserkennung, der Erfassung von Nummernschildern und bei der Anwesenheitsdetektion zum Einsatz kommen kann.

Qualcomm (https://www.qualcomm.com) hat KI-Chips, die einen lokalen digitalen Assistenten auf dem Endgerät ermöglichen. Lokale digitale Assistenten sind eine Alternative zu den cloudbasierten Assistenten wie Siri, Cortana und Alexa.

Aufsichtsbehörden empfehlen lokale KI-Dienste

In ihrem Positionspapier zur Entwicklung und zum Betrieb von KI-Systemen erklären die Aufsichtsbehörden, dass mit fortschreitender Technik zu erwarten ist, dass KI-Dienste vermehrt auf lokalen oder gar mobilen Geräten direkt ausgeführt werden, statt die Verarbeitung in einer Cloud durchzuführen.

Die Datenschutzkonferenz empfiehlt dabei: „Wann immer diese Möglichkeit besteht, sollte hiervon Gebrauch gemacht werden, um die Entstehung eingriffsintensiver Datensammlungen z. B. erlernter Gewohnheiten oder Vorlieben einer großen Anzahl von Personen zu vermeiden“ (Positionspapier Seite 16, https://ogy.de/Positionspapier-KI).

Genau hier setzen KI-Chips an, die eine (noch begrenzte) Möglichkeit zur lokalen, KI-basierten Datenverarbeitung bieten. Deshalb sollten Unternehmen, die den Einsatz von KI-Diensten planen, auch KI-Chips in Erwägung ziehen und wenn möglich gegenüber Cloud-KI-Diensten bevorzugen.

Datenschutz lässt sich auf Geräteebene prüfen

Es versteht sich, dass auch KI-Chips alle Anforderungen des Datenschutzes, wie sie z.B. die „Hambacher Erklärung zur künstlichen Intelligenz“ aufführt, erfüllen müssen. Auch die Dienste in KI-Chips müssen transparent, nachvollziehbar und erklärbar sein.

Der Vorteil ist aber, dass der Ort der Datenverarbeitung beim Anwender selbst liegt. Damit kann er die notwendigen Prüfungen also auf Geräteebene durch Experten vor Ort vornehmen lassen. Bei cloudbasierten KI-Diensten ist das dagegen nicht so leicht möglich.

Oliver Schonschek, Dipl.-Phys., ist Technology Analyst mit Fokus auf IT-Sicherheit und Datenschutz. Er ist zudem Host unserer Podcasts: https://ogy.de/dp-podcast.

Bild: iStock.com / http://www.fotogestoeber.de

Rechtsberatung gehört zu den grundlegenden Aufgaben eines DSB

Gefährliche Zurückhaltung

DSB und die Rechtsberatung

Manchmal sagen DSB, die nicht zugleich Rechtsanwälte sind, „Ich darf dazu keine Auskunft geben, das wäre Rechtsberatung". Was an diesem Satz dran ist und ob ein DSB nicht verpflichtet ist, zu datenschutzrechtlichen Fragen Stellung zu nehmen und zu beraten, klärt dieser Beitrag.

Die Antwort auf diese Punkte findet sich versteckt in einem Zusammenspiel zwischen dem Gesetz über außergerichtliche Rechtsdienstleistungen (RDG) und der Datenschutz-Grundverordnung (DSGVO).

Das sagt das RDG

Zweck des RDG ist es, die Rechtssuchungen, den Rechtsverkehr und die Rechtsordnung vor unqualifizierten Rechtsdienstleistungen zu schützen. Wer Rechtsdienstleistungen erbringen will, braucht dafür also eine Befugnis. Eine Rechtsdienstleistung ist gemäß § 2 Abs. 1 RDG „jede Tätigkeit in konkreten fremden Angelegenheiten, sobald sie eine rechtliche Prüfung des Einzelfalls erfordert."

Vertretung vor Gericht

Das RDG regelt nur außergerichtliche Rechtsdienstleistungen. Es sagt nichts über die Befugnis zur Vertretung vor Gericht aus. Herrscht Anwaltszwang, wie z.B. vor Landgerichten, kann der Datenschutzbeauftragte den Verantwortlichen nur vertreten, wenn er die entsprechende (Anwalts-)Zulassung hat.

Das sagt die DSGVO

Die wesentlichen Aufgaben des Datenschutzbeauftragten (DSB) schreibt Art. 39 DSGVO fest. Danach hat er u.a. die Pflicht,

- den Verantwortlichen im Bereich des Datenschutzrechts und der Datenschutzpraxis zu unterrichten und zu beraten sowie
- die Einhaltung von Rechtsvorschriften mit datenschutzrechtlichem Bezug im Allgemeinen zu überwachen.

Zu seinen Aufgaben gehört also z.B., datenschutzrechtliche Stellungnahmen zu diversen Sachverhalten wie zur Zulässigkeit einer beabsichtigten Videoüberwachung zu erstellen sowie Verträge mit Dienstleistern zu prüfen und zu bewerten. Das alles erfordert eine rechtliche Prüfung im Einzelfall.

Was würde es dem Verantwortlichen auch bringen, wenn der DSB nicht den Einzelfall beleuchtet? Insofern ist der überwiegende Teil seiner Tätigkeiten unter den Begriff der Rechtsdienstleistung zu subsumieren.

Fachkunde im Datenschutzrecht und in der Datenschutzpraxis

Hinzu kommt: Wesentliche Voraussetzung für die Benennung des DSB ist seine Fachkunde im Datenschutzrecht und der Datenschutzpraxis (siehe Erwägungsgrund 97 DSGVO). Er muss also rechtliche Bewertungen vornehmen können.

Dass der konkrete Umfang stark vom Einzelfall und vom jeweiligen Unternehmen abhängt, hat keinen Einfluss. Es dürfte praktisch keine Situation und kein Unternehmen geben, in denen der DSB nicht zumindest „einmal" eine rechtliche Prüfung und Bewertung im Einzelfall (siehe § 2 Abs. 1 RDG) vornehmen muss.

Rechtsdienstleistung als zulässige Nebenleistung

Bei der Frage, ob der DSB die im Rahmen seiner Aufgaben zu erbringenden Rechtsdienstleistungen vornehmen darf, hilft ein Blick in § 3 RDG. Hiernach ist die selbstständige Erbringung außergerichtlicher Rechtsdienstleistungen nur in dem Umfang zulässig, wie sie das RDG oder ein anderes Gesetz erlaubt.

Der DSB könnte sich auf § 5 Abs. 1 RDG berufen. Danach ist eine Rechtsdienstleistung erlaubt, wenn sie erforderlich ist, um die Haupttätigkeit auszuüben. DSB üben – auch nach Ansicht von Bundesfinanzhof (BFH) und Bundesgerichtshof (BGH) – einen völlig eigenständigen Beruf mit einem eigenen Berufsbild aus.

So führte der BGH u.a. aus, dass der Kern und der Schwerpunkt der Tätigkeit des DSB im Grunde die Auslegung und An-

wendung datenschutzrechtlicher Vorgaben ist, was u.a. umfangreiche juristische Kenntnisse voraussetzt. Wofür bräuchte er solche Kenntnisse, wenn er damit – aufgrund des RDG – nichts anfangen könnte?

WICHTIG

Zur Haupttätigkeit „DSB" gehört daher zweifelsohne die Erbringung von Rechtsdienstleistungen. Diese sind auch zwingend erforderlich, da sie im Hinblick auf die gesetzlichen Aufgaben des DSB untrennbar mit dieser Funktion verbunden sind. Folglich darf und muss der DSB im Rahmen seiner Tätigkeit Rechtsdienstleistungen erbringen.

In der Praxis sieht man leider allzu oft DSB, die nicht selbst datenschutzrechtlich beraten, sondern auf einen externen Anwalt verweisen – mit zusätzlichen Kosten für den Verantwortlichen. Das ist in der Regel eine schwerwiegende Verletzung der gesetzlichen Pflichten des DSB, selbst wenn sie auf dem Trugschluss beruht, nicht beraten zu dürfen. Das kann zur fristlosen Kündigung und Abberufung führen.

Was darf der DSB nicht?

In der Praxis gibt es jedoch einige Sachverhalte, die der DSB nicht erledigen darf. Beispiel: Der Inhaber einer Arztpraxis möchte weitere Praxen zum Ausbau seines Unternehmens erwerben. Er bittet seine DSB darum, entsprechende Verträge zu erstellen (z.B. Übernahmevertrag und Verwahrvertrag für die Patientenakten).

Zwar besitzen die Verträge auch datenschutzrechtliche Inhalte, etwa Klauseln, wie die Übergabe der Patientenakten nach erfolgter Einwilligung zu handhaben ist. Jedoch darf die DSB nur im Hinblick auf diese Klauseln beraten, nicht hingegen hinsichtlich der sonstigen Klauseln abseits des Datenschutzrechts. Die Beratung in rein zivilrechtlichen Fragen lässt sich weder als Nebenleistung zum Berufsbild und zur Haupttätigkeit zählen, noch ergibt sich etwas anderes aus der DSGVO.

Auch wenn die Abgrenzung im Einzelfall nicht immer einfach ist, so sollte sich jeder DSB auf das besinnen, was er kann, nämlich die Vorschriften des Datenschutzrechts auszulegen und anzuwenden. Dem Datenschutzrecht (sach-)fremde Fragen sollte und muss der DSB unbeantwortet lassen.

Fazit: Ein DSB darf und muss beraten

Ein DSB darf also Rechtsdienstleistungen erbringen – und er muss es im Rahmen seiner Tätigkeiten gemäß Art. 37 bis 39 DSGVO auch. Das RDG sieht entsprechende Ausnahmetatbestände vor. Tut er dies nicht, kann das erhebliche Konsequenzen für den Verantwortlichen und für den Datenschutzbeauftragten selbst haben.

Es ist unklar, woher dieser Mythos stammt. Umso wichtiger ist es, allen DSB klar zu machen, dass es sich um einen solchen handelt. Sofern der Datenschutzbeauftragte die bestehenden Grenzen (und Graubereiche) beachtet, steht einer rechtsberatenden Tätigkeit nichts im Weg. In diesem Zusammenhang hat der BvD e.V. übrigens erst kürzlich gefordert, klarzustellen, dass die Tätigkeit des DSB kein Verstoß gegen das RDG ist (https://ogy.de/bvd-rdg).

Was ist keine Rechtsdienstleistung im Sinne des RDG?

Einige Tätigkeiten fallen erst gar nicht unter den Begriff der Rechtsdienstleistung. Diese Dienste kann grundsätzlich jeder erbringen. Hierzu zählen gemäß § 2 Abs. 3 RDG etwa wissenschaftliche Gutachten zu einem bestimmten Thema oder an die Allgemeinheit gerichtete Darstellungen von Rechtsfragen und Rechtsfällen in den Medien.

Dr. Kevin Marschall ist Geschäftsführer der GDPC GbR, einer auf Datenschutz spezialisierten Unternehmensberatung mit Sitz in Kassel.

IMPRESSUM

Verlag:
WEKA MEDIA GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA MEDIA GmbH & Co. KG
Gesellschafter der WEKA MEDIA GmbH & Co. KG sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG und als Komplementärin:
WEKA MEDIA Beteiligungs-GmbH

Geschäftsführer:
Stephan Behrens, Michael Bruns, Wolfgang Materna

Redaktion:
Ricarda Veidt, M.A. (V.i.S.d.P)
E-Mail: ricarda.veidt@weka.de

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 082 33.23-5 72 68
E-Mail: anton.sigllechner@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-740
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben 219,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 20 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
metamedien
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4079

ISSN-Nr.:
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

Technisch-organisatorische Maßnahmen

Kein Zutritt mit ohne Gesichtsmaske

In vielen Unternehmen und Behörden müssen die Beschäftigten derzeit zumindest in bestimmten Bereichen Gesichtsmasken tragen. Das stellt manche Technik vor besondere Herausforderungen.

Für die eindeutige Identifikation durch biometrische Merkmale gelten beim Datenschutz eigene Regeln. Das betrifft v.a. die Gesichtserkennung und den biometrischen Fingerabdruck, beides Methoden, die bei mobilen Geräten wie Smartphones, Tablets und Notebooks zum Einsatz kommen. Sie dienen aber auch der Zutrittskontrolle in sensible Bereiche.

Gesichtserkennung streikt bei der Maske

Eigentlich funktionieren diese Systeme eher unspektakulär. Aber seit Corona ist vieles anders. Plötzlich ist die Gesichtserkennung bei der Zutrittskontrolle vor eine besondere Herausforderung gestellt.

In einem Unternehmen verweigerte sich die Gesichtserkennung an der Tür zum Rechenzentrum, als einzelne Kollegen eine Gesichtsmaske trugen. Also wurde das System umprogrammiert. Erkannte das System typische Merkmale einer Gesichtsmaske, erfolgte die akustische Aufforderung: „Bitte nehmen Sie Ihre Gesichtsmaske ab!“ Erst dann war die Identifikation und damit der Zutritt möglich.

Sonderfall Make-up

Die einzige Kollegin im Kreis der Zutrittsberechtigten legte gern öfter Make-up auf. Nach Auffassung der Kollegen manchmal etwas zu viel. Deshalb trug sie auch in den Hochzeiten von Corona nie eine Gesichtsmaske. Umso größer war ihre Überraschung, als das System sie aufforderte, doch bitte die Gesichtsmaske abzunehmen. Sehr zur Freude der „zufällig“ anwesenden Kollegen aus dem Team.

Des Rätsels Lösung: Der Entwickler, der für die Änderung der Gesichtserkennung zuständig war, hatte für die Kollegin einprogrammiert, dass sie auch ohne Gesichtsmaske diese Aufforderung bekam.

Unbefugte Nutzung biometrischer Daten

Da es sich neben einem fragwürdigen Umgang mit Kollegen um eine unbefugte Nutzung biometrischer Daten handelte, hatte der „Spaß“ allerdings schnell ein Ende. Der Datenschutzbeauftragte wurde eingeschaltet. Nach einem klärenden Gespräch gibt es jetzt auch bei Gesichtsmasken keine Sonderfälle mehr.

Eberhard Häcker ist seit vielen Jahren externer Datenschutzbeauftragter. Da er in zahlreichen verschiedenen Branchen berät, ist sein Erfahrungsschatz riesig.

IN DER NÄCHSTEN AUSGABE

Microsoft Teams

Eines der häufig verwendeten Videokonferenz-Systeme ist derzeit Teams. Doch wie steht es hier um den Datenschutz?

Best Practice Cybersicherheit

Medizinische Einrichtungen sind immer stärker Ziel von Cyberangriffen. Lesen Sie, wie sie sich dagegen schützen können.

Fiebermessen bei Beschäftigten

In Zeiten von Corona ein wichtiges Thema im Beschäftigtendatenschutz. Was geht, was geht nicht?