Republik Österreich
Datenschutzbehörde

NEWSLETTER 3/2020

Datenschutzrechtliche Implikationen von Contact-Tracing-Apps

Mag. Andreas Zavadil

Kurz nach Ausbruch der aktuellen Ausnahmesituation rund um COVID-19 waren sogenannte „Contact-Tracing-Apps“ Gegenstand zahlreicher Diskussionen. Bei diesen Apps handelt es sich – vereinfacht formuliert – um elektronische Kontaktbücher, die es ermöglichen sollen, mit Hilfe eines Endgeräts über Bluetooth einen Kontaktabgleich mit Menschen in der Umgebung durchzuführen. In Folge werden die generierten Kontakte eine gewisse Zeit lang gespeichert. Kommt es innerhalb dieses Zeitfensters dazu, dass ein gespeicherter Kontakt die Meldung abgibt, dass dieser positiv auf SARS-CoV-2 getestet wurde, wird eine entsprechende Warnung versendet, dass möglicherweise Nahkontakt mit einer infizierten Person bestanden hat.

Der gegenständliche Beitrag beleuchtet die datenschutzrechtlichen Rahmenbedingungen, unter denen der Einsatz von solchen Apps – und damit einhergehend, der Eingriff in das Grundrecht auf Datenschutz – zulässig ist und geht weiters auf die Bedeutung der Interoperabilität zwischen Apps ein.

Ganz zu Beginn stellt sich die Frage, welches Ziel Contact-Tracing-Apps verfolgen und welche Rolle solche Apps im Rahmen der jeweils nationalen Pandemiestrategie einnehmen. Aufgrund der Vielfalt an national entwickelten Apps – so gibt es keine „EU Corona App“ – und der unterschiedlichen Zugangsweisen gibt es darauf keine einheitliche Antwort. Als gemeinsamer Nenner lässt sich aber dem Grunde nach festhalten, dass diese Apps ergänzend zu manuellem Contact-Tracing (etwa durch Gesundheitsbehörden) eingesetzt werden und dass Infektionsketten möglichst früh erkannt und unterbrochen werden sollen. Dies dient im Ergebnis dazu, dass die Reproduktionszahl unter einen Wert von Eins sinkt (dies bedeutet, dass eine infizierte Person weniger als eine weitere Person ansteckt). Die Senkung der Reproduktionszahl und die damit verbundenen Folgen – insbesondere die Verhinderung des Zusammenbruchs des Gesundheitssystems – ist ohne Zweifel ein gewichtiges öffentliches Interesse.

In Folge stellt sich die Frage, ob der Einsatz von Contact-Tracing-Apps überhaupt geeignet ist, um das soeben dargestellte Ziel zu erreichen. Diesbezüglich ist festzuhalten, dass elektronisches Contact-Tracing im Einzelfall durchaus zur frühen Unterbrechung einer Infektionskette führen kann, selbst wenn dieser Einzelfall keine (nennenswerte) Auswirkung auf die epidemiologische Gesamtsituation hat. Die Geeignetheit ist daher grundsätzlich zu bejahen.

Im Hinblick auf die Erforderlichkeit von derartigen Apps – also der Frage, ob gelindere Mittel zur Zieler-

reichung vorhanden sind – ist festzuhalten, dass es unterschiedliche Mittel gibt, die kombiniert werden müssen, um die Reproduktionszahl zu senken. Der Einsatz einer Contact-Tracing-App kann daher neben weiteren Maßnahmen (Schließung von Geschäften, Kontakteinschränkungen, Maskenpflicht u.a.) eine wichtige Rolle im Rahmen einer Pandemiestrategie einnehmen.

Schließlich ist zu hinterfragen, ob der mit der Nutzung einer solchen App verbundene Eingriff in das Grundrecht auf Datenschutz angemessen ist. Die Beantwortung dieser Frage hängt von der konkreten Gestaltung der jeweiligen App ab. Neben vielen Institutionen haben auch der Europäische Datenschutzausschuss in den Leitlinien 4/2020 sowie die Europäische Kommission im Rahmen der Mitteilung 2020/C 124 I/01 Anforderungen für den Einsatz von Contact-Tracing-Apps formuliert.

Dazu ist grundsätzlich festzuhalten, dass im Rahmen der (Weiter-) Entwicklung von Contact-Tracing-Apps die Grundsätze „Privacy by Design" und „Privacy by Default" gemäß Art. 25 DSGVO zu beachten sind. Insbesondere ist genau festzulegen, welche Funktionen die jeweilige App besitzen soll, welche personenbezogenen Daten hierfür notwendigerweise verarbeitet werden müssen, wie lange Daten gespeichert werden und wie ein angemessenes Datenschutzniveau gewährleistet wird. Die im Rahmen der App gesammelten Daten dürfen ausschließlich zum Zwecke des Contact-Tracing zur Unterstützung der Bekämpfung der COVID -19 Pandemie verwendet werden. Sofern ein weiterer Verarbeitungszweck hinzutritt – wie etwa die Überwachung von Quarantänemaßnahmen oder die Erstellung von (individuellen) Bewegungsprofilen mithilfe der App – handelt es sich nicht mehr um Contact-Tracing-Apps im Sinne des gegenständlichen Beitrags und ist dies mit einem weitaus intensiveren Eingriff in das Grundrecht auf Datenschutz verbunden.

Im Hinblick auf die Zulässigkeit der Datenverarbeitung wird in den oben genannten Quellen wiederholt auf die Freiwilligkeit der Nutzung einer solchen App verwiesen. In diesem Zusammenhang ist zu bemerken, dass Contact-Tracing die Speicherung und/oder den Zugang zu Informationen, die bereits im Endgerät gespeichert sind, voraussetzt, weshalb Art. 5 Abs. 3 der Richtlinie 2002/58/EG idgF einschlägig ist. Für die Verarbeitung von Gesundheitsdaten – etwa der Meldung einer Infektion – kommt insbesondere die datenschutzrechtliche Einwilligung iSd DSGVO in Betracht. Die DSB weist an dieser Stelle auf ihre stRsp hin, wonach einem Betroffenen kein Nachteil für den Fall erwachsen darf, dass eine Einwilligung nicht abgegeben wird (vgl. den Bescheid vom 30. November 2017, GZ: DSB-D122.931/0003-DSB/2018 mwN). Die Abgabe einer informierten Einwilligung setzt zudem die vollständige Einhaltung des Transparenzgrundsatzes und der Informationspflichten voraus.

Umgelegt auf die gegenwärtige Situation bedeutet dies, dass kein Betroffener benachteiligt werden darf, sofern dieser keine Contact-Tracing-App nutzt.

Der Europäische Datenschutzausschuss verweist weiters darauf, dass anstelle der Einwilligung eine qualifizierte Rechtsgrundlage als Erlaubnistatbestand für die Datenverarbeitung in Betracht kommt, wobei auch diesfalls die Freiwilligkeit der Teilnahme sowie eine entsprechende Diskriminierungsfreiheit im Falle einer Nichtteilnahme sichergestellt sein muss.

Auf nationaler Ebene hat der Gesetzgeber etwa in § 15 Abs. 3 Epidemiegesetz 1950 idgF normiert, dass das Zusammenkommen von Menschenmengen nicht an die Verwendung von Contact-Tracing-Technologien geknüpft werden darf. Die Schaffung weiterer geeigneter Garantien wäre wünschenswert. Sofern derartige Apps (zumindest auch) von staatlicher Seite als Verantwortliche betrieben werden, ist die Schaffung einer klaren gesetzlichen Grundlage bereits aufgrund des Legalitätsprinzips notwendig.

Zur konkreten technischen Ausgestaltung sei – neben vielen Anforderungen – an dieser Stelle jedenfalls erwähnt, dass kein Zugriff von Dritten auf personenbezogene Daten möglich sein darf. Da das Contact-Tracing ohne Identifizierung von konkreten Personen zu erfolgen hat, sind Mechanismen zu implementieren, um das Risiko für die Herstellung eines Personenbezugs soweit wie möglich zu reduzieren. Hierzu wird empfohlen, dass Kontaktabgleiche dezentral verarbeitet und verschlüsselt am Endgerät des Nutzers gespeichert werden. Weiters wird empfohlen, die von der App gesendeten pseudonymen Kennungen („IDs") regelmäßig zu rotieren.

Zuletzt ist auf das Thema der Interoperabilität einzugehen. Wie bereits eingangs ausgeführt sind zahlreiche nationale Contact-Tracing-Apps im Einsatz und gibt es derzeit keine „EU Corona App". Dies hat zur Folge, dass Contact-Tracing im Falle des Aufenthaltes in einem anderen Staat aufgrund der unterschiedlichen Ausgestaltung der jeweiligen App nur schwer oder gar nicht durchführbar ist. In Anbetracht der sukzessiven Grenzöffnungen und der weitgehenden Rückkehr des sozialen Lebens ist ein funktionierendes grenzüberschreitendes Contact-Tracing für den Erfolg derartiger Apps aber unumgänglich. Der Europäische Datenschutzausschuss hat sich in seiner Stellungnahme vom 16. Juni 2020 mit diesem Thema bereits aus rechtlicher und technischer Sicht auseinandergesetzt, worauf verwiesen wird.

An dieser Stelle wird auch auf die Rolle der von Google und Apple entwickelten API für die Smartphone-Betriebssysteme Android und iOS hingewiesen. Hierbei handelt es sich um eine Contact-Tracing-Schnittstelle

zur Programmierung von Anwendungen, die ein systemübergreifendes Contact-Tracing auf Bluetooth-LE-Basis ermöglichen soll. Es ist festzuhalten, dass Google und Apple keine App betreiben; vielmehr können sich die Betreiber der jeweiligen Contact-Tracing-App dieser Schnittstelle bedienen, um die Bluetooth Low Energy Funktechnik in Smartphones zu nutzen und die Interoperabilität mit anderen Contact-Tracing-Apps zu fördern. Die technischen Spezifikationen wurden seitens Apple und Google veröffentlicht und auch gegenüber den Aufsichtsbehörden erläutert. Eine Überprüfung seitens der (zuständigen) irischen Aufsichtsbehörde ist anhängig.

Abschließend weist die DSB darauf hin, dass das Datenschutzrecht kein Hindernis für den Einsatz einer Contact-Tracing-App (und allgemein, für die Bekämpfung der aktuellen Pandemie) darstellt; unter den im gegenständlichen Beitrag erläuterten Bedingungen steht dem Einsatz einer solchen App nichts im Wege. Die Einhaltung der datenschutzrechtlichen Vorgaben ist – im Gegenteil – eine notwendige Voraussetzung für den Erfolg von Contact-Tracing-Apps, da solche Apps ansonsten auf keine breite Akzeptanz in der Bevölkerung stoßen werden. Das Vertrauen der Bevölkerung ist zwingend erforderlich, damit die jeweilige Contact-Tracing-App auch heruntergeladen wird.

Im Fokus

Mag. Andreas Zavadil

Information Lehrerbewertungsplattform Lernsieg

Im Rahmen des amtswegigen Prüfverfahrens zur Zahl DSB-D213.953 wurde die datenschutzrechtliche Zulässigkeit der App „Lernsieg“ überprüft. Bei der App Lernsieg handelt es sich um eine Bewertungsplattform, auf der Schüler ihre Schule und ihre Lehrer nach einem vorgegebenen Punktesystem bewerten können. Zu den einzelnen bewertbaren Kriterien zählen (derzeit): Unterricht, Respekt, Geduld, Erklärungsstil, Persönlichkeit, Fairness, Motivation und Organisation. Der Betreiber der App (in Folge: „der Verantwortliche“) hat sich im Hinblick auf die Verarbeitung der Lehrerdaten (Name, Dienststelle, zugehörige Bewertungen) auf die Rechtsgrundlage gemäß Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen) gestützt, weshalb in Folge eine Interessenabwägung durchzuführen war.

Der Verantwortliche brachte dazu vor, dass durch die Verarbeitung das Interesse der Ausübung des Rechts auf freie Meinungsäußerung und Information nach Art. 11 EU-GRC verfolgt werde, wobei dieses Grundrecht auch den Empfang von Informationen beinhalte. So solle eine verstärkte Transparenz im Bereich der Bildung erreicht werden und die Qualität der Ausbildung im Unterricht einer nachvollziehbaren Kontrolle zugänglich sein. Insgesamt könne durch die erfassten Bewertungen die Unterrichtsqualität gesteigert und den Schülern eine bessere Möglichkeit für ihre Entwicklung geboten werden.

Aus Sicht der betroffenen Personen war zu berücksichtigen, dass sich Lehrer durch die gegenständliche Datenverarbeitung einer anonymen Bewertung aussetzen müssen, dass grundsätzlich auch Nichtschüler des jeweiligen Lehrers eine Bewertung abgeben können, dass diese Bewertung mitunter nicht den wahren Gegebenheiten entspricht (etwa unsachliche Bewertungen) und dass diese Bewertungen der Öffentlichkeit preisgegeben werden und es zu einer Prangerwirkung kommen kann.

Diesbezüglich war zunächst festzuhalten, dass die anonyme Nutzung dem Internet immanent ist und dass die Verpflichtung, sich namentlich zu einer bestimmten Bewertung zu bekennen, die Gefahr begründen würde, dass der Bewertende aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich entscheidet, seine Meinung gar nicht zu äußern. Eine solche Selbstzensur ist nach Auffassung der DSB nicht mit Art. 11 EU-GRC vereinbar. Ebenso wenig ist das Recht auf freie Meinungsäußerung und Information auf objektivierbare allgemein gültige Werturteile beschränkt.

In Anlehnung an die stRsp der DSB zu Ärztebewertungsplattformen (vgl. den Bescheid vom 15. Jänner 2019, GZ DSB-D123.527/0004-DSB/2018 mwN) war auch festzuhalten, dass die gegenständliche Lehrerbewertung die berufliche Tätigkeit des Lehrers betrifft, sohin einen Bereich, in dem sich die persönliche Entfaltung von vornherein im Kontakt mit der Umwelt vollzieht. Die Berufsgruppe der Lehrer muss sich daher auf die Beobachtung ihres Verhaltens durch eine breite Öffentlichkeit und auf Kritik an den Leistungen einstellen. Im vorliegenden Fall ist nämlich die berufliche Sphäre betroffen, die im Gegensatz zur intimen Sphäre einen geringeren Schutz genießt.

Darüber hinaus hat der Verantwortliche mehrere Mechanismen implementiert, um einer Prangerwirkung entgegenzuwirken: So ist es bspw. zum Schutz vor Missbrauch notwendig, dass sich der Bewertende zunächst über eine Telefonnummer (die nicht gespeichert oder anderweitig verwendet wird) verifiziert („Überwinden einer Hemmschwelle“), ist eine gewisse Mindestanzahl an Bewertungen erforderlich, bevor diese angezeigt wird, ist die Abgabe eines persönlichen, mitunter beleidigenden Kommentars nicht möglich (wobei im Gegenzug dafür die Bewertung in Form von Unterkategorien näher begründet werden kann) oder ist ein Melde- und Änderungsbutton für Lehrer eingebaut. Der Verantwortliche hat auch keine Volks- und Sonderschulen in

die App aufgenommen und die Bewertungsmöglichkeit somit an ein gewisses Mindestalter bzw. geistige Entwicklung geknüpft.

Kritisch zu hinterfragen war, dass – anders als etwa bei einer Ärztebewertungsplattform und der damit im Zusammenhang stehenden freien Arztwahl – grundsätzlich keine freie Lehrerwahl besteht. Allerdings existiert insofern eine indirekte Lehrerwahl, als Eltern (im Einvernehmen mit ihren Kindern, also den Schülern) die Schule auswählen und sich ein entsprechendes Bild über die dort konkret tätigen Lehrkräfte machen können und für gewisse Fächer (etwa Wahlfächer) durchaus eine freie Lehrerwahl bestehen kann. Ebenso ist die konkrete Lehrerbewertung für die Beurteilung der Auswahl von Schwerpunktschulen (etwa, ob die fachlichen Schwerpunkte der Schule auch mit entsprechender Qualität umgesetzt werden) relevant. Weiters können Bewertungen eines Lehrers Anlass dazu geben, dass Schüler oder Eltern ein Gespräch mit dem Lehrer (oder umgekehrt) suchen. Der Umstand, dass es sich gegenständlich um eine vergleichsweise neue App handelt und diese für die Schulwahl der breiten Bevölkerung womöglich noch keine große faktische Bedeutung hat, ist nach Auffassung der DSB nicht ausschlaggebend. Bewertungsplattformen können einen Mehrwert für die Gesellschaft in Form von einfach zugänglichen Informationen bieten, wobei jede Bewertungsplattform eine gewisse Anlaufzeit benötigt, um eine entsprechende Relevanz zu erreichen.

Vor dem Hintergrund dieser Überlegungen gelangte die DSB zu dem Ergebnis, dass die Verarbeitung der Lehrerdaten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO rechtmäßig erfolgt, die Interessen der breiten Allgemeinheit und insbesondere der Schüler an der gegenständlich relevanten Verarbeitung also überwiegen.

Zur Vollständigkeit ist festzuhalten, dass auch die Verarbeitung der Daten der Bewerter (Kinder bzw. Jugendliche) überprüft wurde und diesbezüglich nichts zu beanstanden war. Insbesondere wurde aufgrund des Ermittlungsverfahrens festgestellt, dass die Daten der Bewerter in keiner Form (etwa zu Werbezwecken) verwendet oder an Dritte übermittelt werden. Die DSB wird die Entwicklung der App Lernsieg jedoch weiterhin beobachten und behält sich im Falle einer solchen Kommerzialisierung die Einleitung eines weiteren Prüfverfahrens vor.

Ausgewählte Entscheidungen der DSB

DSB-D124.720 2020-0.280.699, Verletzung im Recht auf Geheimhaltung: Verarbeitung eines Lichtbildausweises aufgrund eines Geldwechsel im Gegenwert von 100 Euro

Im Bescheid vom 28. Mai 2020 zur GZ: DSB-D124.720 2020-0.280.699 hatte sich die Datenschutzbehörde mit einer Beschwerde im Recht auf Geheimhaltung (§ 1 DSG) und dem Finanzmarkt-Geldwäschegesetz (FM-GwG) zu befassen.

Der Beschwerdeführer wollte in einer Bankfiliale 100 Euro in Türkische Lira (TRY) wechseln lassen. Daraufhin wurde er vom Bankmitarbeiter aufgefordert, einen Lichtbildausweis für den Wechsel vorzulegen, bei sonstigem Abbruch des Geldwechsels. Der Beschwerdeführer weigerte sich vorerst, aber schließlich legte er seinen Führerschein vor, welcher kopiert und gespeichert wurde.

Die Bank als Beschwerdegegnerin begründete die gegenständliche Verarbeitung des Lichtbildausweises mit ihren Obliegenheiten aufgrund des FM-GwG. Demnach habe sie ohne Rücksicht auf die Höhe des ein- und auszahlenden Betrages, bei bloßem Verdacht hinsichtlich Geldwäsche oder Terrorismusfinanzierung (§ 5 Z 4 FM-GwG) Sorgfaltsmaßnahmen anzuwenden und im Zweifel Identitätsdokumente gemäß § 6 Abs 1 Z 1 FM-GwG zu verlangen. Seine Weigerung sei als auffälliges Kundenverhalten interpretiert worden. Darüber hinaus sei es dem Bankfilialleiter erinnerlich gewesen, dass der Beschwerdeführer bei einer höheren Bundesbehörde gearbeitet habe, daher sei gemäß § 2 Z 6 iVm § 11 FM-GwG eine PeP (Politisch exponierte Person) Prüfung durchzuführen gewesen.

Die Datenschutzbehörde gab der Beschwerde statt und stellte eine Verletzung im Recht auf Geheimhaltung fest, da es sich bei dem Geldwechsel des Beschwerdeführers im Gegenwert von 100 Euro jedenfalls um einen Betrag unterhalb der Wertgrenze von 1.000 Euro, bzw. 15.000 Euro des § 5 Z 2 FM-GwG handle. Weiters kann allein aus einer Weigerung, einen Lichtbildausweis vorzulegen, noch nicht geschlossen werden, dass es sich bei einem Geldwechsel um Terrorismusfinanzierung oder Geldwäsche handelt. Darüber hinaus ist ein Bediensteter einer höheren Bundesbehörde nicht gleichbedeutend mit einer PeP-Eigenschaft, wonach es sich beispielsweise um Staatschefs, Parlamentsabgeordnete oder Verfassungsrichter handle. Daher lag keine Rechtfertigung für die gegenständliche Verarbeitung von personenbezogenen Daten vor.

Dieser Bescheid ist nicht rechtskräftig.

DSB-2020-0.251.582 (D124.1791), Unerlaubte Einsichtnahme in Patientenakte

Im Bescheid vom 20.05.2020, GZ: DSB-D2020-0.251.582 (D124.1791), hatte sich die DSB mit dem Vorwurf der unerlaubten Einsichtnahme eines Ordinationsgehilfen in die Patientenakte eines Betroffenen zu befassen.

Die Beschwerdeführerin brachte in ihrer Beschwerde zunächst vor, dass sie sich bei der Beschwerdegeg-

nerin in ärztlicher Behandlung befunden habe. Aufgrund eines versäumten Arzttermins sei es zwischen ihr und dem Ordinationsgehilfen der Beschwerdegegnerin zu einem Disput gekommen und habe sie in der Folge eine negative Bewertung zur Beschwerdegegnerin im Internet abgegeben. Daraufhin, so der Verdacht der Beschwerdeführerin, habe der Ordinationsgehilfe Einsicht in ihre Patientenakte genommen, um so die Daten ihres Arbeitgebers ausfindig zu machen, um selbst im Internet eine negative Bewertung zur Beschwerdeführerin abzugeben.

Im Rahmen des Verfahrens vor der Datenschutzbehörde brachte die Beschwerdegegnerin bzw. der Ordinationsgehilfe vor, dass die abgegebene Bewertung nicht in Zusammenhang mit der Beschwerdeführerin stehen würde, sondern eine andere Mitarbeiterin des Arbeitgebers der Beschwerdeführerin gemeint gewesen wäre.

Nach der Durchführung des Ermittlungsverfahrens sah es die Datenschutzbehörde als erwiesen an, dass die Bewertung des Ordinationsgehilfen gegen die Beschwerdeführerin gerichtet war. Darüber hinaus sah es die Datenschutzbehörde als erwiesen an, dass der Ordinationsgehilfe Einsicht in die Patientenakte der Beschwerdeführerin genommen hatte, da es sich bei der Information hinsichtlich des Arbeitgebers der Beschwerdeführerin um keine im Internet abrufbare Information handelte und auch die Datenschutzbehörde im Rahmen einer amtswegigen Recherche den Arbeitgeber der Beschwerdeführerin nicht eruieren konnte.

Der Beschwerde wurde daher stattgegeben und festgestellt, dass die Beschwerdeführerin in ihrem Recht auf Geheimhaltung verletzt wurde.

Der Bescheid ist nicht rechtskräftig.

DSB-D123.768/0004-DSB/2019, Abwägung zwischen dem Recht auf Geheimhaltung und dem Recht auf freie Meinungsäußerung

Im Bescheid vom 18. Dezember 2019, GZ: DSB-D123.768/0004-DSB/2019, hatte sich die Datenschutzbehörde mit einer Abwägung des Rechts auf Geheimhaltung gegen das Recht auf freie Meinungsäußerung auseinander zu setzen. Der Beschwerdeführer gehört einer politischen Partei an und ist Stadtrat einer österreichischen Gemeinde. Im November fand eine Besprechung der Gemeinde zum „Parkraumkonzept“ statt, zu welcher ein bestimmter Adressatenkreis, darunter auch der Beschwerdeführer, geladen war. An dieser Besprechung hat der Beschwerdeführer auf Grund einer falschen Einladungszustellung nicht teilgenommen.

Die Beschwerdegegnerin, eine andere politische Partei, hat daraufhin auf ihrer öffentlichen Facebook-Seite einen Eintrag gepostet, in welchem, durchaus überspitzt formuliert, Kritik an dem Nichterscheinen des Beschwerdeführers geübt wurde.

Die Datenschutzbehörde wies die Beschwerde ab. Zum einen wurde festgestellt, dass selbst bei einer weiten Auslegung des Begriffes „Journalismus“ verfahrensgegenständlich keine Verarbeitung zu journalistischen Zwecken erkannt werden kann. Da § 9 Abs. 1 DSG nicht zur Anwendung kommt, war eine Zuständigkeit der Datenschutzbehörde gegeben.

Weiters stellte die Datenschutzbehörde fest, dass mit dem Posting ein Beitrag zu einer Debatte von öffentlichem Interesse, nämlich, ob der Beschwerdeführer als Politiker und Person des öffentlichen Interesses seinen Aufgaben bzw. Anforderungen als Stadtrat gerecht wird, vorlag. Nach Rsp. des OGH sind Grenzen zulässiger Kritik in Bezug auf einen Politiker, der in seiner öffentlichen Funktion handelt, weiter auszulegen als in Bezug auf eine Privatperson. Jeder Politiker setzt sich selbst unvermeidlich und willentlich einer genauen Beurteilung seiner Worte und Taten nicht nur durch Journalisten und das breitere Publikum, sondern insbesondere auch durch den politischen Gegner aus.

Darüber hinaus war die verfahrensgegenständliche Verwendung der Daten des Beschwerdeführers deshalb nicht rechtswidrig, weil diese Form der politischen Arbeit Deckung in § 1 Abs. 2 PartG, und damit in einer Rechtsgrundlage iSd § 1 Abs. 2 DSG, findet.

DSB-D213.1042 (2020-0.0.203.677), Mandatsbescheid vom 30. März 2020 – Arzt veröffentlicht Patientendaten auf Facebook

Der Datenschutzbehörde wurde zur Kenntnis gebracht, dass ein Arzt auf seiner persönlichen Facebook-Seite sowie auf dem offiziellen Facebook-Auftritt der Ärztekammer personenbezogene Gesundheits- und Patientendaten in Form von ausgewählten Ausschnitten aus Patientenbriefen, Befunden oder sonstigen ärztlichen Aufzeichnungen/Protokollen „poste“, um öffentlich Kritik zu üben. Die Datenschutzbehörde leitete ein Verfahren nach den Art. 58, 57, 55 iVm Art. 1 DSGVO („amtswegiges Prüfverfahren“) ein.

Unterlassungsaufforderungen der Ärztekammer sowie ein Disziplinarverfahren hätten den Verantwortlichen bisher nicht davon abgehalten, Gesundheitsdaten seiner Patientinnen und Patienten weiterhin auf öffentlich zugänglichen Social-Media-Plattformen zu veröffentlichen.

Nach § 22 Abs. 4 DSG in Verbindung mit § 57 Abs. 1 AVG ist die Datenschutzbehörde berechtigt, ohne vorangegangenes Ermittlungsverfahren die Weiterführung einer Datenverarbeitung mit Mandatsbescheid zu untersagen, wenn durch eine Datenverarbeitung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen betroffener Personen (Ge-

fahr im Verzug) vorliegt. Dies war gegenständlich der Fall. Durch die Veröffentlichung von Patienten- und Gesundheitsdaten lag zweifelsohne ein schwerwiegender Eingriff in das Grundrecht auf Datenschutz der Betroffenen gemäß § 1 DSG vor. Eine diese Art der Veröffentlichung tragende Rechtsgrundlage war nicht ohne weiteres ersichtlich.

Mit Mandatsbescheid wurde dem Verantwortlichen daher die Offenlegung personenbezogener Gesundheits- und Patientendaten auf der persönlichen Facebook-Seite sowie auf dem offiziellen Facebook-Auftritt der Ärztekammer für Wien sowie sonstigen öffentlichen Facebook-Gruppen/Seiten und Social-Media-Plattformen mit sofortiger Wirkung untersagt.

DSB-D124.024/0008-DSB/2019, Speicherdauer von Stammdaten iSd § 97 TKG 2003 durch einen Mobilfunkanbieter

Im Bescheid vom 11.2.2020 hatte sich die Datenschutzbehörde mit der Frage zu beschäftigen, wie lange ein Mobilfunkanbieter nach Beendigung eines Vertrages Stammdaten aufbewahren darf. Bei Stammdaten handelt es sich um Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind (zB Name, Anschrift, Information über Art und Inhalt des Vertragsverhältnisses). Der Mobilfunkanbieter verweigerte zum Teil die beantragte Löschung und brachte vor, Stammdaten würden erst nach sieben Jahren ab Vertragsbeendigung gelöscht werden. Grundlage dafür seien die Bestimmungen § 132 BAO sowie § 212 UGB. Dazu führte die Datenschutzbehörde aus, dass § 97 Abs. 1 TKG 2003 eine strenge Zweckbindung für die Verarbeitung personenbezogener Daten normiert. Gemäß § 97 Abs. 2 TKG 2003 sind Stammdaten spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen. § 132 BAO und § 212 UGB normieren zwar eine Aufbewahrungspflicht von sieben Jahren und stellen daher auch grundsätzlich eine Rechtsgrundlage für die weitere Verarbeitung der Daten nach Vertragsbeendigung dar. Die siebenjährige Frist beginnt jedoch nicht ab Beendigung des Vertrages zu laufen, sondern gemäß ausdrücklichem Gesetzeswortlaut dieser Bestimmungen im Allgemeinen bereits ab Schluss des Geschäftsjahres, auf das sich die Unterlagen beziehen.

Der Bescheid ist rechtskräftig.

Ausgewählte Entscheidungen der Gerichte

BVwG-Erkenntnis vom 28.05.2020, W274 2230370-1/4E (Zeugen Jehovas)

Beschwerdegegenstand des Ausgangsverfahrens war eine behauptete Verletzung im Recht auf Auskunft aufgrund einer behaupteten mangelhaften Auskunft. Der Beschwerdeführer bestand auf der Übermittlung einer Kopie aller Dokumente betreffend sein Ausschlussverfahren aus der Religionsgemeinschaft der Zeugen Jehovas (Beschwerdegegner im Ausgangsverfahren), die sich in der sog. Verkündigerberichtskarte in einem verschlossenen Umschlag befinden würden. Die Datenschutzbehörde hat die Ausgangsbeschwerde abgewiesen, da sich im Zuge des Ermittlungsverfahrens ergeben hatte, dass die Zeugen Jehovas den Umschlag geöffnet und die enthaltenen personenbezogenen Daten (insb. die Ausschlussgründe) vollständig beauskunftet haben. Ein darüberhinausgehender Anspruch auf Erhalt exakter Kopien aller enthaltenen Dokumente wurde im Ausgangsverfahren verneint.

Das BVwG argumentierte anders: Bei dem Umschlag handle es sich um einen Papierakt, weshalb die Anwendbarkeit der DSGVO ausgeschlossen wäre. Papierakten seien keine Dateisysteme. Überdies sei das Auskunftsrecht nach der Rsp des EuGH nicht geeignet, sich Zugang zu Verwaltungsdokumenten zu sichern. Die internen Unterlagen aus einem Ausschlussverfahren nach den internen Satzungen der Zeugen Jehovas seien Verwaltungsdokumenten gleichzuhalten. Auf den Umfang der Datenkopie nach Art. 15 Abs. 3 DSGVO sei mangels genereller Anwendbarkeit der DSGVO nicht einzugehen.

BVwG-Erkenntnis vom 29.04.2020, GZ W274 2228071-1/6E

Mit diesem Erkenntnis bestätigte das BVwG, dass die DSB die Behandlung einer Beschwerde wegen „Exzessivität“ zurecht abgelehnt hatte.

Die DSB ist zwar verpflichtet, sich mit Beschwerden gemäß Art. 57 Abs. 1 lit. f DSGVO zu befassen, kann die Behandlung einer Beschwerde aber ablehnen, wenn die Beschwerdeerhebung offenkundig unbegründet oder – insbesondere im Fall von häufiger Wiederholung – exzessiv erfolgt (Art. 57 Abs. 4 DSGVO). Ablehnung bedeutet diesfalls, dass die DSB keine inhaltliche Beurteilung der Beschwerde vornimmt, sondern die Behandlung vor einer solchen Prüfung ablehnt.

Im vorliegenden Fall brachte der Beschwerdeführer seit Juni 2018 mehr als 90 Beschwerden ein, die sich im Kern um dieselbe Sache drehten, nämlich darum, dass der Beschwerdeführer verschiedenen Verantwortlichen (in Österreich und einem anderen Staat der

EU) vorwarf, seine Daten und die Daten seines Kindes unrichtig bzw. unrechtmäßig zu verarbeiten.

Das BVwG bestätigte im genannten Erkenntnis, dass die Ablehnung wegen exzessiver Verfahrensführung zurecht erfolgte und hielt begründend fest:

„Der BF zeigt in seiner Beschwerde an das BVwG nicht auf, dass der der Datenschutzbeschwerde zugrundeliegende Sachverhalt […] so individuell wäre, dass trotz der hohen Anzahl von Beschwerden generell als auch den mehreren Beschwerden gegen Beschwerdegegner im Zusammenhang mit [Einrichtung] eine Behandlung der Beschwerde berechtigt wäre."

Gesetzesbegutachtung – Stellungnahmen

Die DSB hat zu folgenden Gesetzesvorhaben eine Stellungnahme abgegeben:

- Bundesgesetz, mit dem das Gesundheitstelematikgesetz 2012 und das Bundesgesetz BGBl. I Nr. 37/2018 geändert werden
- Bundesgesetz, mit dem das Hochschul-Qualitätssicherungsgesetz geändert wird, ein Bundesgesetz über Privathochschulen erlassen wird und das Fachhochschul-Studiengesetz sowie das Hochschulgesetz 2005 geändert werden
- Vorarlberger Gesetz über Sozialleistungen für hilfsbedürftige Personen - Sammelgesetz
- Änderung des PStSG und Erlassung der Vertrauenswürdigkeitsprüfungs-Verordnung (BMVIT) 2019
- Entwurf eines Bundesgesetzes, mit dem ein Investitionskontrollgesetz erlassen und das Außenwirtschaftsgesetz 2011 geändert wird
- Bundesgesetz, mit dem ein neues Tierärztegesetz erlassen und das Tierärztekammergesetz geändert wird

Weblink:

- Parlament aktiv: alle Stellungnahmen

News

Folgende neue Mitarbeiterinnen und Mitarbeiter nahmen ihre Tätigkeit in der DSB auf:

Frau **Mag. Stephanie Mezler-Andelberg** studierte Rechtswissenschaften an der Karl-Franzens-Universität Graz und unterstützt das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Herr **Mag. Quentin Soyer** war nach dem Studium in Wien und Maastricht (NL) sowie diversen Praktika zuletzt als Wissenschaftlicher Mitarbeiter am Verwaltungsgerichtshof tätig und absolvierte dort auch seine Grundausbildung. Nun unterstützt er das Team der Juristinnen und Juristen in den Bereichen nationales und internationales Verfahren.

Impressum:
Medieninhaber, Herausgeber und Redaktion: Österreichische Datenschutzbehörde (DSB), Barichgasse 40-42, 1030 Wien, E-Mail: dsb@dsb.gv.at, Web: http://www.dsb.gv.at

Offenlegung gemäß § 25 Mediengesetz:
Der Newsletter der DSB ist ein wiederkehrendes elektronisches Medium (§ 1 Abs. 1 Z 5a lit. c MedienG); die gesetzlich gebotenen Angaben sind über folgenden Link abrufbar: http://www.dsb.gv.at/impressum.