Landesbeauftragte veröffentlicht Tätigkeitsbericht Datenschutz 2021

Dienstag, 10 Mai 2022

https://www.datenschutz.de/landesbeauftragte-veroeffentlicht-taetigkeitsbericht-datenschutz-2021/

Presseinformation der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht vom 09.05.2022

Heute überreicht die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Dagmar Hartge, der Präsidentin des Landtages Brandenburg, Prof. Dr. Ulrike Liedtke, ihren Tätigkeitsbericht zum Datenschutz für das Jahr 2021.

Der bereits in den Vorjahren spürbare Aufwind für die Digitalisierung in Verwaltung und Wirtschaft hat im Berichtszeitraum nicht an Dynamik eingebüßt. Dies zeigte sich auch an den Schwerpunkten unserer Tätigkeit, die auf dem Gebiet des technisch-organisatorischen Datenschutzes lagen.

Das Onlinezugangsgesetz schreibt Bund und Ländern vor, Verwaltungsleistungen bereits bis Ende 2022 in digitaler Form über Verwaltungsportale anzubieten. Die Umsetzung wirft jedoch immer neue Probleme auf; der bundesweite Abstimmungsbedarf ist sehr hoch. An einer im Auftrag der Datenschutzkonferenz eingerichteten Arbeitsgruppe wirkten die Datenschutzaufsichtsbehörden mehrerer Bundesländer unter unserer Leitung mit. Die Arbeitsgruppe befasste sich insbesondere mit der Frage, wie Verwaltungsleistungen datenschutzkonform realisiert werden können. Ihre Ergebnisse fasste sie in einem Sachstandsbericht zusammen, der dem Bundesministerium des Innern und für Heimat übergeben wurde. Der Bericht bildet die Basis für weitere Gespräche sowie Abstimmungen mit dem Ministerium und gegebenenfalls für eine Gesetzesanpassung (A I 1.1, Seite 15).

Ein Digitalisierungsvorhaben des Onlinezugangsgesetzes, mit dem wir uns detailliert befasst haben und das federführend durch das Ministerium des Innern und für Kommunales koordiniert wird, war das Projekt „Aufenthaltstitel für Erwerbstätigkeit“. Im Mittelpunkt steht dabei die Ausstellung von Aufenthaltstiteln, Aufenthaltskarten und aufenthaltsrelevanten Bescheinigungen sowie von Daueraufenthaltsbescheinigungen. Bereits im Rahmen der Pilotierung hat uns das Ministerium in die Erarbeitung der umfangreichen Projektdokumentation eingebunden. Wir wirkten unter anderem an der Erstellung des Rahmenkonzepts, des Datenschutzkonzepts und der IT-Sicherheitsbetrachtung mit. Für die Verfahren bleiben die kommunalen Ausländerbehörden datenschutzrechtlich verantwortlich (A I 1.2, Seite 18). Dagmar Hartge:

Die Digitalisierung von Verwaltungsdienstleistungen verspricht Bürgerinnen und Bürgern einen großen Nutzen. Andererseits stehen die Behörden vor der Herausforderung, die notwendigen Prozesse so zu konzipieren, dass personenbezogene Daten genauso sicher verarbeitet werden wie im Rahmen klassischer Verwaltungsverfahren. Meine Mitarbeiterinnen und Mitarbeiter werden die Umsetzung des Onlinezugangsgesetzes auch künftig soweit beratend begleiten, wie die personellen Kapazitäten unserer Behörde dies erlauben.

Auch im zweiten Jahr der Pandemie standen Datenschutzthemen vielfach im Fokus der Diskussionen um technische Lösungen zur Eindämmung des Corona-Virus. Die Hauptlast trugen weiterhin die kommunalen Gesundheitsämter. Sie sollten z. B. Kontakte nachverfolgen und die Isolation Infizierter bzw. die Quarantäne von Kontaktpersonen verfügen. Als Hilfsmittel standen ihnen unter anderem die Softwaresysteme SORMAS und Luca zur Verfügung. Leider mussten wir feststellen, dass beide dem Datenschutz nicht ausreichend Rechnung trugen:

SORMAS, eine speziell an COVID-19 angepasste Software für das Management und die Analyse von Infektionsausbrüchen, sollte die Kontaktnachverfolgung vereinheitlichen und die Gesundheitsämter unterstützen. Das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz hatte ihren Einsatz in allen brandenburgischen Gesundheitsämtern angewiesen. Das Programm wies jedoch datenschutzrechtliche Mängel auf, insbesondere war die Dokumentation der Datenverarbeitung unzureichend. Eine solche dient nicht etwa nur einer formalen Vollständigkeit, sondern stellt einen zentralen Baustein dar, der unter anderem die für einen datenschutzgerechten Betrieb umzusetzenden Maßnahmen beschreibt. Für SORMAS bestanden Unklarheiten über die Datenflüsse, über das Berechtigungskonzept, über Verschlüsselungen, über das Löschkonzept und andere wesentliche Komponenten.

Vor dem Hintergrund der hohen Belastung der Gesundheitsämter in der Pandemie verzichteten wir darauf, diese mit aufsichtsrechtlichen Verfahren noch weiter zu belasten und strebten stattdessen an, zentral Verbesserungen für alle teilnehmenden Behörden zu erreichen. Die unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern wirkten zunächst mit konkreten Empfehlungen zur Behebung der Mängel gegenüber den Projektverantwortlichen auf Verbesserungen hin. Dies führte nicht zum Erfolg. In einer zweiten Phase fanden monatliche Beratungen von Vertretern einiger Datenschutzaufsichtsbehörden (zu denen auch wir gehörten) sowie den Projektverantwortlichen auf Bundesebene statt. Immer mehr Unzulänglichkeiten traten zutage: selbstgesetzte Fristen zur Behebung von Mängeln verstrichen, die Verarbeitungszwecke von SORMAS wurden erweitert, manche Datenverarbeitungen waren nicht von Rechtsgrundlagen gedeckt und die Software sollte auf einmal auch zur langfristigen Aufbewahrung personenbezogener Daten dienen. Die Projektverantwortlichen sagten zwar zu, die Kritikpunkte zu berücksichtigen, zumeist blieb es aber dabei. Als Konsequenz aus dem unzureichenden Projektfortschritt haben wir unsere Mitarbeit in der Arbeitsgruppe eingestellt. Im Ergebnis ist für uns nicht nachvollziehbar, dass die Gesundheitsämter zum Einsatz von SORMAS als einem nicht vollständig datenschutzkonformen Produkt gedrängt wurden (A I 2, Seite 22).

Ähnlich frustrierend war aus Sicht des Datenschutzes die Auseinandersetzung mit dem Einsatz des Luca-Systems. Auch hier strebten wir an, die in der Pandemie ohnehin stark beanspruchten Gesundheitsämter möglichst wenig zusätzlich zu belasten. Daher wollten wir mit dem Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz sowie ausgewählten Gesundheitsämtern einheitliche Vorgaben für die Nutzung der Daten aus dem Luca-System absprechen. Wir wiesen das Gesundheitsministerium frühzeitig auf unsere grundsätzlichen Bedenken hin. Neben nachgewiesenen Sicherheitslücken gehörten dazu auch unsere Zweifel an der grundsätzlichen Eignung des Luca-Systems für die Zwecke der Kontaktnachverfolgung. Das Gesundheitsministerium hielt trotzdem an seiner Entscheidung zur Nutzung des Luca-Systems fest und passte die Eindämmungsverordnung des Landes entsprechend an. Die von uns alternativ empfohlene Nutzung der datensparsamen Corona-Warn-App war damit nicht möglich.

Lange Zeit war gar nicht bekannt, wie das Luca-System durch die Gesundheitsämter tatsächlich genutzt

wurde. Wir initiierten deshalb eine entsprechende Umfrage. Das Ministerium baten wir um die Versendung von Fragebögen und die statistische Auswertung der Antworten. Im Ergebnis teilte nur ein einziges Gesundheitsamt mit, Kontaktdaten aus dem Luca-System zur Kontaktnachverfolgung eingesetzt zu haben. Unsere Auffassung, dass dem Vorhaben die Geeignetheit zur Pandemiebekämpfung fehlte, bestätigte sich dadurch. Die Ergebnisse der Umfrage zeigten zudem, dass die Mehrheit der Gesundheitsämter keine hinreichenden Vorkehrungen getroffen hatte, um Kontaktdaten mit Hilfe des Luca-Systems datenschutzkonform zu verarbeiten. Erst im laufenden Jahr hat sich die Landesregierung entschieden, das Luca-System nicht weiter zu nutzen (A I 3, Seite 29). Dagmar Hartge:

Bei allem Verständnis für die Absicht der Landesregierung, die bedrohliche Corona-Pandemie so schnell wie möglich einzudämmen: Mit SORMAS und Luca standen dafür keine aus Datenschutzsicht geeigneten Mittel zur Verfügung. Wer sich mit der Luca-App in einem Restaurant eingecheckt hat, durfte erwarten, im Falle einer Infektion eines anderen Gastes benachrichtigt zu werden. Genau das geschah faktisch aber nicht. Die Speicherung der Daten war somit völlig zwecklos. Dies hätten die Verantwortlichen viel früher erkennen und die Reißleine ziehen müssen.

Unsere Behörde beteiligte sich im vergangenen Jahr an einer länderübergreifend koordinierten Prüfung von Webseiten verschiedener Medienunternehmen. Dabei ging es um das Werbe-Tracking – eine Datenverarbeitung, die zunehmend Gegenstand von Beschwerden ist. Wer ein Internetangebot besucht, bekommt in der Regel nicht mit, dass eine Vielzahl personenbezogener Informationen an Hunderte von Unternehmen übermittelt und dort ausgewertet wird. Für eine solche Datenverarbeitung bedarf es einer Einwilligung der Nutzerin oder des Nutzers. Zu diesem Zweck werden Cookie-Banner verwendet, die häufig eine Einwilligung mit einem Klick, eine Ablehnung aber unter wesentlich höherem Aufwand anbieten. Datenschutzrechtlich wirksam ist eine Einwilligung aber nur, wenn die Auswahl in gleichrangiger Weise angeboten wird. Mängel bestehen häufig auch bei der Information über die Weiterverarbeitung der zu Werbezwecken übermittelten Daten.

Mithilfe eines Fragebogens haben die an der Prüfung beteiligten Datenschutzaufsichtsbehörden unter anderem die eingesetzten Tracking-Methoden erfragt. Das in unserem Zuständigkeitsbereich geprüfte Verlagshaus übermittelte beispielsweise die nutzerspezifischen Daten an bis zu 150 eingebundene Partnerunternehmen, informierte aber nur pauschal über den Einsatz von Cookies. Zwar nahm das Unternehmen anschließend Verbesserungen vor, erfüllte das Erfordernis des Angebots einer gleichwertigen Ablehnungsoption jedoch nicht. Schließlich entschied es sich für ein Modell, das die Wahl eröffnet, in das Tracking zu Werbezwecken einzuwilligen oder ein kostenpflichtiges Abonnement abzuschließen und im Gegenzug von dem Werbe-Tracking verschont zu bleiben. Dieses immer häufiger verwendete Modell wird zurzeit noch von den Datenschutzaufsichtsbehörden rechtlich geprüft (A I 4, Seite 36).

Kurz nach Bekanntwerden einer Sicherheitslücke in der Software Microsoft Exchange Server waren allein in Deutschland bereits zehntausende Unternehmen und zum Teil auch öffentliche Stellen betroffen. Über mehrere Wochen hinweg erhielten wir zahlreiche Meldungen von Datenschutzverletzungen. Viele Verantwortliche reagierten angemessen, professionell und zügig. In fünf Fällen geschah dies jedoch nicht, sodass wir dort Prüfungen vornahmen. Drei dieser Verantwortlichen haben den Sachverhalt im Berichtszeitraum nicht ausreichend aufgeklärt bzw. nicht auf unsere Nachfragen reagiert. Wir werden hierzu die nächsten Schritte prüfen und ggf. Sanktionsmaßnahmen einleiten. Der Vorfall zeigt, wie wichtig es ist, die aktuelle Bedrohungslage in der Informationstechnik stets zu beobachten und

unverzüglich geeignete Gegenmaßnahmen zu ergreifen (A IV 1, Seite 80).

Credential Stuffing ist eine Form von Angriffen, die auf gestohlenen Nutzerdaten aufbaut. Hier probieren Kriminelle durch automatisierte Massenabfragen aus, ob erbeutete Zugangsdaten wie E-Mail-Adresse und Passwort auch auf anderen Internetplattformen eine Anmeldung ermöglichen. Im Berichtszeitraum meldete uns eine Unternehmensgruppe eine entsprechende Datenschutzverletzung, von der über 250.000 Nutzerkonten betroffen waren. Der Verantwortliche informierte die Betroffenen, setzte deren Passwörter zurück und forderte sie auf, neue Passwörter zu vergeben. (A IV 4, Seite 88). Dagmar Hartge:

Unternehmen müssen Warnsysteme betreiben, durch die digitale Angriffe entdeckt werden können. Gleichzeitig sind aber auch ihre Kundinnen und Kunden gefragt. Mit relativ einfachen Mitteln können sie selbst dazu beitragen, dass Angriffe ins Leere laufen. Sie sollten beispielsweise bei jedem Internetdienst ein anderes, möglichst sicheres Passwort und, falls dies angeboten wird, eine Zwei-Faktor-Authentisierung verwenden. Ein Verzicht darauf ist vielleicht bequemer, sicherer jedoch garantiert nicht.

Ausführlich beschäftigte uns eine Beschwerde über die Nutzung des Nachrichtendienstes WhatsApp in einer Pflegeeinrichtung für die Organisation der Arbeit sowie für die Kommunikation mit Bewohnerinnen und Bewohnern und deren Angehörigen. Ausgetauscht wurden dabei neben innerbetrieblichen Daten Informationen zum Leben in der Einrichtung sowie Gruppenbilder der Pflegebedürftigen. Wie selbstverständlich nutzten die Beschäftigten ihre privaten Mobiltelefone. Auf unser Tätigwerden hin wechselte die Pflegeeinrichtung den Kurznachrichtendienst, konnte uns aber nicht zweifelsfrei darlegen, welche konkreten Vorkehrungen zur Sicherung des Datenschutzes tatsächlich umgesetzt wurden. Im Ergebnis haben wir eine Reihe von Maßnahmen empfohlen, darunter den Verzicht auf Angebote aus Drittstaaten zugunsten einer Lösung im Rahmen der eigenen IT-Infrastruktur oder bei einem Webhoster in Europa, die Verwendung von Pseudonymen zur Benennung der Beschäftigten und der Pflegebedürftigen sowie das Verbot der Verwendung privater Mobiltelefone der Beschäftigten (A IV 2, Seite 82).

Das Ministerium des Innern und für Kommunales bat uns um Auskunft, inwieweit eine Recherche durch die Ausländerbehörden in sozialen Netzwerken, insbesondere auf Facebook, zur Identitätsfeststellung, zulässig ist. Wir bezweifelten die Rechtmäßigkeit aus verschiedenen Gründen und legten unsere Position ausführlich dar. Unter anderem ist eine Überprüfung der Authentizität und des Wahrheitsgehalts von Angaben in sozialen Netzwerken grundsätzlich nicht möglich und es können Daten unbeteiligter Personen bei der Recherche erfasst werden. Außerdem steht der Nutzung von Plattformen mit Sitz in den Vereinigten Staaten von Amerika der Umstand entgegen, dass hier ein angemessener Schutz der personenbezogenen Daten nur durch zusätzliche Maßnahmen gewährleistet werden kann (A V 6, Seite 120).

Erneut erhielten wir viele Meldungen von Datenschutzverletzungen, bei denen die Daten von Kindern betroffen waren – häufig durch Einbrüche und Diebstähle in Kindertagesstätten. In den meisten Fällen wurden elektronische Geräte gestohlen, wie zum Beispiel Kameras oder Laptops. Zwecks Aufklärung der Ursachen für diese Vorfälle starteten wir eine Befragung. Zu unserem Erstaunen geschahen die Diebstähle sowohl während als auch außerhalb der Öffnungszeiten der Einrichtungen. Wir empfehlen daher, die Geräte nicht nur nach Dienstschluss, sondern direkt nach Gebrauch zu verschließen. Zudem sollten Kameraaufnahmen nur möglichst kurz auf den Geräten vorgehalten und anschließend in ein geschütztes Speichersystem übertragen werden. Um die teils sensitiven Daten der Kinder zu schützen, ist

es unabdingbar, möglichst verschlüsselte Datenträger einzusetzen. Den Datenschutzbeauftragten der Kindertagesstätten bzw. ihrer Träger haben wir empfohlen, die Beschäftigten intensiv für diese Belange zu sensibilisieren (A II 3, Seite 68).

Aber auch andere Verantwortliche erstatteten Meldungen von Datenschutzverletzungen (A VI 4, Seite 135). Dagmar Hartge:

Der erneute Anstieg der obligatorischen Meldungen von Datenschutzverletzungen – der sogenannten Datenpannen – bereitet mir große Sorgen. Häufig liegen solchen Meldungen die Ausnutzung von bekannten Sicherheitslücken und gezielte Hackerangriffe zu Grunde. Hieran wird deutlich, dass Verantwortliche dem Einsatz und der Aktualisierung der technischen und organisatorischen Datenschutzmaßnahmen verstärkt Aufmerksamkeit widmen müssen. Die IT-Sicherheit ist als Grundlage für einen effektiven Datenschutz unabdingbar. In zunehmendem Maße gilt das nicht nur für große Konzerne, sondern auch für kleine und mittlere Unternehmen.

Vor dem Hintergrund verschiedener Anfragen, die einen erheblichen Beratungsbedarf der zuständigen Behörden erkennen ließen, haben wir die Einhaltung der datenschutzrechtlichen Vorgaben bei der Aufgabenwahrnehmung nach dem Asylbewerberleistungsgesetz durch die Sozialbehörden von drei Landkreisen überprüft und Mängel festgestellt. Die Leistungsakten enthielten unter anderem Rezepte, Überweisungsträger und auch Diagnosen, denen ein detailliertes Bild des gesundheitlichen Zustands der betroffenen Personen zu entnehmen war. Auch befanden sich darin personenbezogene Daten Unbeteiligter, die Rückschlüsse auf deren gesundheitlichen Zustand ermöglichten. Schutzmaßnahmen, die der hohen Sensitivität dieser Gesundheitsdaten angemessenen gewesen wären, fehlten. Die Daten waren zur Leistungsgewährung nicht notwendig. Wir haben die Verletzung der datenschutzrechtlichen Vorgaben moniert und die Sozialbehörden zu Korrekturen aufgefordert (A III 4, Seite 70).

Im Berichtszeitraum beschwerte sich ein Mitglied eines Garagenvereins darüber, dass der Vorstand seine vertrauliche Korrespondenz in Schaukästen auf dem Vereinsgelände veröffentlicht hatte. Alle anderen Mitglieder sowie Gäste des Vereins konnten so Einzelheiten des Schriftwechsels zur Kenntnis nehmen. Das war weder erforderlich noch rechtmäßig. Wir haben gegen den Verein deshalb eine Verwarnung ausgesprochen (A II 3, Seite 50).

Bizarr mutet der Fall eines Aktenverlustes an: Ein Mitarbeiter einer Körperschaft des öffentlichen Rechts ließ eine Akte mit personen- und unternehmensbezogenen Daten, die eigentlich besonders sorgfältig zu verwahren gewesen wäre, auf dem Autodach liegen und fuhr los. Das Fahrzeug und die Aktenmappe nahmen dann unterschiedliche Wege; die Dokumente waren später nicht mehr auffindbar. Der Verantwortliche meldete uns diese Datenschutzverletzung und sensibilisierte die gesamte Belegschaft für einen sorgsameren Umgang mit solchen sensitiven Daten (A IV 7, Seite 95).

Die Landesbeauftragte setzte ihre Begleitung des Pilotprojekts zum Einsatz von Bodycams bei der Polizei Brandenburg fort. Den Schwerpunkt legten wir dabei auf die technischen und organisatorischen Maßnahmen, die ergriffen werden müssen, um einen sicheren und datenschutzgerechten Betrieb der Körperkameras zu gewährleisten. Die Polizei legte uns schließlich eine stimmige Risikoanalyse vor. Natürlich müssen die daraus folgenden Maßnahmen zur Gewährleistung des Datenschutzes auch umgesetzt werden. Großen Wert legten wir in unserer Beratung auf solche Maßnahmen, die verhindern, dass die Hersteller dieser Kameras unberechtigten Zugriff auf die von der Kamera erfassten Daten

erhalten (B 3.1, Seite 152).

Bei einem großen Informationsverbund wie dem der Polizei Brandenburg bedarf es eines verfahrensunabhängigen Rahmenkonzepts für die IT-Sicherheit. Es dient als Basis für darauf aufbauende Teil-Sicherheitskonzepte für die einzelnen automatisierten Verfahren. Die Entwicklung eines solchen Rahmensicherheitskonzeptes wies über Jahre hinweg erhebliche Defizite auf. Inzwischen haben sich erfreulicherweise sowohl die Realisierungsplanung als auch der Umsetzungsstand insbesondere der als hoch-prioritär erkannten technischen und organisatorischen Maßnahmen deutlich verbessert. Die Landesbeauftragte wird die Arbeit der Polizei an dem Rahmensicherheitskonzept weiterhin konstruktiv und kritisch begleiten (B 3.2, Seite 154). Dagmar Hartge:

Immer wieder habe ich das Fehlen eines IT-Rahmensicherheitskonzepts der Polizei Brandenburg bemängelt. Dass es endlich vorliegt und wir jetzt nur noch über Details diskutieren, ist ein großer Fortschritt. Auch bei der Vorbereitung des Einsatzes von Bodycams hat die Polizei mich rechtzeitig und umfassend beteiligt. Datenschutzkonforme Lösungen sind gerade da besonders wichtig, wo der Staat tief in die Grundrechte der Bürgerinnen und Bürger eingreift.

Feststellen müssen wir aber auch, dass die Zahl der bußgeldrelevanten Vorgänge im Zusammenhang mit unbefugten Datenverarbeitungen von Polizeibediensteten des Landes Brandenburg im Vergleich zum Vorjahr erneut gestiegen ist. Insgesamt betreffen ca. 26 % unserer Bußgeldverfahren derartige Verarbeitungen (A II 4.4, Seite 56).

Die Bußgeldstelle der Landesbeauftragten verfolgte datenschutzrechtliche Ordnungswidrigkeiten aber auch in anderen Fällen. In 23 Fällen verhängte sie wegen der festgestellten datenschutzrechtlichen Verstöße ein Bußgeld. Die Gesamtsumme der festgesetzten Bußgelder betrug 13.430 Euro (A VI 5.2, Seite 137).

Beispielsweise veröffentlichte ein Gartenbauunternehmen die Videoaufnahme von Probearbeiten eines Beschwerdeführers. Zu Werbezwecken publizierte es die Aufnahmen sowohl im sozialen Netzwerk Facebook als auch auf der Online-Plattform YouTube und der Webseite des Unternehmens. Die vorsätzliche Veröffentlichung des Videos sowie die unterlassene Löschung haben wir mit einem Bußgeld geahndet (A II 4.2, Seite 53).

Eine ehemalige Mitarbeiterin eines Unternehmens hatte sich – als sie noch dort angestellt war – von ihrem dienstlichen Rechner eine Tabelle mit den Daten anderer Beschäftigter an ihre private E-Mail-Adresse zugesandt. Die Tabelle umfasste neben den vollständigen Namen u. a. auch einen Überblick über Urlaubstage, Krankentage, Lohndaten, geleistete Überstunden und Sozialversicherungsbeiträge. Zur Erfüllung ihrer betrieblichen Aufgaben war dies nicht erforderlich und damit rechtswidrig. Diesen Verstoß ahndeten wir ebenfalls mit einer Geldbuße (A II 4.5, Seite 58). Genauso erging es einem Angestellten, der Bewerbungsunterlagen, die bei seinem Arbeitgeber eingegangen waren, an seine private E-Mail-Adresse weiterleitete. Er wollte sich damit für die visuelle Gestaltung eigener Bewerbungen inspirieren lassen (A II 4.6, Seite 58).

Ihre neue Praxisanschrift teilte eine Ärztin für Kinder- und Jugendlichenpsychotherapie einer großen WhatsApp-Gruppe mit. Dieser gehörten Eltern, Therapeutinnen und Therapeuten, Sozialpädagoginnen und Sozialpädagogen sowie Lehrkräfte an. Ihnen wurden so die Telefonnummern der anderen Mitglieder

offenbart. Wer diese Nummern als eigene Kontakte führte, konnte Rückschlüsse darauf ziehen, dass sich Kinder aus ihnen bekannten Familien bei der Ärztin in Behandlung befinden oder befunden hatten. Gegen die Ärztin haben wir ein Bußgeld verhängt (A II 4.7, Seite 60).

Verantwortlich: Sven Müller, Tel. 033203 356-0
Kleinmachnow, 9. Mai 2022
