Die Landesbeauftragte für den Datenschutz Niedersachsen

28. Tätigkeitsbericht 2022

Niedersachsen

28. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für das Jahr 2022

Herausgeber: Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich: Barbara Thiel

Layout: Thomas Kupas | design@in-fluenz.de
Lavesstraße 20/21, 30159 Hannover

Illustrationen: Seiten 9, 90, 120: LfD Niedersachsen
alle anderen: Adobe Stock

Druck: Druckerei Albert Funke GmbH
Sorststraße 6, 30165 Hannover

Inhaltsverzeichnis

A. Vorwort

Das Jahr 2022 war in vielerlei Hinsicht ein spannendes und ereignisreiches Jahr für den Datenschutz und damit auch für meine Behörde. Seit Einführung der DS-GVO sind Austausch und Zusammenarbeit der nationalen und europäischen Aufsichtsbehörden zu einem kritischen Erfolgsfaktor für Vollzug, aber auch für Öffentlichkeitsarbeit und Akzeptanz beim Datenschutz insgesamt geworden. Auf europäischer Ebene wurden wesentliche Fortschritte erzielt und die Wirkweise des Kohärenzmechanismus am Beispiel der Bußgelder gegen drei Social Media Dienste des Meta Konzerns sehr deutlich demonstriert. Diese Fälle wurden im europäischen Datenschutzausschuss behandelt und damit die Entscheidung über die Sanktionen und deren Höhe nicht allein der irischen Aufsichtsbehörde überlassen. So kam es zu drei Geldbußen in jeweils dreistelliger Millionenhöhe, was im Lichte der schwerwiegenden und langandauernden Datenschutzverstöße des Meta-Konzerns ein überfälliges und durchaus richtungsweisendes Ergebnis darstellt.

Auf nationaler Ebene habe ich mich im Laufe meiner Amtszeit stets für die konsequente Weiterentwicklung der Datenschutzkonferenz (DSK) ausgesprochen und daran mitgewirkt. So wurden in diesem Jahr wichtige Weichen gestellt, um die koordinierende und steuernde Wirkung der DSK im föderalen Kontext zu stärken und deren Außenwirkung zu verbessern. Die Geschäftsordnung wurde novelliert, um insbesondere die Beschlussfähigkeit des Gremiums zu stärken. Weiterhin wurden ein Präsidiumsmodell eingeführt, wichtige Impulse in Richtung des Gesetzgebers zur Institutionalisierung der DSK gesetzt und die Aufgaben und Zuständigkeiten einer in Zukunft erforderlichen DSK Geschäftsstelle vereinbart.

In Niedersachsen stand im Jahre 2022 die Landtagswahl im Mittelpunkt des Interesses. Der Koalitionsvertrag von SPD und Bündnis 90/Die Grünen weist eine große Vielfalt an Vorhaben rund um die Digitalisierung auf. Ich empfehle, hier frühzeitig auch auf die Expertise meiner Behörde zurückzugreifen. Momentan ist dies gerade bei Digitalisierungsprojekten leider noch viel zu selten der Fall. Die Erfahrungen in der Vergangenheit haben aber gezeigt, dass Projekte immer dann gut und störungsfrei funktionieren, wenn der Datenschutz von Anfang an einbezogen wird. Naturgemäß nimmt das Thema Digitale Bildung an Schulen und Hochschulen einen breiten Raum ein. Die Aussagen dazu im Koalitionsvertrag begrüße ich. Es bleibt zu hoffen, dass es nunmehr gelingen wird, eine nach wie vor ausstehende Gesamtstrategie zu entwickeln, die angefangen vom Kultusminis-

Barbara Thiel

terium bis zu den Schulen den Verantwortlichen beim Einsatz digitaler Lösungen Hilfestellung und Rechtssicherheit beim Datenschutz bietet.

Die begrenzten Möglichkeiten zur Durchführung von anlasslosen Prüfungen machen mir nach wie vor große Sorgen. Die Kapazität für diese wichtigen „Standortbestimmungen" können aufgrund meiner begrenzten Ressourcen nur durch Verschlankung und Arbeitsverdichtung an anderen Stellen gewonnen werden. An welcher Ecke man auch zieht – das Tischtuch ist immer zu klein! Ich freue mich deshalb, dass wir trotz dieser Umstände mit unseren Prüfungen wie etwa in Schulen, Krankenhäusern und Justizvollzuganstalten, sowie den Prüfungen zu Tracking auf Webseiten und zum Datentransfer in unsichere Drittstaaten in der Lage waren, wichtige und aktuelle datenschutzrechtliche Problembereiche aufzudecken.

Schließlich wurden im Berichtszeitraum einige Bußgelder rechtskräftig, die von ihrer Höhe her tatsächlich geeignet sind, das Bewusstsein für die Folgen von Rechtsverstößen im Datenschutzbereich zu schärfen. Ein Datenschutzverstoß ist eben kein Kavaliersdelikt, sondern greift unmittelbar in die Grundrechte und Freiheiten der jeweils Betroffenen ein. Neben Beratung und Prävention wird daher meine Behörde auch in Zukunft mit Nachdruck Verstöße sanktionieren, um dem Datenschutz so umfassend Geltung zu verschaffen.

B. Management Summary

Das Wichtigste in Kürze

Europäischer Datenschutz

Die Harmonisierung des Datenschutzrechts und dessen einheitlicher Vollzug sind wesentliche Ziele der Datenschutz-Grundverordnung (DS-GVO). Neben zwei wichtigen Leitlinien – die eine zum Recht auf Auskunft und eine weitere zur Berechnung von Geldbußen – hat der Europäische Datenschutzausschuss (EDSA) auch im Vollzug wichtige Entscheidungen getroffen. Auch in den drei Streitbeilegungsverfahren gem. Art. 65 Abs.1 lit. a DS-GVO in Sachen Facebook, Instagram und WhatsApp war meine Behörde an den Verhandlungen zur Ausarbeitung der Entscheidungen des EDSA beteiligt.

In diesen Streitbeilegungsverfahren hat sich der EDSA mit der Frage auseinandergesetzt, ob der US-amerikanische Konzern Meta personenbezogene Daten für verhaltensbezogene Werbung verwenden und sich hierfür auf die Rechtsgrundlage der Vertragserfüllung (Art. 6 Abs. 1 lit. b DS-GVO) stützen darf. Die zuständige irische Datenschutzaufsichtsbehörde (Data Protection Commission, DPC) hatte diese Praxis des Meta Konzerns zunächst als rechtmäßig angesehen. Unter Beteiligung der weiteren europäischen Länder gelangte der EDSA dagegen zu dem Ergebnis, dass sich Meta nicht auf Einwilligungen gestützt und auch keine andere Rechtsgrundlage dargelegt hat. Zugleich hat er die DPC angewiesen, auf die so festgestellten, massiven Verstöße von Meta angemessen zu reagieren. Dies zeigt aus meiner Sicht einmal mehr, dass der europäische Kohärenzmechanismus ein funktionstüchtiges Instrument darstellt, um auch großen multinationalen Konzernen bei Verstößen gegen die DS-GVO wirksam begegnen zu können.

Internationaler Datenverkehr

Meine anlasslose Kontrolle zur Umsetzung der Anforderungen des Schrems II-Urteils habe ich im Jahr 2022 fortgesetzt. Erfreulicherweise konnte ich mich bislang bei meinen Überprüfungen davon überzeugen, dass sich die eingesetzten Internet-Server innerhalb des Europäischen Wirtschaftraums befinden. Probleme finden sich allerdings oft im Bereich der Wartungs- oder Supportdienstleistungen sowie der Einbindung von Drittdiensten. Ich habe je nach Ausgestaltung der Fernwartung im konkreten Einzelfall Warnungen ausgesprochen oder Hinweise erteilt.

Seit dem Frühjahr 2022 richtete sich der Blick von Wirtschaft, Verwaltung und Fachöffentlichkeit auf die Zukunft des transatlantischen Datenschutzes, nachdem von der Kommission der Europäischen Union der Entwurf für einen Angemessenheitsbeschluss für die USA vorgelegt worden war. Grundlage für diesen Entwurf ist eine Anordnung des US-amerikanischen Präsidenten für die Verbesserung von (Sicherheits-) Garantien für US-nachrichtendienstliche Aktivitäten („EO 14086"). Ob dies allerdings ausreicht, um ein angemessenes Schutzniveau bejahen zu können, bleibt der gründlichen Prüfung durch den EDSA vorbehalten, deren Ergebnis im Frühjahr 2023 vorgelegt werden soll.

Gesetzgebungsverfahren

Ein bedeutendes Gesetzgebungsverfahren im Rahmen der Digitalisierung der Verwaltung ist die Novellierung des Onlinezugangsgesetzes (OZG). Die unter der Bezeichnung OZG 2.0 bekannte Neufassung soll die sichtbar gewordenen Umsetzungsdefizite der alten Fassung beseitigen und für mehr Rechtssicherheit sorgen. Meine Behörde ist Mitglied der Kontaktgruppe „OZG 2.0" der Datenschutzkonferenz (DSK) und begleitet in dieser Funktion den Gesetzgebungsprozess mit. Aus datenschutzrechtlicher Sicht muss dabei insbesondere die eindeutige Zuweisung der datenschutzrechtlichen Verantwortlichkeit entlang der neu entstehenden, digitalen Serviceketten vom Antragsteller bis zur Fachbehörde und zurück normenklar abgebildet werden.

Digitalisierung der Schulen

Mit meinem Kontrollverfahren zu Datenschutzkonzepten an 50 allgemeinbildenden und berufsbildenden Schulen konnte ich mir einen Überblick über das dort bestehende Datenschutzniveau verschaffen und daraus, soweit erforderlich, entsprechende Handlungsempfehlungen ableiten. Es hat sich dabei gezeigt, dass die Schulen viele Anforderungen der DS-GVO, wie beispielsweise die Bestellung von Datenschutzbeauftragten, die Aufstellung eines Verzeichnisses der Verarbeitungstätigkeiten oder die Entwicklung eines Löschkonzeptes, überwiegend zufriedenstellend gelöst haben. Deutlich schlechter sieht es hingegen bei der Nutzung digitaler Lernsoftware im Unterrichtsalltag aus. Hier hat es das Kultusministerium versäumt, im Vorfeld die datenschutzrechtliche Unbedenklichkeit der eingesetzten „intelligenten Tutorensysteme" zu prüfen. Nach wie vor fehlt es darüber hinaus an einer Gesamtstrategie, die angefangen vom Kultusministerium bis zu den Schulen den Verantwortlichen beim Einsatz digitaler Lösungen ausreichend Hilfestellung und Rechtssicherheit bietet.

MS 365

Im aktuellen Berichtszeitraum legte die DSK ihren Abschlussbericht zu den Mängeln des Datenschutznachtrags von Microsoft („DPA“) und den Auswirkungen des Schrems II-Urteils auf den internationalen Datenverkehr vor. Wir mussten feststellen, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten DPA vom 15. September 2022 nicht geführt werden kann. Damit können Verantwortliche durch den Abschluss der Standardvertragsunterlagen von Microsoft ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nicht nachkommen. Ich werde mich im kommenden Berichtszeitraum sowohl mit dem zum 01.01.2023 aktualisierten DPA als auch mit den Entwicklungen im Bereich des internationalen Datenverkehrs weiter befassen und den Verantwortlichen im öffentlichen Bereich auch beratend zur Seite stehen.

Smart-Data-Verfahren der genossenschaftlichen Banken

Im Berichtszeitraum habe ich 89 genossenschaftliche Banken in Niedersachsen vor der Durchführung von acht in der Erprobung befindlichen Smart-Data-Verfahren aufgrund nicht vorhandener Rechtsgrundlagen gewarnt. Bei diesen Smart-Data-Verfahren handelt es sich um Algorithmen, die vor allem aus den bei der Bank vorhandenen personenbezogenen Daten eine Wahrscheinlichkeit dafür berechnen, dass Kunden bei werblicher Ansprache ein bestimmtes Produkt erwerben. Darüber hinaus habe ich weitere Kontrollverfahren gegen

niedersächsische Genossenschaftsbanken in diesem sensiblen Bereich eingeleitet, die ich im nächsten Berichtszeitraum fortsetzen werde.

PUR-Abo-Modell auf Webseiten

Neben den zahlreichen Beschwerden gegen gängige Einwilligungsbanner auf Webseiten erreichten mich immer mehr Eingaben gegen sogenannte Pur-Abo-Modelle. Entweder schließen Nutzer das Pur-Abo ab und zahlen einen Monatsbeitrag, um ohne Werbung und ohne Werbetracking die Webseite besuchen zu können oder sie willigen insbesondere in personalisierte Werbung, Werbetracking, individuelle Profilbildung und individuelle Nutzungsanalyse ein. Aus dem Datenschutzrecht lässt sich kein Anspruch des Nutzers auf einen kostenlosen Zugang zu Onlinemedien ableiten. Der Medienanbieter kann grundsätzlich entscheiden, an welche Voraussetzungen er das Lesen der Webseite knüpft und wie er diese finanziert. Allerdings muss jedes gewählte Geschäftsmodell und dessen Umsetzung auf der Webseite den rechtlichen Anforderungen des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) und der DS-GVO entsprechen, was in der Praxis häufig nicht der Fall ist.

Ich bin sicher, dass mich die Pur-Abo-Modelle auf Webseiten auch 2023 noch intensiv beschäftigen werden. Verantwortlichen sollten klare Bewertungsmaßstäbe an die Hand gegeben werden. Ich werde mich dafür einsetzen, dass sich die DSK zum Pur-Abo-Modell positioniert.

Aufklärung und Öffentlichkeitsarbeit

Bereits heute sammelt ein modernes Fahrzeug im Gigabyte-Maßstab Daten. Mit der Weiterentwicklung in Richtung auf autonomes und vernetztes Fahren wird der Datenberg um ein Vielfaches anwachsen – eine große Herausforderung für den Datenschutz. Daher war es aus meiner Sicht an der Zeit, mit Experten aus Forschung und Wirtschaft zu beleuchten, wie es um die Datenverarbeitung und den Datenschutz in modernen Fahrzeugen bestellt ist. In einer gut besuchten Veranstaltung meiner Behörde mit dem Titel „Autos und ihre Daten – so fährt die Zukunft“ diskutierte ich mit Experten, welche Herausforderungen und Chancen daraus entstehen.

In meinem Datenschutzinstitut konnte ich anders als im Jahr 2021 in 2022 sowohl im Online Format als auch in Präsenz Kurse anbieten. Erstmalig wurden auch Schulungen zum Thema „Datenschutz im Verein“ und zum Beschäftigtendatenschutz für Teilnehmer aus kleinen und mittleren Unternehmen durchgeführt.

C. Europäischer Datenschutz

C.1. Wien-Beschlüsse zur Zusammenarbeit im Kooperationsverfahren der Aufsichtsbehörden

Die Mitglieder des Europäischen Datenschutzausschusses (EDSA) haben in einer Sitzung in Wien im Frühjahr 2022 beschlossen, die Zusammenarbeit in strategisch bedeutsamen Fällen weiter zu verstärken. Jedes Jahr soll eine Reihe von grenzüberschreitenden Fällen mit strategischer Bedeutung ermittelt werden, bei denen der EDSA Unterstützung bietet und für die ein fester Zeitplan für die Zusammenarbeit aufgestellt wird. Meine Behörde hat in einer Arbeitsgruppe mitgearbeitet, um die Kriterien zur Fallauswahl und das Verfahren im Einzelnen festzulegen. Auf dieser Grundlage hat der EDSA im Juli 2022 das Papier „Selection of cases of strategic importance" verabschiedet.

Zusammenarbeit der europäischen Aufsichtsbehörden in Fällen grenzüberschreitender Datenverarbeitungen

Bei grenzüberschreitenden Datenverarbeitungen, beispielweise dem Betrieb eines Onlineshops, dessen Angebote sich an Kundinnen und Kunden in mehreren Mitgliedsstaaten der EU richten, findet die Aufsicht und Durchsetzung der DS-GVO im Kooperationsverfahren gem. Art. 60 DS-GVO statt. In diesem Verfahren wird zwischen einer federführenden und einer oder ggf. mehreren betroffenen Aufsichtsbehörden unterschieden. Federführend ist die Aufsichtsbehörde am Ort der europäischen Hauptniederlassung eines Verantwortlichen. Betroffen sind Aufsichtsbehörden am Ort anderer europäischer Niederlassungen sowie die Aufsichtsbehörde, bei welcher eine Beschwerde eingereicht wurde. Die federführende Behörde führt die Ermittlung des Sachverhaltes durch und legt den betroffenen Aufsichtsbehörden unverzüglich einen Beschlussentwurf vor. Während des Kooperationsverfahrens sind die federführende und die betroffenen Aufsichtsbehörden dazu verpflichtet, un-

tereinander so zeitnah wie möglich alle zweckdienlichen Informationen auszutauschen. Dazu muss die federführende Behörde frühzeitig den betroffenen Behörden ihre Ermittlungsergebnisse übermitteln. In der bisherigen Praxis hat sich gezeigt, dass insbesondere in sehr komplexen Fällen die Zusammenarbeit der Aufsichtsbehörden noch weiter verbessert werden kann. Insbesondere soll erreicht werden, dass die federführenden Aufsichtsbehörden ihre Beschlussentwürfe rascher vorlegen.

Kriterien zur Auswahl von Fällen von strategischer Bedeutung

Die Tätigkeit der Arbeitsgruppe war erfolgreich, sodass der EDSA bereits nach wenigen Wochen die folgenden Kriterien zur Auswahl von Fällen strategischer Bedeutung verabschieden konnte:
Vorliegen eines strukturellen oder wiederkehrenden Problems in mehreren Mitgliedstaaten, insbesondere wenn der Fall eine allgemeine rechtliche Frage im Zusammenhang mit der Auslegung, Anwendung oder Durchsetzung der DS-GVO betrifft,

- Vorliegen eines Falles, der die Schnittstelle zwischen dem Datenschutz und anderen Rechtsbereichen betrifft,
- Vorliegen eines Falles, der eine große Zahl betroffener Personen in mehreren Mitgliedstaaten betrifft,
- Vorliegen eines Falles, der zu einer großen Zahl von Beschwerden in mehreren Mitgliedstaaten geführt hat,
- Vorliegen eines Falles, der eine grundlegende Frage betrifft, die in den Anwendungsbereich der EDSA-Strategie fällt,
- Vorliegen eines Falles, bei dem nach der DS-GVO von einem hohen Risiko auszugehen ist, beispielsweise
  - bei der Verarbeitung besonderer Datenkategorien,
  - bei der Verarbeitung von Daten schutzbedürftiger Personen wie Minderjähriger,
  - in Situationen, in denen eine Datenschutz-Folgenabschätzung erforderlich ist.

Anhand dieser Kriterien wurden bereits im Juli-Plenum des EDSA erste Pilotfälle von strategischer Bedeutung ausgewählt, und die vertiefte Zusammenarbeit der Aufsichtsbehörden in diesen Fällen hat begonnen. Erste Erfolge sind bereits sichtbar, denn es ist zu erwarten, dass erste Fälle im ersten Halbjahr 2023 erfolgreich abgeschlossen werden können und weitere Fälle im zweiten Halbjahr folgen werden.

Ich bin zuversichtlich, dass sich infolge der Wien-Beschlüsse die Zusammenarbeit der Aufsichtsbehörden noch weiter verbessern und der Vollzug der DS-GVO dadurch auch langfristig spürbar gestärkt wird.

C.2. Leitlinien zur Berechnung von Bußgeldern

Der Europäische Datenschutzausschuss (EDSA) hat im Frühjahr 2022 Leitlinien zur Berechnung von Geldbußen nach Artikel 83 DS-GVO in einer Konsultationsfassung veröffentlicht (Version 1.0). Ziel ist eine harmonisierte Sanktionierung von Verstößen gegen Datenschutzvorschriften im gesamten Europäischen Wirtschaftsraum.

Ausgangslage

Verschiedene europäische Aufsichtsbehörden haben sich bereits öffentlich bekannte oder interne Leitlinien gegeben, um Geldbußen gleichmäßig zumessen zu können. Zu nennen sind hier beispielsweise die niederländische Aufsichtsbehörde, die deutsche Datenschutzkonferenz (DSK) und die dänische Aufsichtsbehörde. Mit den neuen Bußgeldleitlinien des EDSA soll die Methodik der Bußgeldberechnung im gesamten Europäischen Wirtschaftsraum harmonisiert werden. Die neuen Leitlinien sollen grundsätzlich für die Berechnung gegenüber allen Arten von Verantwortlichen oder Auftragsverarbeitern gelten. Ausnahmen, beispielsweise für Vereine, sind nicht vorgesehen.

Bußgeldleitlinien des EDSA vom 12.05.2022 (Kurzlink): https://t1p.de/Bussgeld-leitlinien

Berechnungsmethode

Das Standardmodell für die Berechnung sieht fünf Schritte vor:

1. Konkurrenzen
2. Ermittlung eines Ausgangsbetrages
3. Berücksichtigung weiterer erschwerender oder mildernder Umstände
4. Prüfung des ermittelten Betrages am gesetzlichen Höchstbetrag
5. Prüfung auf Wirksamkeit, Verhältnismäßigkeit und Abschreckungseffekt der Geldbuße

Schritt 1: Konkurrenzen

Im ersten Schritt werden zum einen unechte Konkurrenzen (Spezialität, Subsidiarität und Konsumtion) betrachtet, bei denen ein Tatbestand von einem anderen verdrängt wird und somit nicht zur Anwendung kommt. Zum anderen geht es um Fälle echter Konkurrenzen (Idealkonkurrenz, Realkonkurrenz), bei denen alle konkurrierenden Tatbestände in der Entscheidung der Behörde aufgeführt werden, weil dieselbe Handlung mehrere Tatbestände (ungleichartige Tateinheit) oder denselben Tatbestand mehrfach verletzt (gleichartige Tateinheit) oder mehrere Tatbestände durch mehrere Handlungen verletzt wer-

den (Realkonkurrenz). Als Beispiel für Idealkonkurrenz wird in den Leitlinien angegeben, dass ein Verantwortlicher im Laufe eines Tages in verschiedenen Wellen gebündelte Marketing-E-Mails an Gruppen von betroffenen Personen versendet, ohne dafür eine Rechtsgrundlage zu haben, und damit mehrmals mit einer einzigen Handlung gegen Art. 6 Abs. 1 DS-GVO verstößt.

Beispiel

Im deutschen Recht wird bei Idealkonkurrenz nur eine Geldbuße festgesetzt (§ 41 Abs. 1 BDSG i.V.m. § 19 Abs. 1 OWiG), wobei bei der Verletzung mehrerer Gesetze die Geldbuße nach dem Gesetz bestimmt wird, das die höchste Geldbuße androht (§ 41 Abs. 1 BDSG i.V.m. § 19 Abs. 2 OWiG). Bei Realkonkurrenz wird für jede Gesetzesverletzung eine Geldbuße festgesetzt (§ 41 Abs. 1 BDSG i.V.m. § 20 OWiG), und die Geldbußen werden im Bußgeldbescheid addiert.

Außerdem wird Art. 83 Abs. 3 DS-GVO berücksichtigt, der den Gesamtbetrag der Geldbuße auf das gesetzliche Höchstmaß des schwersten Verstoßes begrenzt, wenn ein Verantwortlicher oder ein Auftragsverarbeiter schuldhaft mehrere DS-GVO-Vorschriften verletzt und es sich um gleiche oder miteinander verbundene Verarbeitungsvorgänge handelt. Die Vorschrift erinnert an Fälle der Idealkonkurrenz im deutschen Recht und ist damit einschlägig, wenn durch dieselbe Handlung mehrere DS-GVO-Bestimmungen verletzt werden. Völlige Deckungsgleichheit besteht allerdings nicht, zumal eine Orientierung an Begriffen der deutschen Konkurrenzlehre ohnehin nur der besseren Veranschaulichung dienen kann, aber aufgrund der erforderlichen europarechtsautonomen Auslegung letzten Endes nicht maßgeblich ist.

Besondere Konkurrenz im EU-Recht

Schritt 2: Ausgangsbetrag der Geldbuße

Zunächst wird der Verstoß in den maßgeblichen gesetzlichen Bußgeldrahmen eingeordnet, also in den Korridor bis 10 Millionen Euro bzw. 2 Prozent des weltweiten Jahresumsatzes oder in den Korridor bis 20 Millionen Euro bzw. 4 Prozent. Anschließend erfolgt die Einteilung in einen von drei Schweregraden anhand der Kriterien des Art. 83 Abs. 2 Satz 2 lit. a, b, g DS-GVO. Berücksichtigt werden also insbesondere Art, Schwere und Dauer des Verstoßes, die Verschuldensform wie Vorsatz und Fahrlässigkeit und die Kategorien der verarbeiteten personenbezogenen Daten. Aus diesen Kriterien wird eine Spanne ermittelt, die sich zunächst prozentual am gesetzlichen Höchstbetrag einer möglichen Geldbuße orientiert.

Erstens: Bußgeldrahmen

Zweitens: Schweregrad

Anschließend kann (und wird im Regelfall) der Umsatz des Unternehmens berücksichtigt werden. Die Einteilung erfolgt in sieben verschiedene Größenklassen. Je umsatzschwächer ein Unternehmen der jeweiligen Klasse ist, desto niedriger ist der Rechenfaktor und desto stärker die Reduzierung des individuellen Bußgeldkorridors, der für die weitere Berechnung herangezogen wird.

Drittens: Umsatz des Unternehmens

Exemplarisch ergibt sich folgende Tabelle bei Verstößen im höheren Bußgeldrahmen (Art. 83 Abs. 5 und 6 DS-GVO, Beträge in Euro):

Umsatz im Vorjahr	Rechenfaktor	Verstoß „niedrig“	Verstoß „mittel“	Verstoß „hoch“
Bis zu 2 Mio.	0,002 (0,2 %)	Über 0 bis 4.000	4.000 bis 8.000	8.000 bis 40.000.
Über 2 Mio. bis zu 10 Mio.	0,004 (0,4 %)	Über 0 bis 8.000	8.000 bis 16.000	16.000 bis 80.000
Über 10 Mio. bis zu 50 Mio.	0,020 (2,0 %)	Über 0 bis 40.000	40.000 bis 80.000	80.000 bis 400.000
Über 50 Mio. bis zu 100 Mio.	0,100 (10,0 %)	Über 0 bis 200.000	200.000 bis 400.000	400.000 bis 2.000.000
Über 100 Mio. bis zu 250 Mio.	0,200 (20,0 %)	Über 0 bis 400.000	400.000 bis 800.000	800.000 bis 4.000.000
Über 250 Mio. bis zu 500 Mio.	0,500 (50 %)	Über 0 bis 1.000.000	1.000.000 bis 2.000.000	2.000.000 bis 10.000.000
Über 500 Mio.	Anteil des Umsatzes	Über 0 bis 0,4 %	0,4 % bis 0,8 %	0,8 % bis 4,0 %

Bei der abgebildeten Tabelle handelt es sich um mein Verständnis der Konsultationsfassung der Leitlinien. Der Ausschuss hat angekündigt, mit der finalen Fassung der Leitlinien eine offizielle Tabelle zu veröffentlichen. Zudem sind infolge der Konsultation weitere Änderungen am Berechnungsmodus nicht ausgeschlossen.

Schritt 3: Weitere erschwerende oder mildernde Umstände

Hier werden alle Kriterien angewendet, die nicht bereits im zweiten Schritt zur Ermittlung des Ausgangsbetrags verwendet wurden. Die Leitlinien enthalten zahlreiche Beispiele, welche Ausprägungen erschwerend und welche mildernd auf die Geldbuße wirken können. So wird etwa klargestellt, dass einschlägige frühere Verstöße erschwerend wirken. Mildernd wirkt es hingegen, wenn Verantwortliche Maßnahmen ergreifen, um Schäden für die Betroffenen zu reduzieren, wobei wiederum zu berücksichtigen ist, wie zeitnah diese Maßnahmen nach dem Verstoß ergriffen wurden und wie effektiv sie sind. Dabei wirken solche Maßnahmen eher mildernd, die ergriffen werden, bevor die Aufsichtsbehörde ein Verfahren aufnimmt.

Maßnahmen vor Einschreiten der Aufsicht

Außerdem wird Art. 83 Abs. 2 Satz 1 lit. k DS-GVO näher umrissen, also jegliche anderen erschwerenden oder mildernden Umstände, die im Kriterienkatalog nicht explizit genannt sind. So kann sich das Nachtatverhalten mildernd auswirken, wenn der Vorwurf eingeräumt wird. Von besonderer Bedeutung ist ein etwaig erlangter wirtschaftlicher Vorteil, der abgeschöpft werden soll. Die Geldbuße muss einen solchen wirtschaftlichen Vorteil deutlich übersteigen.

Abschöpfung wirtschaftlicher Vorteile

Schritt 4: Abgleich gegen den gesetzlichen Höchstbetrag

Es wird geprüft, ob die bis zu diesem Schritt ermittelte Geldbuße den gesetzlichen Höchstbetrag überschreitet. Hierzu wird der ermittelte Betrag mit dem maßgeblichen gesetzlichen Höchstbetrag abgeglichen.

Die Leitlinien beinhalten an dieser Stelle zudem Ausführungen zur Ermittlung des Umsatzes und zur Verantwortlichkeit im Unternehmenskontext, beispielsweise wenn Verstöße durch Beschäftigte begangen wurden. Sehr wichtig und erfreulich ist zudem, dass sich der EDSA in den Leitlinien im Vorgriff auf die erwartete Klärung durch den EuGH ausdrücklich für eine unmittelbare Verbandshaftung von Unternehmen ausgesprochen hat. Hiervon geht eine hohe Signalwirkung aus. Wie bereits 2019 in einer Entschließung der DSK formuliert, gilt damit der Grundsatz: Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten.

Schritt 5: Wirksamkeit, Verhältnismäßigkeit, Abschreckungseffekt
Im letzten Schritt werden die Wirksamkeit und die Verhältnismäßigkeit des ermittelten Betrages geprüft. Ebenso wird geprüft, ob die Geldbuße hinreichend abschreckend ist, sowohl spezialpräventiv hinsichtlich des konkreten Verantwortlichen oder Auftragsverarbeiters als auch generell hinsichtlich anderer verantwortlicher Stellen.

Sollte die Geldbuße als Ergebnis dieser Prüfung nicht ausreichend hoch sein, besteht die Möglichkeit den Betrag zu erhöhen. Beispielsweise kann ein so genannter „Abschreckungsmultiplikator" angewendet werden. Zudem können in diesem Schritt Besonderheiten der wirtschaftlichen Situation berücksichtigt werden. Dies ist allerdings in der Regel nur bei außergewöhnlichen Umständen möglich, beispielsweise wenn die Rentabilität unwiederbringlich gefährdet wäre.

Ergebnis der Berechnung ist ein Bußgeldbetrag, der den Ansprüchen des Art. 83 Abs. 1 DS-GVO genügt, also wirksam, verhältnismäßig und auch abschreckend ist.

Flexibilität

Die Leitlinien weisen schon mit ihrer oben dargestellten Berechnungsmethode eine erhebliche Flexibilität auf. Der EDSA ist sich allerdings bewusst, dass dies im Einzelfall nicht genügen könnte. In den Leitlinien finden sich daher zwei wesentliche Möglichkeiten, um bei der Festsetzung der Geldbuße zusätzliche Flexibilität zu gewinnen.

Umstände des Einzelfalls
Die Leitlinien stellen in Randnummer 48 klar, dass ein Ausgangsbetrag die Behörden nicht daran hindern soll, die Geldbuße herabzusetzen oder zu erhöhen, wenn die Umstände es erfordern. Dies kann insbesondere sinnvoll sein, wenn der vom Konzept eröffnete Korridor nicht ausreichend erscheint. Besonders bei sehr schweren Verstößen kleinerer Unternehmen könnte anhand der Berechnungsmethode kein angemessen hoher Ausgangsbetrag zu identifizieren sein. Ebenso kann eine Abweichung bei weniger schwerwiegenden Verstöße sehr großer Unternehmen notwendig werden, um einen angemessenen „niedrigen" Betrag festsetzen zu können. Allerdings sollte klar sein, dass diese zusätzliche Flexibilisierung nur im Ausnahmefall angewendet werden kann und – gerade bei Abweichungen nach oben – einer besonderen Begründung bedarf.

Schwere Verstöße kleiner Unternehmen

Geldbußen mit festen Ausgangsbeträgen („fixed amounts“)
In den Randnummern 18 bis 20 räumen die Leitlinien den Aufsichtsbehörden die Möglichkeit ein, Geldbußen mit „fixed amounts“ festzusetzen und dazu eigene Maßstäbe aufzustellen.

Kein statischer Bußgeldkatalog

Die Bezeichnung ist möglicherweise etwas irreführend, da der Terminus „fixed amounts“ suggeriert, dass es sich um einen statischen Bußgeldkatalog handelt, so wie er beispielsweise aus dem Straßenverkehrs-Ordnungswidrigkeitenrecht bekannt ist. Um mit dem hergebrachten europäischen und nationalen Recht kompatibel zu sein, kann es sich indes nur um konkrete „Sockel-Beträge“ handeln, welche die Basis für die weitere Zumessung darstellen würden. Diese Sockel- oder Ausgangsbeträge wären nicht an den Umsatz eines Unternehmens gekoppelt, sondern können von den Aufsichtsbehörden für bestimmte Verstöße im Vorhinein festgelegt werden. Selbstverständlich entbindet die Festlegung solcher Ausgangsbeträge nicht davon, Art. 83 DS-GVO vollumfänglich zur Anwendung zu bringen und insbesondere die maßgeblichen Zumessungskriterien zu berücksichtigen. Letztlich kann auch die Umsatzkomponente berücksichtigt werden, allerdings auf nachgelagerter Ebene. Vor diesem Hintergrund ist die Bezeichnung „Geldbußen mit festen Ausgangsbeträgen“ deutlich treffender.

Einpreisung

Sofern eine Aufsichtsbehörde dementsprechend einen Katalog mit festen Ausgangsbeträgen für bestimmte Verstöße festlegen würde, könnte dies dazu führen, dass Unternehmen mögliche Bußgeldrisiken vorab recht konkret abschätzen könnten. Dies lässt sich kritisieren, weil Geldbußen dann in die Kalkulation „eingepreist“ werden könnten. Bei weniger gewichtigen Verstößen erscheint mir dieses Risiko allerdings vertretbar. Ohnehin rechne ich nicht damit, dass Verstöße tatsächlich häufiger „eingepreist“ werden, schließlich würde jede Aufsichtsbehörde bei erkennbar wiederholten, systematischen Verstößen zur regulären Bußgeldmethodik übergehen. Zudem dürfte ein absichtlicher Verstoß eher zur Anwendung des Standardmodells führen – und somit meist zu einer höheren Geldbuße.

Harmonisierung

Zwar kann diese Methode dazu führen, dass in den unterschiedlichen Mitgliedstaaten verschiedene Modelle für Geldbußen mit festen Ausgangsbeträgen entstehen. Deutlich unterschiedliche Beträge für gleiche Verstöße entsprächen dabei nicht dem Harmonisierungsgedanken. Allerdings kann und darf die Harmonisierung bei weniger gewichtigen Verstößen durchaus weniger ausgeprägt sein als bei schwerwiegenderen Verstößen. So ist auch zu erklären, dass das Modell in die Konsultationsfassung der Leitlinien aufgenommen wurde.

Finale Fassung der Leitlinien

Der EDSA hat im vergangenen Jahr eine öffentliche Konsultation zu den Bußgeldleitlinien durchgeführt. Zum Redaktionsschluss meines Tätigkeitsberichts war noch nicht abschließend klar, welche Änderungen noch an der Berechnungsmethodik oder den weiteren Inhalten der Leitlinien vorgenommen werden. Eine Verabschiedung der finalen Version der Leitlinien erwarte ich für das erste Halbjahr 2023. Das DSK-Konzept zur Bußgeldberechnung wird damit keine Anwendung mehr finden.

C.3. Leitlinien zum Recht auf Auskunft

Seit Einführung der Datenschutz-Grundverordnung (DS-GVO) ist insbesondere das Recht auf Auskunft gemäß Artikel 15 DS-GVO Gegenstand zahlreicher Fragen zur Anwendung und Auslegung. Die neuen Leitlinien 01/2022 des Europäischen Datenschutzausschusses (EDSA) tragen zum einfacheren Umgang mit diesem Betroffenenrecht bei.

Die am 18. Januar 2022 vom EDSA angenommene Version 1.0 der Leitlinien zum Recht auf Auskunft befasst sich mit dem Inhalt und Umfang des Rechts, mit den Modalitäten zur Geltendmachung des Rechts durch die betroffene Person und zur Erfüllung des Rechts durch den Verantwortlichen sowie mit möglichen Einschränkungen des Auskunftsrechts. Daneben werden Fragen rund um das Recht auf Kopie in Artikel 15 Absatz 3 DS-GVO behandelt. Die Leitlinien befanden sich bei Redaktionsschluss in der öffentlichen Konsultation.

Zweck des Rechts auf Auskunft

An den Anfang der Leitlinien stellt der EDSA die Bestimmung des Zwecks des Auskunftsrechts: Die betroffene Person soll durch die Ausübung des Auskunftsrechts in die Lage versetzt werden, die Kontrolle über die Verarbeitung der eigenen personenbezogenen Daten (wieder-) zu erhalten. Nur über die entsprechende Information zur Verarbeitung der eigenen Daten ist es der betroffenen Person überhaupt möglich, weitere Rechte wie das Recht auf Löschung oder Berichtigung auszuüben. Des Weiteren kann die betroffene Person die Rechtmäßigkeit der Datenverarbeitung prüfen. Die Festlegung dieses Zwecks des Auskunftsrechts bedeutet jedoch nicht, dass dieser Zweck Bedingung ist für die Ausübung des Rechts oder gar von der betroffenen Person glaubhaft dargelegt werden muss. Es genügt, wenn der Wunsch nach Transparenz über die Verarbeitung der eigenen Daten jedenfalls auch Ziel der Geltendmachung des Auskunftsrechts ist.

Inhalt und Umfang des Rechts auf Auskunft

Das Recht auf Auskunft bezieht sich auf alle beim Verantwortlichen vorhandenen personenbezogenen Daten und ist weit auszulegen. Nach den Leitlinien sind von den personenbezogenen Daten, über die Auskunft gegeben werden muss, auch solche Daten umfasst, welche Teil einer rechtlichen Bewertung,

einer Meinungsäußerung oder eines Protokolls sind, so lange sie einen Bezug zu der betroffenen Person aufweisen. Auch Daten, welche die betroffene Person ursprünglich selbst dem Verantwortlichen zur Verfügung gestellt hatte (zum Beispiel in einem Fragebogen), sind nicht von der Auskunft ausgenommen. Das Auskunftsrecht umfasst weiter Ton- oder Bilddaten oder Rohdaten, die aufgrund der Nutzung eines Dienstes erzeugt werden, wie z. B. die Historie von Webseiten-Aufrufen, Aktivitätsprotokolle oder Standortdaten. Weiterverarbeitungen von personenbezogenen Daten wie eine gesundheitliche Bewertung oder eine Bewertung auf Basis eines Algorithmus sind ebenfalls mitzuteilen. Die zuvor durchaus umstrittene Reichweite des Auskunftsrechts wird durch die eindeutigen Aussagen in den Leitlinien konkreter. Auskunft ist über die personenbezogenen Daten selbst zu erteilen, eine Umschreibung oder Zusammenfassung genügt nicht.

Soweit nicht anders ausdrücklich von der betroffenen Person erklärt, umfasst das Auskunftsrecht alle vorhandenen personenbezogenen Daten. Wenn besonders viele personenbezogene Daten verarbeitet werden, darf der Verantwortliche die betroffene Person zwar zur Konkretisierung des Auskunftsersuchens auffordern (Erwägungsgrund 63). Konkretisiert die betroffene Person jedoch ihr Auskunftsverlangen nicht, bleibt es bei der Pflicht, alle Informationen zu dieser Person herauszugeben. Auch diese Frage war bisher umstritten, da manche Verantwortliche bei Auskunftsanfragen auf einer Beschränkung der Auskunft auf bestimmte Bereiche der Datenverarbeitung bestanden und so das Auskunftsrecht auf unzulässige Weise einschränkten.

Das Recht auf Auskunft geltend machen

Die Leitlinien stellen klar, dass die betroffene Person nicht zur Angabe eines Grundes oder zur sonstigen Rechtfertigung verpflichtet ist, um Auskunft zu erhalten. Eine besondere Form dafür, dieses Recht einzufordern, ist nicht vorgesehen. Der übliche, für die Kommunikation mit Außenstehenden vorgesehene Weg kann auch dann für ein Auskunftsersuchen genutzt werden, wenn der Verantwortliche einen anderen, speziellen Kommunikationsweg vorgesehen hat. Daneben kann das Auskunftsrecht grundsätzlich auch für Dritte geltend gemacht werden, etwa für eine minderjährige Person.

Erteilung der Auskunft

Der Verantwortliche muss gemäß Artikel 12 Absatz 1 Satz 1 DS-GVO geeignete Maßnahmen treffen, um die Auskunft in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Diese Anforderungen sind nach den Leitlinien jeweils im Einzelfall anhand der Komplexität der Datenverarbeitung oder bestimmter besonderer Bedürfnisse der betroffenen Personen zu bestimmen.

Die Leitlinien treffen wichtige Aussagen zur Bedeutung des Rechts auf Kopie nach Artikel 15 Absatz 3 DS-GVO: Die Kopie der personenbezogenen Daten ist kein zusätzliches Recht neben dem

Auskunftsrecht, sondern stellt eine Modalität der Erfüllung des Auskunftsanspruchs dar. Dies bedeutet, dass das Recht auf Auskunft in der Regel durch Übermittlung einer Kopie der personenbezogenen Daten zu erfüllen ist. Dabei ist keine Übermittlung einer Reproduktion der Original-Dokumente erforderlich, sondern lediglich die Herausgabe einer Kopie der verarbeiteten personenbezogenen Daten in den Dokumenten. Diese Kopie kann durch eine Zusammenstellung aller personenbezogenen Daten übermittelt werden, soweit dies eine Überprüfung der Rechtmäßigkeit der Verarbeitung ermöglicht. Dies ist allerdings nicht zu verwechseln mit einer Zusammenfassung der Daten, vielmehr sind vollständige Informationen zu allen Daten zu beauskunften.

Auch zu anderen möglichen Formen der Auskunft und zur Erleichterung der Auskunftserteilung treffen die Leitlinien klare Aussagen: In geeigneten Fällen kann die Auskunft auch in anderer Form erteilt werden, zum Beispiel durch Fernzugriff auf Online-Dokumente. Vor allem in Fällen, in welchen eine sehr große Menge an Daten zu der betroffenen Person vorhanden ist, kann die Auskunft mehrschichtig erfolgen. In der ersten Ebene der Auskunft sollten dann diejenigen Informationen enthalten sein, welche für die betroffene Person voraussichtlich am relevantesten sind oder die größten Auswirkungen haben könnten. Der mehrschichtige Ansatz soll allerdings ausschließlich der betroffenen Person helfen, die bereitgestellten Informationen zu verstehen und nicht etwa dem Verantwortlichen Arbeit ersparen, weitere Informationen zu übermitteln. Die betroffene Person hat immer ein Wahlrecht, ob sie sofort auf alle vorhandenen Daten zugreifen möchte oder mit dem Zugriff auf eine oder zwei Ebenen zufrieden ist. Bei besonders komplexen Datenverarbeitungen besteht eine zusätzliche Verpflichtung des Verantwortlichen zur Erläuterung der Daten, zum Beispiel bei unverarbeiteten Rohdaten.

Gemäß Artikel 12 Absatz 3 Satz 1 DS-GVO ist die Auskunft unverzüglich zu erteilen, jedenfalls aber innerhalb eines Monats nach Eingang des Auskunftsersuchens. Diese Frist beginnt, wenn das Auskunftsersuchen den Verantwortlichen auf einem der offiziellen Kommunikationswege erreicht. Sind weitere Nachfragen zum Auskunftsersuchen erforderlich, etwa zur Identifizierung der betroffenen Person oder zum Umfang der Auskunft, wird die Frist entsprechend ausgesetzt.

Einschränkungen des Auskunftsrechts

Einschränkungen des Auskunftsrechts sind nach Artikel 15 Absatz 4 DS-GVO möglich, wenn die Auskunft die Rechte und Freiheiten anderer Personen beeinträchtigen würde. Dies betrifft gemäß Erwägungsgrund 63 insbesondere Geschäftsgeheimnisse, Rechte des geistigen Eigentums und das Urheberrecht

an Software. Auch Datenschutzrechte anderer Personen stellen in diesem Sinne Rechte anderer Personen dar. Die Leitlinien erläutern weiter, dass bei Betroffenheit solcher Rechte anderer der Verantwortliche eine Abwägung zwischen den verschiedenen Interessen unter Berücksichtigung der konkreten Risiken für die anderen Personen bei Offenlegung der Daten vorzunehmen hat. Jedenfalls berechtigt eine Beeinträchtigung der Rechte anderer den Verantwortlichen nicht dazu, die Auskunft insgesamt zu versagen, gegebenenfalls sind Schwärzungen oder Ähnliches bei der Auskunft vorzunehmen. Nach Festlegung in den Leitlinien gilt die Regelung des Artikel 15 Absatz 4 DS-GVO nicht nur für die Übermittlung einer Kopie der personenbezogenen Daten nach Absatz 3, sondern für alle Formen in denen Daten zur Vefügung gestellt werden.

Bei einem offenkundig unbegründeten oder exzessiven Auskunftsantrag darf der Verantwortliche gemäß Artikel 12 Absatz 5 DS-GVO entweder ein angemessenes Entgelt verlangen oder die Auskunft verweigern. Nach den Leitlinien ist nach den Umständen des Einzelfalles unter Berücksichtigung der vorhergehenden Auskunftsanträge zu bewerten, ob ein exzessiver Auskunftsantrag in diesem Sinne vorliegt. Treten öfter Veränderungen in der konkreten Datenverarbeitung auf, handelt es sich um besonders sensible Daten, sind mit der Datenverarbeitung besondere Risiken verbunden oder betrifft der aktuelle Auskunftsantrag andere Datenverarbeitungssituationen als die vorherigen, handelt es sich eher nicht um einen exzessiven Auskunftsantrag. In jedem Fall obliegt dem Verantwortlichen die Pflicht zu begründen, warum er von einem offenkundig unbegründeten oder exzessiven Antrag ausgeht und die Auskunft verweigert.

C.4. Streitbeilegungsverfahren des EDSA

Im Jahr 2022 führte der Europäische Datenschutzausschuss (EDSA) fünf Streitbeilegungsverfahren gem. Art. 65 Abs.1 lit. a DS-GVO durch. Solche Verfahren sind erforderlich, wenn sich bei grenzüberschreitenden Verarbeitungen die beteiligten Datenschutzaufsichtsbehörden im Kooperationsverfahren gem. Art. 60 DS-GVO hinsichtlich des Ergebnisses einer Untersuchung nicht einigen können. Meine Behörde war an den Verhandlungen zur Ausarbeitung der Entscheidungen des EDSA an allen im Jahr 2022 durchgeführten Streitbeilegungsverfahren beteiligt.

Klarstellungen zur Reichweite von Art. 6 Abs. 1 lit. b DS-GVO

In drei Streitbeilegungsverfahren in Sachen Facebook, Instagram und WhatsApp wurde die Fragestellung erörtert, ob sich Verantwortliche für Verarbeitungen personenbezogener Daten zur Erstellung verhaltensbezogener Werbung bzw. der Verbesserung des Produktes und von Sicherheitsfunktionen, die über die Anforderungen von Art. 32 DS-GVO hinausgehen, auf Art. 6 Abs. 1 lit. b DS-GVO stützen können. Die irische Datenschutzaufsichtsbehörde (Data Protection Commission, DPC) hatte das in ihren Beschlussentwürfen bejaht. Verschiedene europäische Aufsichtsbehörden legten gegen diese Beschlussentwürfe Einsprüche ein.

Der EDSA gelangte nach mehreren vorbereitenden Sitzungen der Enforcement Subgroup, in der meine Behörde die Interessen der deutschen Länder vertritt, zu dem Ergebnis, dass die DPC ihre Beschlussentwürfe ändern muss, denn die Datenverarbeitungen zu den genannten Zwecken sind nicht für die Erfüllung vertraglicher Verpflichtungen gegenüber den Nutzern erforderlich. Daher haben sich die Verantwortlichen bei der Verarbeitung zu Unrecht auf Art. 6 Abs. 1 lit. b DS-GVO gestützt. Da sich die Verantwortlichen nicht auf Einwilligungen gestützt haben und im Übrigen in den konkreten Fällen keine weitere Rechtsgrundlage in Frage kam, haben sie folglich gegen Art. 6 Abs. 1 DS-GVO verstoßen. Zudem wurden Verstöße gegen den Grundsatz zur Datenverarbeitung nach Treu und Glauben gem. Art. 5 Abs. 1 lit. a DS-GVO festgestellt.

Die DPC wurde angewiesen, auf diese massiven Verstöße gegen die DS-GVO durch Anweisungen gem. Art. 58 Abs. 2 lit. d DS-GVO zu reagieren. Diese sollen die Verantwortlichen verpflichten, die oben genannten Datenverarbeitungen in Einklang

mit der DS-GVO zu bringen. Zusätzlich sollten wirksame, verhältnismäßige und abschreckende Bußgelder gegen die Verantwortlichen verhängt werden.

Bezüglich der folgenden Fragestellungen soll die DPC weitere Ermittlungen anstellen und zu diesem Zweck neue Kooperationsverfahren eröffnen:

- Verarbeitet Meta Irland in seinem Facebook- und/oder Instagram-Dienst besondere Kategorien personenbezogener Daten (Artikel 9 DS-GVO) zum Zwecke verhaltensbezogener Werbung?
- Verarbeitet WhatsApp besondere Kategorien personenbezogener Daten sowie personenbezogene Daten für Zwecke verhaltensbezogener Werbung, für Marketingzwecke oder für die Bereitstellungen von Kennzahlen an Dritte und für den Austausch von Daten mit verbundenen Unternehmen zum Zwecke der Verbesserung der Dienste?
- Sofern das der Fall ist, werden dabei die einschlägigen Verpflichtungen der DS-GVO eingehalten?

Hintergrund der Anordnung weiterer Ermittlungen durch den EDSA ist, dass die DPC mit ihrem Untersuchungsumfang hinter den in der Beschwerde vorgetragenen Punkten zurückgeblieben ist.

Ende Dezember 2022 hat die DPC als Reaktion auf die in den Streitbeilegungsverfahren Facebook und Instagram ergangenen verbindlichen Beschlüsse ihre endgültigen Entscheidungen erlassen. Gegen Meta wurde wegen der Verstöße im Zusammenhang mit Facebook ein Bußgeld in Höhe von 210 Millionen Euro erlassen. Dabei entfällt ein Anteil von 60 Millionen Euro auf die Sanktionierung des Verstoßes gegen Art. 6 Abs. 1 DS-GVO. Der restliche Bußgeldbetrag wurde wegen Verstößen gegen die Informationspflichten verhängt. Die Höhe des wegen der Verstöße im Zusammenhang mit Instagram erlassenen Bußgeldes beträgt 180 Millionen. Hier entfallen 50 Millionen Euro auf eine Sanktionierung des Art. 6 Abs. 1 DS-GVO-Verstoßes.

Mitte Januar 2023 hat die DPC in Sachen WhatsApp ihren endgültigen Beschluss erlassen. Das gegen WhatsApp verhängte Bußgeld beträgt 5,5 Millionen Euro.

Ich begrüße die Entscheidung des EDSA, dass es Verantwortlichen nicht gestattet ist, das Erfordernis der Einwilligung für Tracking und Online-Werbung zu umgehen, indem sie argumentierten, dass die Einblendung verhaltensbasierter Werbeanzeigen Teil ihrer vertraglich gegenüber den Nutzern geschuldeten Leistung ist. Diese Entscheidung wird dazu beitragen, in zukünftigen

Verfahren den Schutz der personenbezogenen Daten der Bürgerinnen und Bürger spürbar zu verbessern.

Ich hoffe, dass von diesen Verfahren die Botschaft an die Verantwortlichen ausgeht, dass sich Verstöße gegen die DS-GVO nicht auszahlen.

Stärkung des Schutzes minderjähriger Nutzer sozialer Netzwerke

In einem weiteren Streitbeilegungsverfahren hat der EDSA die DPC wegen eines festgestellten Verstoßes gegen Art. 6 Abs. 1 DS-GVO zur Verhängung eines wirksamen, verhältnismäßigen und abschreckenden Bußgeldes gegen den Verantwortlichen verpflichtet. Hintergrund dieses Streitbeilegungsverfahrens war eine Untersuchung der von Instagram praktizierten Offenlegung der E-Mail-Adressen und/oder Telefonnummern von Kindern, welche die Funktion Instagram Business-Konto nutzen. Betrachtet werden musste weiterhin die Tatsache, dass während des Untersuchungszeitraums die persönlichen Konten von Kindern auf Instagram laut der Voreinstellung standardmäßig öffentlich waren. Während der laufenden Untersuchung hatte der Verantwortliche für Abhilfe gesorgt.

Die DPC hatte in ihrem Beschlussentwurf Verstöße gegen die Art. 5 Abs. 1 lit. a und c, 12 Abs. 1, 25 Abs. 1 und 2 sowie 35 Abs. 1 DS-GVO festgestellt. Der EDSA hat die DPC angewiesen, einen zusätzlichen Verstoß gegen Art. 6 Abs. 1 DS-GVO festzustellen, weil sich der Verantwortliche weder auf Art. 6 Abs. 1 lit. b DS-GVO noch auf Art. 6 Abs. 1 lit. f DS-GVO berufen konnte. Einwilligungen hatte der Verantwortliche nicht eingeholt. Ferner hat der EDSA die irische Aufsichtsbehörde angewiesen, ihre geplanten Abhilfemaßnahmen im Einklang mit den Schlussfolgerungen des EDSA erneut zu bewerten, um dem zusätzlichen Verstoß gegen Art. 6 Abs. 1 DS-GVO Rechnung zu tragen und sicherzustellen, dass der Verantwortliche die Verpflichtungen nach Art. 6 Abs. 1 DS-GVO in vollem Umfang umsetzt. In Bezug auf die Berechnung der Bußgeldhöhe hat der EDSA die DPC u. a. angewiesen, den festgestellten Verstoß gegen Art. 6 Abs. 1 DS-GVO bei der Festsetzung der Geldbußen zu berücksichtigen, eine zusätzliche Geldbuße zu verhängen, die wirksam, verhältnismäßig und abschreckend ist. Zudem sollte die Auffassung des EDSA berücksichtigt werden, dass jede Geldbuße im vorliegenden Fall in den höheren Bereich der von der DPC vorgeschlagenen Bußgeldspannen fallen sollte.

In ihrer final decision hat die DPC gegen den Verantwortlichen ein Bußgeld in Höhe von insgesamt 405 Millionen Euro verhängt.

Diese Entscheidung des EDSA begrüße ich, denn mit seinem verbindlichen Beschluss hat der EDSA verdeutlicht, dass Unternehmen, die Minderjährige als Zielgruppe haben, besonders sorgfältig mit deren personenbezogenen Daten umgehen müssen.

Erhöhung eines von der federführenden Aufsichtsbehörde vorgeschlagenen Bußgeldes

In diesem Streitbeilegungsverfahrens war zwischen Frankreich und Polen umstritten, ob ein Bußgeld in Höhe von 100.000 € gegen die französische Hotelkette Accor wegen Verstößen gegen Art. 12 Abs. 1, 12 Abs. 3, 13, 15 Abs. 1, 21 Abs. 2 und 32 DS-GVO wirksam, verhältnismäßig und abschreckend wäre.

Als Ergebnis dieses Streitbeilegungsverfahrens wies der EDSA die französische Datenschutzbehörde an, das vorgesehene Bußgeld neu zu berechnen, um das Kriterium der Abschreckung nach Art. 83 Abs. 1 DS-GVO zu erfüllen, wobei insbesondere der relevante Umsatz des Unternehmens zu berücksichtigen sei. Um die Auswirkungen der Corona-Krise bei der Bußgeldhöhe zu berücksichtigen, sollte Frankreich die finanzielle Lage des Unternehmens auf der Grundlage dessen relevanter Umsatzzahlen gem. Art. 83 Abs. 1 DS-GVO berücksichtigen.

In ihrem endgültigen Beschluss verhängte die französische Aufsichtsbehörde ein Bußgeld in Höhe von 600.000 Euro gegen das Unternehmen. Davon entfallen 500.000 Euro auf die festgestellten Verstöße gegen die DS-GVO. Der Betrag von 100.000 Euro wurde wegen Verstößen gegen nationales französisches Recht verhängt.

D. Internationaler Datenverkehr

Neue Entwicklungen im internationalen Datenverkehr

Im Jahr 2022 habe ich meine Prüfung zur Umsetzung der Anforderungen des Schrems II-Urteils[1] fortgesetzt und erreicht, dass eine Vielzahl von Datentransfers abgestellt wurde. Außerdem habe ich mich 2022 mit der Frage beschäftigt, unter welchen Rahmenbedingungen europäische Tochterunternehmen von US-Cloud-Anbietern als Auftragsverarbeiter gemäß der DS-GVO eingesetzt werden dürfen. Seit dem Frühjahr 2022 richtet sich der Blick von Wirtschaft, Verwaltung und Fachöffentlichkeit auf die Zukunft des transatlantischen Datenschutzes, nachdem von der Politik ein Nachfolge-Abkommen zum Privacy Shield angekündigt und im Dezember von der Kommission der Europäischen Union der Entwurf für einen Angemessenheitsbeschluss für die USA vorgelegt worden war.

Fortsetzung der Schrems II-Prüfung

Meine anlasslose Kontrolle zur Umsetzung der Anforderungen des Schrems II-Urteils[2] habe ich im Jahr 2022 fortgesetzt. Erfreulicherweise konnte ich mich bislang bei meinen Überprüfungen davon überzeugen, dass sich die eingesetzten Internet-Server innerhalb des Europäischen Wirtschaftraums befinden. Ungeachtet des Serverstandorts verblieb in vielen Fällen das Problem, dass es im Rahmen von Wartungs- oder Supportdienstleistungen ggf. zu einer kurzfristigen Kenntnisnahmemöglichkeit von personenbezogenen Daten durch eingesetzte US-Auftragsverarbeiter kommen kann. Die Ansicht der Verantwortlichen, dass aufgrund der ergriffenen zusätzlichen vertraglichen, organisatorischen oder technischen Maßnahmen die vom EuGH festgestellten Unzulänglichkeiten des US-Rechts ausgeglichen und die Wirksamkeit der genutzten Standardvertragsklauseln als Transferinstrument sichergestellt werde, hat mich nicht restlos überzeugt. Ich habe je nach Ausgestaltung der Fernwartung im konkreten Einzelfall Warnungen ausgesprochen oder Hinweise erteilt.

Hosting im EWR

Warnungen und Hinweise

Weitere datenschutzrechtliche Probleme habe ich im Zusammenhang mit der Einbindung von Drittdiensten festgestellt. In mehreren Verfahren habe ich im Rahmen der Prüfung Datentransfers in Drittländer festgestellt, obwohl die Verantwortlichen dies in meinem Fragebogen zunächst

Eingebundene Drittdienste

1 Zum Schrems II-Urteil ausführlich siehe TB 2020, S. 27.
2 Siehe TB 2021, S. 25.

verneint hatten. Im Zuge der Kontrolle entfernte ein Verantwortlicher in den USA fremdgehostete Webfonts von seiner Webseite, wechselte zu einem datenschutzfreundlicheren Tracking-Tool und ersetzte alle Verknüpfungen zu gespeicherten Videos bei einem US-Anbieter durch die Einbindung lokaler Videos. Zwei Verantwortliche beendeten die Einbindung eines Content Delivery Networks mit US-Standort. Ein Verantwortlicher behob in seinem Content Management System eine Fehlkonfiguration und änderte die Einstellung auf Europa. Ein Verantwortlicher wechselte von einem US-Hosting-Anbieter (mit deutschem Server-Standort) zu einem deutschen Webhoster. In zwei Fällen befasste ich mich mit stetigen Datenübermittlungen an in den USA konnektierte Domains zu Authentisierungszwecken. Nach Angaben des Verantwortlichen handelte es sich dabei um eine zu Sicherheitszwecken stattfindende Übermittlung verschlüsselter Hash-Werte der Nutzerkennworte. Ich habe insoweit verbleibende datenschutzrechtliche Bedenken vorerst zurückgestellt, mir aber vorbehalten, hierauf zu einem späteren Zeitpunkt noch einmal zurückzukommen. Weiter erteilte ich in einigen Fällen Hinweise zur rechtskonformen Ausgestaltung von Cookie-Bannern. Schließlich wies ich mehrere Verantwortliche darauf hin, dass personenbezogene Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung von Nutzerverhalten auf Webseiten oder in Apps verarbeitet werden, nicht auf Grundlage einer Einwilligung nach Art. 49 Abs. 1 Satz 1 Buchstabe a DS-GVO in ein Drittland übermittelt werden dürfen, weil Umfang und Regelmäßigkeit solcher Transfers dem Charakter des Art. 49 DS-GVO als Ausnahmevorschrift widersprechen.[3] Ein Abschluss der verbliebenen letzten Fälle soll im Frühjahr 2023 erfolgen.

Auswirkungen von US-Recht auf europäische Tochterunternehmen von US-Cloud-Anbietern

externes DSK-Gutachten (Kurzlink): https://t1p.de/Vladeck

Im Jahr 2022 hat Wirtschaft und Aufsichtsbehörden unter anderem das Thema „Extraterritoriale Anwendbarkeit von US-Recht" beschäftigt. Anfang des Jahres hatten die Aufsichtsbehörden ein externes Gutachten zur Reichweite der Zugriffsrechte von US-amerikanischen Sicherheitsbehörden veröffentlicht. Danach greift das US-Recht in Bezug auf bestimmte Auslandsaufklärungsprogramme nicht nur ein, wenn Daten in den USA verarbeitet werden, sondern grundsätzlich auch dann, wenn US-Unternehmen oder ihre Tochtergesellschaften Daten außerhalb der USA verarbeiten – etwa in Europa. Das US-Recht ist insoweit extraterritorial anwendbar.

3 Siehe hierzu DSK-Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1 vom Dezember 2022, Rn. 112.

Vergabekammer BW v. 13.07.2022 (Az. 1 VK 23/22)

Im Juli 2022 entschied die Vergabekammer Baden-Württemberg, dass Hosting-Dienste eines europäischen Cloud-Anbieters mit US-amerikanischer Konzernmutter in öffentlichen Vergabeverfahren nicht in Anspruch genommen werden dürfen. Eine berücksichtigungsfähige Offenlegung sei auch dann anzunehmen, wenn eine Einstellung personenbezogener Daten auf eine Plattform erfolge, auf die von einem Drittland aus zugegriffen werden könne, und zwar unabhängig davon, ob der Zugriff tatsächlich erfolge. Dabei sei unerheblich, ob der Server, über den die Daten zugänglich gemacht werden, innerhalb der EU gelegen sei. Eine Zugriffsmöglichkeit – etwa durch Einräumung von Zugriffsrechten – konstituiere ein latentes Risiko, dass eine unzulässige Übermittlung personenbezogener Daten stattfinden könne, ohne dass hierfür die in der DS-GVO normierten rechtlichen Grundlagen gegeben seien. Die Übernahme einer Verpflichtung durch das europäische Tochterunternehmen, zu weit gehende oder unangemessene Anfragen staatlicher Stellen einschließlich solcher Anfragen, die im Widerspruch zum Recht der EU oder zum geltenden Recht der Mitgliedsstaaten stehen, anzufechten, beseitige das latente Risiko eines Zugriffs durch eben diese Stellen nicht.

OVG Karlsruhe v. 07.09.22 (Az. 15 Verg 8/22)

Das OLG Karlsruhe gab mit Beschluss vom September 2022 der Beschwerde statt und hob die Entscheidung unter Zurückweisung des Nachprüfungsantrags auf. Das Gericht lehnte die pauschale Annahme einer latenten Gefahr ab und führte aus, dass der Auftraggeber gerade nicht davon ausgehen müsse, dass es aufgrund der Konzernbindung zu rechts- und vertragswidrigen Weisungen an das Tochterunternehmen kommen bzw. das europäische Tochterunternehmen durch seine Geschäftsführer gesetzeswidrigen Anweisungen der US-amerikanischen Muttergesellschaft Folge leisten werde.

In der zweiten Jahreshälfte 2022 befasste sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) mit Fragen extraterritorialer Zugriffsmöglichkeiten durch öffentliche Stellen und den Auswirkungen auf in der Euro-

päischen Union angesiedelte Anbieter. Die DSK beauftragte in der 3. Zwischenkonferenz 2022 zwei Arbeitskreise, hierzu eine Beschlussvorlage zu erarbeiten. In der eingerichteten Unterarbeitsgruppe arbeitet meine Behörde mit. Zum Ende des Berichtszeitraums dauerten diese Arbeiten an.

Entwurf für einen neuen Angemessenheitsbeschluss USA

Executive Order 14086

Am 13. Dezember 2022 hat die Europäische Kommission ihren Entwurf für den neuen Angemessenheitsbeschluss für die USA veröffentlicht. Grundlage für diesen Entwurf ist das Ergebnis monatelanger Verhandlungen mit der US-Seite, in deren Folge US-Präsident Biden am 7. Oktober 2022 eine Anordnung für die Verbesserung von (Sicherheits-)Garantien für US-nachrichtendienstliche Aktivitäten „EO 14086" erlassen hat. Diese Anordnung zielt vor allem darauf ab, den Rechtsschutz für EU-Bürgerinnen und -Bürger gegen US-Überwachungsmaßnahmen zu verbessern.

Zweistufiges Beschwerdeverfahren

In der EO 14086 werden die legitimen Ziele der Fernmeldeaufklärung katalogmäßig aufgeführt sowie unzulässige Zwecke festgelegt. Die US-Dienste sollen bei ihrer Arbeit den übergreifenden Prinzipien der Erforderlichkeit und Verhältnismäßigkeit unterworfen werden. Es wird ein Vorrang der gezielten (Daten-)Sammlung vor der massenhafte (Daten-)Sammlung bei der Fernmeldeaufklärung festgelegt. Neu eingeführt wird ein zweistufiges Beschwerdeverfahren für EU-Bürgerinnen und -Bürger gegen US-Überwachungsmaßnahmen. Auf der ersten Stufe soll ein Beauftragter für bürgerliche Freiheiten und Datenschutz über Beschwerden entscheiden. Auf zweiter Stufe können der Beschwerdeführer oder eine Stelle der Nachrichtendienste beantragen, dass die Entscheidung des Beauftragten durch ein „Datenschutzkontrollgericht" überprüft wird. Dieses administrative Tribunal soll nach dem Willen der Präsidentenanordnung unabhängig sein. Der Generalstaatsanwalt darf nicht in die Überprüfung einer qualifizierten Beschwerde eingreifen und grundsätzlich keinen Richter entlassen. Sowohl die Entscheidungen des Beauftragten als auch des Datenschutzkontrollgerichts sollen für die Nachrichtendienste verbindlich sein, auch wenn in der EO 14086 nicht geregelt wird, ob und wie Beauftragter oder Gericht die Entscheidungen durchsetzen können.

Die Europäische Kommission ist der Auffassung, dass der Zugang der US-Nachrichtendienste zu europäischen Daten durch die neuen Regelungen der EO 14086 auf das zum Schutz der nationalen Sicherheit der USA notwendige und verhältnismäßige Maß beschränkt werden wird.

Die Daten von EU-Bürgern dürften nur nach der Feststellung erhoben werden, dass die Erhebung auf der Grundlage einer angemessenen Beurteilung aller relevanten Faktoren erfolgt und notwendig sei, um eine bestimmte nachrichtendienstliche Aufgabe zu erfüllen. Bei dieser Prüfung müsse die Verfügbarkeit anderer Quellen geprüft werden. Wenn möglich, solle vorrangig auf diese Quellen zurückgegriffen werden. Sei das nicht möglich, müsse die Überwachung so „maßgeschneidert wie möglich" sein und dürfe nicht die Privatsphäre und die bürgerlichen Freiheiten der EU-Bürgerinnen und -Bürger unverhältnismäßig beeinträchtigen.

Das Thema des Rechtsschutzes für EU-Bürger gegen Überwachungsmaßnahmen von US-Behörden sieht die Europäische Kommission grundsätzlich als gelöst an, da sie das neu einzurichtende Datenschutzkontrollgericht als ein unabhängiges Tribunal betrachtet. Die Unabhängigkeit des Urteilsverfahrens werde durch eine Reihe von Garantien sichergestellt. Insbesondere sei es der Exekutive untersagt, sich in die Prüfung des Gerichts einzumischen oder diese unzulässig zu beeinflussen. Das Gericht sei verpflichtet, die Fälle unparteiisch zu beurteilen und arbeite nach seiner eigenen Geschäftsordnung. US-Strafverfolgungsbehörden und Sicherheitsbehörden unterlägen einem Rechtsrahmen, der sicherstelle, dass der Zugriff und die weitere Verwendung der Daten auf das Wesentliche beschränkt sei. EU-Bürger verfügten über wirksame Rechtsbehelfe gegen US-Überwachungsmaßnahmen.

Die Europäische Kommission gelangt daher im Entwurf des Angemessenheitsbeschlusses der Kommission zu dem Ergebnis, dass die USA für die Zwecke von Art. 45 DS-GVO ein angemessenes Schutzniveau für personenbezogene Daten, die aus der EU an Datenimporteure in den Vereinigten Staaten übermittelt werden, gewährleisten. Voraussetzung ist, dass die US-Organisationen in der öffentlich verfügbaren „Data Privacy Framework List" enthalten sind, wobei es sich grundsätzlich um eine Fortschreibung der früheren Privacy-Shield-Zertifizierung handelt.[4]

Ob das zweistufige Beschwerdeverfahren einen wirksamen Rechtsbehelf darstellt, bleibt indes abzuwarten. Schließlich dürfen weder Beauftragter noch Gericht dem Beschwerdeführer mitteilen, ob Verstöße festgestellt und ob Abhilfemaßnahmen erlassen wurden, solange die Akten noch als Verschlusssache eingestuft sind. Das dürfte dazu führen, dass Beschwerdeführer in aller Regel ihre Beschwerde vorsorglich auch dem Datenschutzkontrollgericht vorlegen.

Ungeachtet dessen bin ich der Meinung, dass das Datenschutzkontrollgericht über eine größere Unabhängigkeit verfügt und nochmal eine erhebliche Verbesserung zum bisherigen Ombudsmann-Mechanismus unter dem Privacy Shield darstellt. Die USA haben sich deutlich auf die EU zubewegt und spürbare Zugeständnisse gemacht. Ob diese Verbesserungen allerdings ausreichend sind, um ein angemessenes Schutzniveau bejahen zu können, bleibt der gründlichen Prüfung durch den Europäischen Datenschutzausschuss vorbehalten, deren Ergebnis im Frühjahr 2023 vorgelegt werden soll.

4 Zum früheren Privacy Shield siehe Tätigkeitsbericht 2017–2018, S. 159.

E. Datenschutzkonfenrenz

E.1. Bericht aus dem Arbeitskreis Beschäftigtendatenschutz

In der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) führe ich den Vorsitz des Arbeitskreises (AK) Beschäftigtendatenschutz.

Entschließung der DSK: https://t1p.de/Forder-BeschDG

Aufgabe des AK Beschäftigtendatenschutz ist es insbesondere, einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten und hierzu Entscheidungen der DSK vorzubereiten.

Rückblick

Diesem Auftrag entsprechend, bereitete der AK im Jahr 2022 – als ein Schwerpunkt – die Entschließung der DSK „Die Zeit für ein Beschäftigtendatenschutz ist ‚Jetzt'!" vom 29. April 2022 vor. Gegenstand dieser Entschließung ist der seit Jahren bestehende Reformbedarf im Beschäftigtendatenschutz. Bei der Erarbeitung des Entschließungsentwurfs berücksichtigte der AK unter anderem den im Januar 2022 veröffentlichten Abschlussbericht des vom Bundesministeriums für Arbeit und Soziales (BAMS) einberufenen interdisziplinären Beirats „Beschäftigtendatenschutz".

siehe auch Abschnitt E.3., S.39

Abschlussbericht des Beirats „Beschäftigtendatenschutz" auf der Website des BAMS: https://t1p.de/Ergebnisse-Beirat

Mindestens einmal jährlich finden Sitzungen des AK statt, so auch im Januar 2022. Diese Sitzungen dienen insbesondere dem Erfahrungsaustausch zu besonderen Fallkonstellationen. Auch dieses Jahr bildeten Fälle im Zusammenhang mit der Corona-Pandemie den Schwerpunkt der Beratungen. Besonders bedeutsam war die Bearbeitung von Fragen zur einrichtungsbezogenen Impf-

Beschluss der DSK: https://t1p.de/DSK_Impfpflicht

pflicht und zur Dokumentation des Impfnachweises. Weiter stand die Klärung sonstiger Rechtsfragen zur Umsetzung der Datenschutz-Grundverordnung (DS-GVO) auf der Agenda. Diesbezüglich berichtete ich beispielsweise zum (umfassenden) Auskunftsrecht im Beschäftigtenkontext unter Berücksichtigung der zwischenzeitlich erfolgten Rechtsprechung.

Zudem wurde außerhalb der Sitzung im Zusammenhang mit der Pandemie der Entwurf eines Beschlusses zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht für die DSK erarbeitet. Der entsprechende Beschluss der DSK wurde am 13. April 2022 gefasst.

Die im AK Beschäftigtendatenschutz gebildeten Unterarbeitskreise haben sich im weiteren Verlauf des Jahres mit der Anpassung von bestehenden Veröffentlichungen der DSK, unter anderem zu den Themen „Internet und E-Mail am Arbeitsplatz“ und „Konzerninterner Datenschutz“, sowie mit der Erstellung einer neuen Publikation „Personalgewinnung/Bewerbungsverfahren/Pre-employment checks“ (Arbeitstitel) befasst. Die Abschlussarbeiten hierzu stehen noch aus.

Ausblick

Siehe auch Abschnitt E.12., S.55

Im Jahr 2023 wird sich der AK Beschäftigtendatenschutz unter anderem mit den oben genannten Veröffentlichungen befassen. Schwerpunktthemen für das Jahr 2023 werden zudem auf der 10. Sitzung des AK Beschäftigtendatenschutz Mitte Januar 2023 festgelegt werden.

E.2. Bericht aus dem Arbeitskreis Versicherungswirtschaft

Auch in diesem Berichtszeitraum hatte ich den Vorsitz des Arbeitskreises (AK) Versicherungswirtschaft inne. Die teilnehmenden Aufsichtsbehörden beraten in dem AK über Fragen, die sich bei der datenschutzrechtlichen Aufsicht über Versicherungsunternehmen stellen. Ziel dieser Beratungen ist es, eine einheitliche Aufsichtspraxis in Deutschland zu gewährleisten.

Hinweis- und Informationssystem

Der Gesamtverband der Deutschen Versicherungswirtschaft und der AK sind in einen intensiveren Austausch zum sogenannten Hinweis- und Informationssystem eingetreten. Das Hinweis- und Informationssystem der Versicherungswirtschaft dient der Erkennung und Prävention von Versicherungsbetrug. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten in diesem Zusammenhang kommt nur Art. 6 Abs. 1 lit. f DS-GVO, also eine Interessenabwägung in Betracht. Solche Interessenabwägungen sind immer Einzelfallentscheidungen und daher besteht für Verantwortliche eine gewisse Rechtsunsicherheit, ob ihre eigenen Wertungen auch von der Datenschutzaufsicht geteilt werden. In Fällen wie dem Hinweis- und Informationssystem, in denen bundesweit für viele Unternehmen erhebliche Aufwände bei der Implementierung neuer Verfahren entstehen, die eine erhebliche technische Komplexität aufweisen und erhebliche Auswirkungen auf betroffene Personen haben können, ist es sowohl für die Unternehmen als auch die Aufsichtsbehörden sehr sinnvoll, frühzeitig Informationen und Einschätzungen auszutauschen.

Rechtsgrundlage für die Verarbeitung bei Leistungsanträgen in der Kranken- und Lebensversicherung

Diskutiert wird im AK zudem die Frage, auf welcher Grundlage Versicherungen besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, bei einem Leistungsantrag durch eine betroffene Person verarbeiten können. In Betracht kommen hier vor allem Art. 9 Abs. 2 lit. f DS-GVO oder Art. 9 Abs. 2 lit. a DS-GVO.

Nach Art. 9 Abs. 2 lit. f DS-GVO dürfen besondere Kategorien personenbezogener Daten verarbeitet werden, wenn dies erforderlich ist, um einen Rechtsanspruch geltend zu machen oder abzuwehren. Wenn es darum geht,

Leistungsansprüche geltend zu machen, sind die Voraussetzungen allein nach dem Wortlaut der DS-GVO gegeben. Es wird jedoch kontrovers diskutiert, ob darüber eine einschränkende Auslegung der DS-GVO geboten ist. So wird teilweise gefordert, es müsse ein rechtlicher Konflikt vorliegen, um Art. 9 Abs. 2 lit. f DS-GVO zur Anwendung kommen zu lassen. Zweck des Art. 9 Abs. 2 lit. f DS-GVO sei es nämlich, die gerichtliche Geltendmachung von Ansprüchen zu erlauben. Daher reiche es nicht aus, wenn eine solche gerichtliche Geltendmachung lediglich möglich sei. Zudem bestünde bei einer weiter gefassten Auslegung die Gefahr, dass letztlich jede Verarbeitung für Vertragszwecke nach Art. 9 Abs. 2 lit. f DS-GVO gerechtfertigt wäre. Nach dieser Auffassung wäre es dann für die Verarbeitung personenbezogener Daten in der Leistungsprüfung aber notwendig, eine Einwilligung einzuholen oder eine gesetzliche Grundlage zu schaffen.

Nach der Gegenauffassung, die auch ich vertrete, rechtfertigt Art. 9 Abs. 2 lit. f DS-GVO die Verarbeitung besonderer Kategorien personenbezogener Daten für die Leistungsprüfung. Die einschränkende Auslegung ist mit dem Wortlaut der DS-GVO nicht vereinbar. Ein rechtlicher Konflikt als zusätzliches Tatbestandsmerkmal ist weder der DS-GVO selbst noch den Erwägungsgründen zu entnehmen. Darüber hinaus darf der Zweck der Norm nicht zu eng verstanden werden. Bei der Geltendmachung oder Abwehr von Ansprüchen werden regelmäßig personenbezogene Daten verarbeitet. Der Verordnungsgeber war sich offenbar der Gefahr bewusst, dass dies durch das Datenschutzrecht erheblich erschwert werden könnte und hat in mehreren Vorschriften Regelungen aufgenommen, um dieses Spannungsverhältnis vom Datenschutzrecht zur übrigen Rechtsordnung zugunsten der Ausübung von Ansprüchen aufzulösen. Die Beratungen hierzu konnte der Arbeitskreis im Berichtszeitraum jedoch noch nicht abschließen.

E.3. Datenschutzkonferenz fordert ein Beschäftigtendatenschutzgesetz

Die Datenschutzkonferenz (DSK) hat mit der Entschließung „Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"!" erneut auf den seit Jahren bestehenden Reformbedarf im Beschäftigtendatenschutz hingewiesen. Die Konferenz macht damit deutlich, in welchen Bereichen weitergehende gesetzliche Regelungen überfällig sind.

Entschließung der DSK: https://t1p.de/Forder-BeschDG

Worum geht es?

Das europäische Recht ermöglicht nach Artikel 88 der Datenschutz-Grundverordnung (DS-GVO) den Mitgliedstaaten, spezifischere Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen. Der Bundesgesetzgeber hat von dieser Öffnungsklausel mit § 26 BDSG Gebrauch gemacht. Die Entschließung verdeutlicht, dass § 26 BDSG aus Sicht der Aufsichtsbehörden nicht hinreichend praktikabel, normenklar und sachgerecht ist. Die Norm ist als Generalklausel formuliert und eröffnet allen Beteiligten weite Interpretationsspielräume. Dadurch führt sie zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber.

Der Arbeitskreis (AK) Beschäftigtendatenschutz der DSK, bei dem meine Behörde den Vorsitz führt, hat die oben genannte Entschließung der DSK vorbereitet. Beispielhaft wurden für die Entschließung sieben Schwerpunkte herausgearbeitet, für die Regelungsbedarf gesehen wird. Hierzu zählen:

- Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI),
- Grenzen der Verhaltens- und Leistungskontrolle,
- Ergänzungen zu den Rahmenbedingungen der Einwilligung,
- Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen,
- Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Artikel 6 und 9 DS-GVO,
- Beweisverwertungsverbote sowie der Bereich
- Datenverarbeitung bei Bewerbungs- und Auswahlverfahren.

Für die Erstellung der Entschließung betrachtete der AK unter anderem die Aussagen des im Januar 2022 veröffentlichten Abschlussberichts des vom Bundesministerium für Arbeit und Soziales (BAMS) einberufenen interdisziplinären Beirats „Beschäftigtendatenschutz“.[1]

Wie geht es weiter?

Das weitere Gesetzgebungsverfahren auf Bundesebene für das im Koalitionsvertrag der Bundesregierung avisierte Beschäftigtendatenschutzgesetz bleibt abzuwarten.[2]

Darüber hinaus ist auch der Landesgesetzgeber gefordert, im Beschäftigtenkontext bestehende landesrechtliche Regelungen im Hinblick auf die in der Entschließung genannten Bereiche zu überprüfen und Anpassungsbedarfe zu ermitteln.

1 Abschlussbericht Beirat: https://t1p.de/Ergebnisse-Beirat
2 Siehe auch Bundestags-Drucksache 20/2506, Antwort der Bundesregierung vom 1. Juli 2022 zu Frage 50

E.4. Entschließungen der DSK zur Nutzung von personenbezogenen Daten zu Forschungszwecken

Ein Themenschwerpunkt der Datenschutzkonferenz (DSK) im Jahr 2022 lag im Forschungsbereich. Die DSK hat hierzu zwei Entschließungen herausgegeben und damit den forschenden Einrichtungen wichtige Hinweise zu den datenschutzrechtlichen Rahmenbedingungen gegeben. Zugleich wurde deutlich gemacht, dass wissenschaftliche Forschung und Datenschutz in keinem Widerspruch zueinanderstehen.

Wissenschaftliche Forschung – selbstverständlich mit Datenschutz

Mit ihrer Entschließung „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" vom 23.03.2022 hat die DSK unterstrichen, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind. So wird die wissenschaftliche Forschung durch die DS-GVO an mehreren Stellen privilegiert. Dies entspricht dem politischen Ziel der Förderung des wissenschaftlichen Fortschritts durch Schaffung eines europäischen Forschungsraumes. Zugleich zielt die DS-GVO auf einen Ausgleich zwischen der Forschungsfreiheit und dem Recht des Einzelnen auf Wahrung seines Grundrechts auf Datenschutz.

Kurzlink zur Entschließung: https://t1p.de/DSKEntschliessungForschung

Die Überlegungen der Bundesregierung, ein allgemeines Forschungsdatengesetz zu schaffen, werden ausdrücklich begrüßt. Dieses muss aber durch bereichsspezifische Regelungen ergänzt werden, um dem Gebot der Normenklarheit Rechnung zu tragen.

Bereits im Jahr 2004 forderte die DSK den Gesetzgeber mit einer Entschließung auf, sicherzustellen, dass die geschützten medizinischen Daten auch nach ihrer Übermittlung an die forschenden Einrichtungen strafrechtlich vor Offenbarung und Beschlagnahme geschützt sind. Da die erforderlichen Änderungen des Strafgesetzbuches und der Strafprozessordnung nicht umgesetzt wurden, wird diese Forderung weiter aufrechterhalten.

Kurzlink zur Entschließung: https://t1p.de/DSKEntschliessungForschungsgeheimnis

Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten

Nicht zuletzt durch die Corona-Pandemie wurde die hohe gesamtgesellschaftliche Bedeutung der wissenschaftlichen Forschung mit Gesundheitsdaten deutlich. Der oftmals geäußerte Einwand, dass datenschutzrechtliche Normen der Nutzung von Gesundheitsdaten zu Forschungszwecken entgegenstehen, trifft nicht zu.

Petersberger Erklärung (Kurzlink): https://t1p.de/PetersbergerErklaerung

Dementsprechend hat sich die DSK im November 2022 mit ihrer „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung" für eine bestmögliche Förderung der wissenschaftlichen Forschung ausgesprochen. Die Gesundheitsdaten unterliegen laut DS-GVO allerdings einem hohen Schutzbedarf, da ihre unsachgemäße Verwendung zu gravierenden Folgen für die betroffenen Personen führen kann. Daher müssen die Verarbeitungsprozesse rechtmäßig und für die betroffene Person stets transparent und nachvollziehbar sein. Grundlegende Garantien und Maßnahmen zum Schutz der Daten der betroffenen Personen, wie beispielsweise Verschlüsselung, Pseudonymisierung durch eine Vertrauensstelle und frühestmögliche Anonymisierung müssen gewährleistet sein.

Eine wichtige Rolle kommt in diesem Kontext den unabhängigen Datenschutzaufsichtsbehörden zu. Diese müssen die Möglichkeit haben, die Einhaltung der datenschutzrechtlichen Anforderungen umfassend und effektiv zu überwachen und durchzusetzen. Dies bedingt, dass sie auch gegenüber öffentlichen Stellen den sofortigen Vollzug von Maßnahmen anordnen können. Meine Forderung an die niedersächsische Landesregierung zur Schaffung einer gesetzlichen Regelung zur Vollstreckung von Maßnahmen gegenüber öffentlichen Stellen wurde bislang leider nicht umgesetzt. Ich werde allerdings weiterhin hierauf beharren.

E.5. Akkreditierung und Zertifizierung: DSK verabschiedet Kriterienkatalog

Im Umlaufverfahren verabschiedete die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) am 13. Juli 2022 die „Anforderungen an Zertifizierungsprogramme", Version 2.0.

Die Anwendungshinweise „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 2.0" wurde um Art. 26 DS-GVO „Gemeinsam Verantwortliche" und Art. 44 ff. DS-GVO zur „Übermittlung personenbezogener Daten an Drittländer" sowie um Grafiken zum Ablauf der Verfahren (nationales und europäisches Siegel) ergänzt.

Anwednungshinweise der DSK (Kurzlink): https://t1p.de/DSKZertifizierung

Die Anwendungshinweise dienen als gemeinsame Grundlage für alle deutschen Aufsichtsbehörden, um eine einheitliche Bewertung von Zertifizierungskriterien im Sinne des Art. 42 Abs. 5 DS-GVO in Deutschland zu erreichen. Zum anderen hilft das Dokument den Programmeignern und den Zertifizierungsstellen bei der Erstellung ihrer Dokumente (insbesondere im Rahmen einer Programmprüfung) als Orientierung.

Die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme" umfassen konkrete Prüfkriterien insbesondere zu den Verarbeitungsgrundsätzen, der Rechtsmäßigkeit, zum technisch-organisatorischen Datenschutz und der Auftragsverarbeitung (Art. 5, 6, 25, 26, 28, 30, 32, 33, 34, 35, 44 ff.). Dabei wurde zu den einzelnen Artikeln der DS-GVO sehr detailliert ausgeführt, was genau die Zertifizierungsstelle mit welchen Prüfmethoden zu prüfen hat. Dieser Detaillierungsgrad wurde nun in der aktuellen Version auch für die Regelungen zu Gemeinsam Verantwortlichen und der Datenübermittlung auf Basis geeigneter Garantien (Artikel 26 und 44 ff.) fortgeschrieben.

Der fortgeschriebene Kriterienkatalog wird bereits in ersten Verfahren zu Akkreditierungen und Zertifizierungen verwendet. Begleitend findet ein Erfahrungsaustausch der Aufsichtsbehörden in dem Arbeitskreis (AK) Zertifizierung und dem zugeordneten Unterarbeitskreis Prüfkriterien statt.

Ich freue mich darüber, einen weiteren, wichtigen Fortschritt für die Akkreditierungs- und Zertifizierungspraxis und für den Datenschutz in Deutschland und Europa erreicht zu haben.

E.6. Update für das Standard-Datenschutzmodell

Am 24.11.2022 stimmte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) der aktuellen Version 3.0 des Standard-Datenschutzmodells (SDM) zu. Es wurden die Bedeutung von „Verarbeitung" und den damit verbunden „Risiken" herausgearbeitet.

SDM 3.0 (Kurzlink): https://t1p.de/SDM3

Mit dem SDM stellt die DSK eine Methode zur systematischen Herleitung von technischen und organisatorischen Maßnahmen (TOM) bei der Verarbeitung personenbezogener Daten aus den rechtlichen Vorgaben der DS-GVO zur Verfügung. Das SDM wird gemeinschaftlich von den deutschen Datenschutzaufsichtsbehörden weiterentwickelt und liegt jetzt in einer überarbeiteten Fassung vor. In der Vergangenheit habe ich immer wieder die aktuellen Entwicklungen in meinen Tätigkeitsberichten dargestellt.

In der aktuellen Fassung des SDM wurde der neue Abschnitt D 2.1 „Aufbereitung einer Verarbeitungstätigkeit in Vorgänge oder in Phasen eines Datenlebenszyklus" aufgenommen. Ausgangspunkt ist dabei die Begriffsbestimmung des Artikels 4 Abs. 2 der DS-GVO zur „Verarbeitung", die aus bis zu 14 „elementaren Verarbeitungsschritten" bestehen kann. Diese elementaren Verarbeitungsschritte werden nun in neun Gruppen von Verarbeitungsvorgängen unterteilt, die zum besseren Verständnis wiederum in vier „Phasen der Datenverarbeitung" gegliedert sind. Die Zuordnung der elementaren Verarbeitungsvorgänge zu Gruppen oder Phasen erfolgt auf Basis datenschutzrechtlicher Anforderungen, die erfahrungsgemäß ähnlich sind.

Mit dem Abschnitt D 2.5 wird ein „Überblick über die Modellierungstechniken des SDM (‚SDM-Würfel')"eingeführt. Dazu werden die rechtlichen Anforderungen der DS-GVO in sieben Gewährleistungsziele „übersetzt", die es dem Verantwortlichen ermöglichen sollen, eine DS-GVO-konforme Verarbeitung personenbezogener Daten (pb Daten) zu gewährleisten.

Die sieben Gewährleistungsziele des SDM sind:

- Datenminimierung (übergreifende Anforderung),
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz und
- Intervenierbarkeit.

Auf dieser Basis können die Risiken analysiert und angemessene technische und organisatorische Maßnahmen ausgewählt werden, die das Risiko der Verarbeitung so gering wie möglich halten. Der „SDM Würfel" unterstützt so den Anwender dabei, die Risiken auch in technisch komplexen Verarbeitungssituationen vollständig erfassen, analysieren und bewerten zu können.

E.7. Umsetzung der Registermodernisierung

In meinem letzten Tätigkeitsbericht habe ich die Einbindung meiner Behörde (vertretend für die Datenschutzkonferenz, kurz DSK) in das Projekt „Gesamtsteuerung Registermodernisierung" dargestellt (siehe Tätigkeitsbericht 2021, Kap. G.8, ab S. 72). Im Jahr 2022 hat sich die Arbeit und der Austausch mit den Projektgremien intensiviert.

Wesentlich für die Umsetzung der Registermodernisierung sind insbesondere die folgenden Aspekte:

- Umfassende Transparenz für die Bürgerinnen und Bürger,
- Möglichkeit für die Bürgerinnen und Bürger, ihren Willen zu der Verarbeitung ihrer personenbezogenen Daten zu äußern und bedingungslose Beachtung dieses Willens,
- Einrichtung technischer Hürden, die eine rechtswidrige Datenverarbeitung verhindern.

Die Mitarbeiterinnen und Mitarbeiter meiner Behörde wirken, vertretend für die DSK und in enger Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auf die Einhaltung dieser Aspekte in Projektgremien hin:

- Im Rahmen der Ausarbeitung des Entwurfs einer gesetzlichen Regelung zur Umsetzung des Once-Only-Prinzips (siehe auch Tätigkeitsbericht 2021, G.8., ab Seite 72.), wurde eine sogenannte Vorschaufunktion als notwendig hervorgehoben. Denn während der Antragstellende bei einem analogen Verwaltungsverfahren sämtliche einzureichenden Dokumente physisch in der Hand hat, soll bei einem digitalen Verfahren die Möglichkeit bestehen, bestimmte für das Verfahren erforderlichen Nachweise (wie z. B. eine Geburtsurkunde) bei anderen Behörden abrufen zu lassen. Bevor die nachweisabrufende Behörde den Nachweis von der nachweisübermittelnden Stelle erhält und für das Verfahren verwendet, ist es dabei wichtig, dass der Antragstellende die Möglichkeit bekommt, den Inhalt dieses Nachweises einzusehen.
- Da das Once-Only-Prinzip nicht nur in den Grenzen der Bundesrepublik, sondern EU-weit gelten soll, wurde eine entsprechende Regelung für Nachweisabrufe ausgearbeitet. Auch diese Abrufe sind nur aufgrund einer entsprechenden Willensäußerung des Antragstellenden und unter Einbindung der Vorschaufunktion möglich. Diese Klarstellung hat in der Gesetzesbegründung des aktuellen Entwurfs Niederschlag gefunden und sorgt für einfachere und klare Rechtsanwendung.
- Bei allem Verständnis für die Notwendigkeit, bestimmte Funktionen der modernisierten Register schnell zu pilotieren, wurde mehrfach betont, dass die datenschutzrechtlichen Grundsätze auch für Pilotprojekte gelten. Sobald im Rahmen dieser Projekte personenbezogene Daten verarbeitet werden sollen, bedarf es hierzu einer Rechtsgrundlage. Soll z. B. die Einspeicherung der zentralen Personenkennziffer (ID-Nummer) in ein zu modernisierendes Register pilotiert werden, darf dies erst geschehen, wenn die Rechtsgrundlage für diese Verarbeitung in Kraft getreten ist.

E.8. Deutsche Verwaltungscloud-Strategie

Der Staat erhebt, speichert und verarbeitet unzählige Daten von Bürgerinnen und Bürgern. Er tut dies auf Basis der jeweils einschlägigen Rechtsgrundlagen, hat dabei die Grundsätze der Rechtsstaatlichkeit einzuhalten und bildet so einen Vertrauensanker für die Betroffenen. Um diesen Anspruch erfüllen zu können, darf sich die Verwaltung bei der Digitalisierung nicht von einzelnen Technologieanbietern abhängig machen. Gerade die in den Markt drängenden Cloud-Architekturen müssen besonders genau geprüft werden, da diese hochintegrierten und oft proprietären Angebote häufig intransparent sind.

In einem Rechtsstaat, auch in einem digitalen Rechtsstaat, hält sich die Exekutive an Gesetz und Recht (Art. 20 Abs. 3 GG). Dazu gehört auch Datenschutzrecht. Es muss möglich sein, dass Bürger staatliche Leistungen in Anspruch nehmen oder mit dem Staat kommunizieren können und dabei darauf vertrauen können, dass ihre personenbezogenen Daten beim Staat sicher sind und in datenschutzkonform verarbeitet werden.

Der Staat kann sich nur dann an Recht und Gesetz halten, wenn ihn niemand daran hindert, dies zu tun. Um über sein Handeln zu bestimmen, muss der Staat, auch nach der Digitalisierung von Dienstleistungen, souverän bleiben.

Transparenz und tatsächliche Steuerungsmöglichkeiten der eingesetzten IT-Verfahren sind wesentliche Merkmale einer digital souveränen Lösung.

Dabei muss es dem Staat sowohl möglich sein, bei Nutzung der digitalen Lösungen Datenschutzrecht einzuhalten, als auch sich von diesen Lösungen wieder zu verabschieden, wenn damit Datenschutzgrundsätze nicht eingehalten werden können.

Mit der Arbeitsgruppe (AG) „Cloud Computing und Digitale Souveränität" des IT-Planungsrats unter Federführung Nordrhein-Westfalens und des Bundes (vertreten durch das Bundesministerium des Innern) wurde ein grundlegender Rahmen zur der Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Deutschland geschaffen.[1] Beraten wird die AG durch die kommunalen Spitzenverbände und die Datenschutzkonferenz.

An dieser AG beteiligt sich auch meine Behörde, mandatiert durch die Datenschutzkonferenz. In der Unterstruktur dieser Arbeitsgruppe finden Arbeiten an der Fortschreibung und Konkretisierung der Deutschen Verwaltungscloud-Strategie (DVS) statt.

Das Ziel der DVS ist es, gemeinsame Standards und offene Schnittstellen für Cloud-Lösungen der öffentlichen Verwaltung zu schaffen, um übergreifend eine interoperable sowie modulare föderale Cloud-Infrastruktur zu etablieren.[2] Dabei sollen Abhängigkeiten der öffentlichen Verwaltung reduziert oder beseitigt werden. So werden Transparenz und Wechselmöglichkeiten erhalten und unerwünschte Lock-in Effekte vermieden. Nach meiner Überzeugung bleibt nur so die öffentliche Verwaltung langfristig Herrin über die ihr anvertrauten personenbezogenen Daten und kann den Bürgerinnen und Bürgern die Einhaltung des Datenschutzes garantieren.

1 Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, Version 1.0, Januar 2021: Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf (it-planungsrat.de); letzter Abruf: 19.1.2023

2 CIO Bund - Deutsche Verwaltungscloud-Strategie; letzter Abruf: 19.1.2023.

E.9. Konsultationsverfahren zur Orientierungshilfe für Anbieter von Telemedien 2021

Am 21.12.2021 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine neue Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien (OH Telemedien 2021) veröffentlicht. Gleichzeitig wurde beschlossen, zu dieser OH, die sowohl für öffentliche als auch nicht-öffentliche Stellen für den Betrieb einer Webseite relevant ist, ein öffentliches Konsultationsverfahren durchzuführen. Vertreterinnen und Vertreter aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung erhielten die Gelegenheit bis 15. März 2022 eine Stellungnahme zu der OH Telemedien 2021 abzugeben. Das Konsultationsverfahren wurde Anfang Dezember 2022 durch die Veröffentlichung der angepassten OH Telemedien 2021 Version 1.1 sowie des Auswertungsberichts des AK Medien zum Konsultationsverfahren abgeschlossen.

OH Telemedien (Kurzlink): https://t1p.de/OHTelemedien

Die OH Telemedien 2021 bietet Betreiberinnen und Betreibern von Webseiten, Apps oder Smarthome-Anwendungen konkrete Hilfestellungen bei der Umsetzung des seit dem 01.12.2021 geltenden Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) – insbesondere von § 25 TTDSG. Zudem vermittelt die Orientierungshilfe betroffenen Bürgerinnen und Bürgern ein umfassendes Bild der rechtlichen Rahmenbedingungen.

Auf europäischer Ebene führt der Europäische Datenschutzausschuss zu veröffentlichten Leitlinien („Guidelines") regelmäßig ein öffentliches Konsultationsverfahren durch. Nach diesem Vorbild hatte die DSK Ende 2021 beschlossen, ein entsprechendes Verfahren zur neuen OH Telemedien 2021 durchzuführen. Ziel war es, die Orientierungshilfe zu überprüfen und gegebenenfalls praxisorientiert weiterzuentwickeln. Die Geltung und Anwendung der OH Telemedien 2021 wurde von dem Konsultationsverfahren nicht berührt.

Insgesamt sind 14 Stellungnahmen, überwiegend von Interessenverbänden aus dem Bereich der digitalen Wirtschaft und Werbung sowie der Medien eingereicht worden. Es wurde eine umfassende Auswertung aller in den Stellungnahmen geäußerten Aspekte vorgenommen. Da nicht alle Hinweise aus den Stellungnahmen zu Änderungen der OH Telemedien 2021 geführt haben,

Auswertungsbericht (Kurzlink): https://t1p.de/Auswertungsbericht

hat der Arbeitskreis Medien einen gut siebzigseitigen Auswertungsbericht erstellt und veröffentlicht. Diesem können auch umfassende Begründungen zu den Änderungen der OH Telemedien 2021 in der Version 1.1 entnommen werden.

Wesentliche Kritikpunkte

Die Hinweise in den Stellungnahmen beziehen sich nicht immer auf konkrete Kapitel oder Textstellen der OH Telemedien 2021. Daher wurde eine themenbezogene Auswertung vorgenommen, bei der jeweils die Aussagen aller Stellungnahmen zu einem Thema gebündelt berücksichtigt worden sind. Es haben sich insbesondere zwei Themen herauskristallisiert, denen in den Stellungnahmen eine besonders hohe Bedeutung beigemessen worden ist.

Ablehnen-Schaltfläche auf erster Ebene des Einwilligungsbanners
Viele Einwilligungsbanner auf Webseiten verfügen auf der ersten Ebene über eine Schaltfläche auf die der Nutzer klicken soll, um in die Einbindung einer Vielzahl Cookies und Drittdienstleistern zu unterschiedlichen Zwecken einzuwilligen. In der OH Telemedien 2021 wird in diesem Fall eine ebenfalls auf der ersten Ebene gleichwertige Schaltfläche gefordert, um eine Einwilligung zu verweigern. Diese Forderung wurde in vielen Stellungnahmen mit unterschiedlichen Argumenten abgelehnt.

Ausnahme vom Einwilligungserfordernis gemäß § 25 Abs. 2 Nr. 2 TTTDSG
Der zweite Themenbereich bezieht sich auf die Voraussetzungen der Ausnahme vom Einwilligungserfordernis beim Einsatz von Cookies und der Einbindung von Drittdiensten auf Webseiten gemäß § 25 Abs. 1 TTDSG. Die Einwilligung ist nur dann nicht erforderlich, wenn die Speicherung von Informationen auf dem Endgerät des Nutzers oder der Zugriff auf bereits im Endgerät gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann. Die OH Telemedien 2021 enthält Ausführungen, wie insbesondere Betreiber von Webseiten die Bewertungen vornehmen können, was der vom Nutzer ausdrücklich gewünschte Telemediendienst ist und wann insbesondere das Setzen und Auslesen von Cookies unbedingt erforderlich ist. In den Stellungnahmen wurde diesen Bewertungsmaßstäben widersprochen. Es wurden alternative Ansätze vertreten, die letztlich dazu führen, dass deutlich mehr Vorgänge i.S.v. § 25 Abs. 1 TTDSG keiner Einwilligung bedürfen.

Wesentliche Änderungen

Die in den Stellungnahmen geäußerten Kritikpunkte führten nicht dazu, dass die DSK wesentliche Änderungen in ihrer rechtlichen Bewertung vorgenommen hat. Die OH Telemedien 2021 Version 1.1 enthält aber zahlreiche und umfassende Klarstellungen und Ergänzungen insbesondere auch im Bezug auf die aufgeführten wesentlichen Kritikpunkte.

Abgesehen von der Anpassung zahlreicher Textpassagen sind folgende Änderungen vorgenommen worden:

- Die OH Telemedien 2019 wurde vollständig in die OH Telemedien 2021 Version 1.1 aufgenommen. Die OH Telemedien 2019 ist damit ungültig.
- Im Kapitel IV. Rechtmäßigkeit der Verarbeitung gemäß DS-GVO sind die Rechtsgrundlagen für die öffentlichen Stellen Art. 6 Abs. 1 lit. c) DS-GVO – Rechtliche Verpflichtung und Art. 6 Abs. 1 lit. e) DS-GVO – Wahrnehmung öffentlicher Interessen in den ergänzten Kapiteln 3. und 4. aufgenommen worden.
- Das Kapitel V. „Gestaltung von Einwilligungsbannern" wurde neu aufgenommen.

Es freut mich sehr, dass meine Behörde an der kleinen Arbeitsgruppe, die das Konsultationsverfahren durchgeführt hat, beteiligt war und dieses zusammen mit dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und dem Bayerischen Landesamt für Datenschutzaufsicht zügig durchführen konnte. Damit ist es der DSK zeitnah mit dem Inkrafttreten des TTDSG gelungen, mit der Orientierungshilfe eine wertvolle Anwendungshilfe für öffentliche und nicht-öffentliche Stellen zur Verfügung zu stellen. Das Konsultationsverfahren sehe ich als Chance, ein erstes und unmittelbares Feedback aus der Praxis einzuholen und gegebenenfalls verbleibende Unklarheiten und Unsicherheiten aufzudecken.

E.10. DSK geht gemeinsam gegen Facebook-Fanpages bei Bundes- und Landesbehörden vor

Im November 2021 hat das Oberverwaltungsgericht (OVG) Schleswig-Holstein nach einem insgesamt zehn Jahre andauernden Rechtsstreit abschließend bestätigt, dass die im Jahr 2011 durch das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein gegenüber der Wirtschaftsakademie Schleswig-Holstein angeordnete Deaktivierung der Facebook-Fanpage rechtmäßig erfolgte. Die Datenschutzkonferenz (DSK) hat daher Anfang 2022 entschieden, gemeinsam aktiv gegen Facebook Fanpages der obersten Bundes- und Landesbehörden vorzugehen.

Bereits 2018 hatte der Europäische Gerichtshof (EuGH) in dem genannten Rechtsstreit festgestellt, dass Betreiber einer Fanpage gemeinsam mit dem Unternehmen Facebook LLC – mittlerweile umbenannt in Meta Platforms Inc. – datenschutzrechtlich verantwortlich sind. Auf diese Entscheidung hat die DSK durch insgesamt drei Veröffentlichungen (Entschließung vom 05.6.2018, Beschluss vom 05.9.2018, Positionierung vom 01.4.2019) immer wieder aufmerksam gemacht. Dennoch konnten die Aufsichtsbehörden kaum einen Rückgang der von deutschen Behörden und Unternehmen in Deutschland betriebenen Facebook-Fanpages feststellen. Selbst die niedersächsische Staatskanzlei ist meiner ausdrücklichen Aufforderung zur Deaktivierung ihrer Fanpage nicht nachgekommen. Die Situation in anderen Bundesländern und bei den Bundesbehörden ist vergleichbar.

Beschluss der DSK (Kurzlink): https://t1p.de/TaskforceFanpages

Daher hat die DSK im März 2022 beschlossen, darauf hinzuwirken, dass von Landes- und Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Rechtlich gestützt wird diese Aktion nicht nur auf die Gerichtsentscheidungen, sondern auf ein von der DSK beschlossenes „Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages“, das mittlerweile in der überarbeiteten Version 1.1 vorliegt. In diesem Kurzgutachten werden die seit den Gerichtsentscheidungen eingetretenen Veränderungen der technischen Gestaltung des sozialen Netzwerkes Facebook.com und der Rechtslage durch die Geltung des TTDSG seit dem 1.12.2021 ebenso berücksichtigt, wie die mittlerweile durch Bundes- und Landesbehörden in den jeweiligen Kontrollverfahren vorgetragenen Argumente für die Rechtmäßigkeit des Betriebs von Fanpages.

Kurzgutachten (Kurzlink): https://t1p.de/KurzgutachtenFanpages

Ich begrüße es sehr, dass die DSK bei diesem wichtigen Thema grundsätzlich mit einer Stimme spricht und ein gemeinsames Vorgehen abgestimmt hat. Bereits 2019 hatte ich darauf hingewiesen, dass es die Aufgabe der Aufsichtsbehörden ist, Gerichtsentscheidungen von grundsätzlicher Bedeutung bei Behörden und Unternehmen durchzusetzen.

E.11. Verbraucherschutz statt Datenschutz? Neue BGB-Vorschriften wirken sich nicht auf das Datenschutzrecht aus

Am 01.01.2022 sind im Bürgerlichen Gesetzbuch (BGB) neue zivilrechtliche Verbraucherschutzvorschriften über digitale Produkte in Kraft getreten. Diese dienen der Umsetzung der europäischen Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DI-RL). In den neuen zivilrechtlichen Verbraucherschutzvorschriften über digitale Produkte wird in § 312 Abs. 1 a BGB und § 327 q BGB „Vertragsrechtliche Folgen datenschutzrechtlicher Erklärungen des Verbrauchers" ein eindeutiger Bezug zum Datenschutzrecht hergestellt. Die Datenschutzkonferenz (DSK) hat Ende November 2022 mit einem Beschluss das Verhältnis der neuen Verbraucherschutzvorschriften zum Datenschutzrecht erläutert.

Die neuen Verbrauchervorschriften haben 2022 zu einer intensiven Diskussion in der Fachwelt geführt. Es wird vertreten, dass die verbraucherschutzrechtlichen Vorschriften das „Bezahlen mit Daten" legitimieren würde. Insbesondere im Internet wird dieses Geschäftsmodell seit langem praktiziert,

wenn werthaltige Inhalte, wie z. B. Zeitungsartikel oder Dienstleistungen, wie die Bereitstellung von Plattformen zur sozialen Vernetzung oder Suchmaschinen, von den Nutzerinnen und Nutzern nicht mit Geld bezahlt werden. Die vermeintlich kostenlosen Inhalte und Dienstleistungen werden häufig über personalisierte Werbung finanziert. Zu diesem Zweck wird das Verhalten der Nutzerinnen und Nutzer häufig nachverfolgt und die so gewonnenen Daten werden zu detaillierten Nutzerprofilen zusammengeführt und ausgewertet. Mit Hilfe dieser Profile kann personalisierte Werbung ausgespielt und dadurch höhere Werbeeinnahmen generiert werden.

DSK-Beschluss (Kurzlink): https://t1p.de/BGBundDatenschutz

Die DSK hat in dem Beschluss „Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht" ihr Rechtsverständnis dargelegt. Die Feststellungen zur DS-GVO und zum TTDSG basieren auf der Kernaussage, dass die Verbraucherschutzvorschriften keine unmittelbaren datenschutzrechtlichen Auswirkungen haben. § 312 Abs. 1 a BGB ist keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten eines Verbrauchers, mit dem ein Vertrag über digitale Inhalte oder digitale Dienstleistungen geschlossen worden ist. § 327 q BGB regelt allein die vertragsrechtlichen Folgen datenschutzrechtlicher Erklärungen des Verbrauchers – dem Widerruf einer datenschutzrechtlichen Einwilligung und dem Widerspruch gemäß Art. 21 DS-GVO.

Ungeachtet der Verbraucherschutzvorschriften im BGB ist das Unternehmen verpflichtet, das Datenschutzrecht einzuhalten.

Meine Behörde hat zusammen mit dem Hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit diesen Beschluss der DSK initiiert. Wir hielten es für sehr wichtig, möglichst frühzeitig in diesem Thema eine einheitliche Position der DSK abzustimmen und diese auch in der Öffentlichkeit transparent zu machen. Nur so kann es gelingen, den immer wieder neuen Ideen der Wirtschaft, Geld mit personenbezogenen Daten zu machen, einen Rahmen vorzugeben.

E.12. Beschluss der DSK zur einrichtungsbezogenen Impfpflicht

Die Datenschutzkonferenz (DSK) hat mit ihrem Beschluss „Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht" zu offenen Fragen im praktischen Vollzug und zum datenschutzkonformen Umgang mit den vorzulegenden Nachweisen Stellung genommen.

Beschluss der DSK (Kurzlink): https://t1p.de/BeschlussImpfpflicht

Inhalt – Worum geht es?

Für gesetzlich bestimmte Einrichtungen und Unternehmen aus dem Gesundheitsbereich galt gemäß § 20 a Absatz 1 des Infektionsschutzgesetzes (IfSG) alter Fassung im Zeitraum vom 15. März 2022 bis zum 31. Dezember 2022 eine einrichtungsbezogene Impfpflicht. In diesem Zeitraum durften in diesen Einrichtungen und Unternehmen nur Personen tätig sein, die gegen das Coronavirus SARS-CoV-2 geimpft oder von diesem genesen waren oder bei denen eine medizinische Kontraindikation für eine Impfung gegen das Coronavirus SARS-CoV-2 vorlag. Für die genannten Personen bestand eine Nachweispflicht über ihre Impfung, Genesung oder das Vorliegen einer medizinischen Kontraindikation.

Der Arbeitskreis Beschäftigtendatenschutz der DSK hat sich unter dem Vorsitz meiner Behörde Anfang 2022 insbesondere mit der Frage beschäftigt, welche personenbezogenen Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht verarbeitet werden dürfen und hierzu für die DSK einen Beschlussentwurf erarbeitet. Dabei wurden die zwischenzeitlich im März 2022 erfolgten Änderungen des IfSG berücksichtigt. Der DSK-Beschluss ist seit dem 14. April 2022 auf der Webseite der DSK veröffentlicht. Mit der Veröffentlichung konnte bei etlichen Fragen zur einrichtungsbezogenen Impflicht auf die bundesweit einheitlichen Wertungen der Aufsichtsbehörden verwiesen werden. Hierdurch wurde die datenschutzkonforme Umsetzung der Regelungen für den Rechtsanwender deutlich vereinfacht.

Wie geht es weiter mit den gespeicherten „Corona-Daten"?

Pressemitteilung (Kurzlink): https://t1p.de/Coronadaten-loeschen

Viele gesetzliche Pflichten, die im Zusammenhang mit der Corona-Pandemie standen, sind bereits weggefallen. Damit sind auch zahlreiche Datenverarbeitungen nicht mehr notwendig. Deshalb habe ich bereits im April 2022 in einer Pressemitteilung Unternehmen und öffentliche Stellen dazu aufgefordert, zu prüfen, ob und welche personenbezogenen Daten sie im Zusammenhang mit Maßnahmen zur Pandemiebekämpfung erhoben und gespeichert haben. Sind diese Maßnahmen und damit der Zweck der Datenverarbeitung weggefallen, müssen die Daten unverzüglich gelöscht werden.

F. Rechtsprechung von grundsätzlicher Bedeutung

F.1. Vorabentscheidungsverfahren zur DS-GVO beim EuGH

Seit Einführung der DS-GVO bestehen viele ungeklärte Rechtsfragen zur Auslegung des neuen Datenschutzrechts. Da die DS-GVO unmittelbar anwendbares europäisches Recht ist, haben den Europäischen Gerichtshof (EuGH) inzwischen zahlreiche Vorabentscheidungsersuchen zur DS-GVO erreicht.

Nach Artikel 267 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) entscheidet der EuGH über die Auslegung europäischen Rechts, wenn ein Gericht eines Mitgliedstaates einen Vorabentscheidungsantrag zu einer konkreten Rechtsfrage stellt. Das Vorabentscheidungsverfahren beim EuGH dient der einheitlichen Anwendung europäischen Rechts in den einzelnen Mitgliedstaaten. Zur DS-GVO sind bis zum Ende des Jahres 2022 rund 40 Vorabentscheidungsersuchen beim EuGH eingegangen. Dieser Bericht stellt die wichtigsten derzeit anhängigen Vorabentscheidungsverfahren dar.

Unmittelbare Verbandshaftung (C-807/21)

Das Kammergericht Berlin legte am 21. Dezember 2021 dem EuGH die für die Verfolgung von Ordnungswidrigkeiten in Unternehmen wichtige Frage vor, ob nach der DS-GVO eine unmittelbare Haftung des Unternehmens für alle innerhalb des Unternehmens begangenen Datenschutzverstöße besteht. Nach deutschem Ordnungswidrigkeitenrecht knüpfen Geldbußen für juristische Personen an den vorwerfbaren Verstoß einer Leitungsperson an, die dem Unternehmen zugerechnet wird (§ 30 Ordnungswidrigkeitengesetz – OWiG). Die Aufsichtsbehörden des Bundes und der Länder sind der Ansicht, dass die Regelung des § 30 OWiG aufgrund der in der DS-GVO vorausgesetzten unmittelbaren Verbandshaftung und der Vorrangigkeit des europäischen Rechts nicht anwendbar ist. Deutsche Gerichte hatten hierzu unterschiedlich geurteilt, so dass letztlich eine Entscheidung durch den EuGH erforderlich ist.

Tätigkeitsbericht 2020, S. 86 und Tätigkeitsbericht 2021, S. 55

Für den Fall, dass der EuGH die unmittelbare Verbandshaftung bejaht, fragt das Kammergericht in einer zweiten, nicht weniger bedeutsamen Vorlagefrage, ob Art. 83 Abs. 4 bis Abs. 6 DS-GVO dahingehend auszulegen ist, dass das Unternehmen den durch Mitarbeitende vermittelten Verstoß schuldhaft begangen haben muss oder ob für die Verhängung eines Bußgeldes im Grundsatz bereits ein ihm zuzuordnender objektiver Pflichtenverstoß ausreicht („strict liability").

Rechtsnatur des Beschwerderechts (C-64/22 und C-26/22) und aufsichtsbehördliche Maßnahmen (C-768/21)

Wiederum aus Deutschland (Verwaltungsgericht (VG) Wiesbaden) stammt die Vorlagefrage zur Rechtsnatur des Rechts auf Beschwerde nach Artikel 77 DS-GVO: Hat das Recht auf Beschwerde petitionsähnlichen Charakter und ist der Bescheid der Aufsichtsbehörde gegenüber der beschwerdeführenden Person gerichtlich voll überprüfbar? Ich bin der Ansicht, dass die Beschwerde zwar keinen petitionsähnlichen Charakter hat, sich die gerichtliche Kontrolle einer Beschwerdeentscheidung aber dennoch darauf beschränkt, ob sich die Behörde mit der Beschwerde befasst, den Beschwerdegegenstand angemessen untersucht und die beschwerdeführende Person über das Ergebnis der Prüfung unterrichtet hat. Weiter begründet das Beschwerderecht keinen Anspruch auf eine bestimmte aufsichtsbehördliche Maßnahme. Die Rechte der beschwerdeführenden Person und der zulässige Prüfumfang im Rahmen einer Klage gegen eine Beschwerdeentscheidung nach Artikel 78 DS-GVO sind Gegenstand dieses Vorlageverfahrens.

Unter Bezugnahme auf das Vorlageersuchen zum Rechtscharakter des Beschwerderechts ergänzte das Verwaltungsgericht Wiesbaden eine weitere Vorlagefrage zu den Regelungen bezüglich der Aufgaben der Aufsichtsbehörden: Ist die Aufsichtsbehörde verpflichtet, bei jedem festgestellten Verstoß eine der in Artikel 58 DS-GVO aufgeführten aufsichtsbehördlichen Maßnahmen gegen den Verantwortlichen zu ergreifen oder steht ihr auch das Recht zu, nach eigenem Ermessen in geeigneten Fällen von einem Einschreiten abzusehen? Das Verwaltungsgericht Wiesbaden sieht jedenfalls

Zum Recht auf Beschwerde: Tätigkeitsbericht 2020, S. 78.

einen Spielraum der Aufsichtsbehörden, von Sanktionen oder Maßnahmen auch bei einem festgestellten Verstoß abzusehen.

Immaterieller Schadensersatz nach der DS-GVO (C-590/22, C-456/22, C-182/22, C-741/21, C-687/21, C-300/21, C-667/21)

Mehrere Vorlageersuchen von verschiedenen deutschen Gerichten behandeln das Recht auf Schadensersatz nach der DS-GVO. Mehrfach wird die Frage gestellt, ob zur Begründung eines Schadensersatzanspruchs der festgestellte Verstoß gegen Datenschutzrecht genügt oder ob zusätzlich eine tatsächliche Beeinträchtigung von gewissem Gewicht bzw. ein spürbarer Nachteil bei der betroffenen Person eingetreten sein muss. Nach ständiger deutscher Rechtsprechung führt nämlich eine Verletzung des allgemeinen Persönlichkeitsrechts nur dann zu einem Anspruch auf Geldentschädigung, wenn es sich um eine schwerwiegende Beeinträchtigung handelt. Weiter ist unklar, ob der Schadensersatz nach Artikel 82 DS-GVO echten Sanktionscharakter hat oder mit diesem nur eine Ausgleichs- oder Genugtuungsfunktion verfolgt wird. Es ist daher fraglich, ob ein Verschulden durch den Verantwortlichen festgestellt werden muss. Außerdem hat der EuGH darüber zu entscheiden, ob die Schadensersatznorm des Artikel 82 DS-GVO wegen Unbestimmtheit bezüglich der konkreten Rechtsfolgen gegebenenfalls unwirksam ist.

Auskunftsrecht (C-307/22, C-203/22, C-579/21, C-487/21, C-154/21)

Zur Reichweite und zum Zweck des Rechts auf Auskunft nach Artikel 15 DS-GVO wurden dem EuGH ebenfalls gleich mehrere Vorlagefragen vorgelegt. Gefragt wird z. B., ob bei Geltendmachung des Auskunftsrechts immer ein datenschutzbezogener Zweck vorliegen muss. Ebenso bedarf der Inhalt des Auskunftsrechts bezüglich der verpflichtenden Angaben zum Profiling und zu den Empfängern von personenbezogenen Daten näherer Konkretisierung. Ein weiteres Gericht beschäftigte sich mit der Frage, ob sich das Auskunftsrecht auch auf die Identität von beim Verantwortlichen beschäftigten Personen bezieht, welche konkret die personenbezogenen Daten einer betroffenen Person verarbeitet haben. Wesentlich ist die zur Auslegung vorgelegte und viel diskutierte Frage, wie der Begriff der „Kopie" in Artikel 15 Absatz 3 DS-GVO auszulegen ist.

Spezifische Regelungen zum Beschäftigtendatenschutz (C-34/21)

Der EuGH hat sich weiter mit der Frage zu befassen, ob § 23 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) mit der Öffnungsklausel des Artikel 88 DS-GVO vereinbar ist. Die DS-GVO gewährt zwar die Möglichkeit, eigene nationale spezifische Regelungen zum besseren Schutz von Beschäftigtendaten zu schaffen. Fraglich ist in diesem Zusammenhang jedoch,

ob eine nationale Vorschrift wie § 23 HDSIG bestimmte inhaltliche Anforderungen erfüllen muss oder ob etwa ein Verweis auf die Geltung der Grundsätze der DS-GVO wie in § 23 Absatz 5 HDSIG genügt. Sollte die Regelung des § 23 HDSIG nicht den Anforderungen an ein „spezifisches Gesetz" im Sinne des Artikel 88 Absatz 2 DS-GVO genügen, stellt sich weiter die Frage, ob die nationale Regelung als Folge ohne weiteres unwirksam ist. Dieses Vorabentscheidungsverfahren könnte überdies mittelbar Bedeutung haben für die vom Wortlaut vergleichbare Norm des § 26 BDSG.

Zuständigkeit des Bundeskartellamts im Datenschutzbereich (C-252/21)

Nachdem das Bundeskartellamt einen Verstoß gegen die DS-GVO festgestellt und gegen den Verantwortlichen eine Anordnung erlassen hatte, stellte das Oberlandesgericht (OLG) Düsseldorf die Frage, ob eine nationale Kartellbehörde überhaupt über eigene Befugnisse im Bereich des Datenschutzrechts verfügt. Die Abgrenzung der Zuständigkeiten von Bundeskartellamt und Datenschutzaufsichtsbehörden bedarf der Auslegung durch den EuGH. Ein weiteres Thema dieses Vorlagebeschlusses des OLG Düsseldorf ist die mögliche Einordnung der Erfassung bzw. Verknüpfung personenbezogener Daten bei Facebook nach dem einfachen Aufruf von Webseiten oder Apps mit einem Bezug zu besonders sensiblen Daten wie Flirting-Apps, Partnerbörsen, gesundheitsbezogener Webseiten oder Webseiten politischer Parteien als eine Verarbeitung besonderer Kategorien von Daten nach Artikel 9 Absatz 1 DS-GVO. Außerdem ist fraglich, ob sich ein werbefinanziertes digitales soziales Netzwerk wie Facebook bezüglich dieser Datenverarbeitung auf die Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe b DS-GVO (Datenverarbeitung ist erforderlich zur Vertragserfüllung) berufen kann.

Betreuter als Verantwortlicher (C-461/22)

Das Landgericht Hannover legte dem EuGH die Frage vor, ob ein gesetzlich bestimmter Betreuer, der berufsmäßig als Betreuer tätig ist, als datenschutzrechtlich Verantwortlicher im Sinne des Artikel 4 Nummer 7 DS-GVO auch gegenüber der von ihm betreuten Person anzusehen ist. Die Folge wäre, dass der Betreuer auch gegenüber der von ihm betreuten Person nach Artikel 15 DS-GVO zur Auskunft verpflichtet ist. Einerseits ist ein Betreuer gemäß § 1902 Bürgerliches Gesetzbuch einem gesetzlichen Vertreter gleichgestellt, so dass jede vom Betreuer durchgeführte Datenverarbeitung stets gleichsam durch die von ihm betreute Person selbst erfolgt. Andererseits hält das Landgericht Hannover aufgrund des gesetzlichen Schuldverhältnisses zwischen dem Betreuer und der von ihm betreuten Person und der damit verbundenen Rechte und Pflichten des Betreuers eine Verpflichtung des Betreuers auch aus der DS-GVO für begründbar.

Begriff der automatisierten Datenverarbeitung (C-634/21)

Gegenstand eines Verfahrens vor dem VG Wiesbaden ist die Auslegung des Begriffs der „automatisierten Verarbeitung" im Sinne des Artikel 22 Absatz 1 DS-GVO. Fraglich ist, ob bereits die automatisierte Erstellung eines Wahrscheinlichkeitswertes über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung darstellt. Insbesondere fraglich ist dies, wenn die rechtliche Wirkung dieser Entscheidung darin besteht, dass der mittels personenbezogener Daten ermittelte Wert von dem Verantwortlichen an einen dritten Verantwortlichen übermittelt wird und der Dritte diesen Wert seiner Entscheidung über die Begründung eines Vertragsverhältnisses zugrunde legt. Diese Vorlagefrage hat unmittelbar Auswirkungen auf die Tätigkeit von Wirtschaftsauskunfteien, welche Score-Werte erstellen und diese an Dritte übermitteln. Handelt es sich hierbei um eine automatisierte Einzelfallentscheidung im Sinne des Artikel 22 Absatz 1 DS-GVO, wäre dieses Wirtschaftsmodell nur nach den Ausnahmetatbeständen des Artikel 22 Absatz 2 DS-GVO zulässig.

F.2. Artikel 5 Absatz 2 DS-GVO als Beweislastregel

Neben den allgemeinen Grundlagen und Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten in Artikel 5 Absatz 1 DS-GVO statuiert die DS-GVO in Absatz 2 des Artikels 5 eine sogenannte Rechenschaftspflicht. Mit der konkreten Bedeutung dieser Pflicht befasste sich in diesem Jahr das Bundesverwaltungsgericht (BVerwG).

Nach Artikel 5 Absatz 2 DS-GVO ist der Verantwortliche für die Einhaltung der Grundsätze des Artikel 5 Absatz 1 DS-GVO verantwortlich und muss deren Einhaltung nachweisen können. Zu diesen Grundsätzen gehören die Rechtmäßigkeit der Verarbeitung, die Transparenz bei der Verarbeitung und Prinzipien wie die Zweckbindung und die Datensparsamkeit. Die Einhaltung dieser Grundsätze wird durch Dokumentationen wie dem Verzeichnis von Verarbeitungstätigkeiten oder beispielsweise die Aufzeichnung von Einwilligungen nachgewiesen.

Die Rechenschaftspflicht als Beweislastregel

Mit Urteil vom 02.03.2022 (6 C 7.20) stellte das BVerwG fest, dass aus der Rechenschaftspflicht des Artikel 5 Absatz 2 DS-GVO auch eine besondere Beweislastregel zulasten des Verantwortlichen folgt. In einem Streit über die Rechtmäßigkeit der Datenverarbeitung trägt nach eindeutiger Aussage des Gerichts der Verantwortliche auch die Beweislast für die Einhaltung der datenschutzrechtlichen Grundsätze. Auch wenn die Rechenschaftspflicht oft nur im Zusammenhang mit Prüfungen durch die Aufsichtsbehörde gesehen wird, gilt diese Beweislast nach dem BVerwG auch im Verhältnis zwischen dem Verantwortlichen und der betroffenen Person.

Die rechtlichen Folgen der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO waren bisher umstritten; mit der eindeutigen Aussage des BVerwG ist eine spezifische Beweislastregel nun stets anzunehmen. Da der Verantwortliche außerdem die Zwecke und Mittel der Datenverarbeitung bestimmt, sind nur diesem die genauen Umstände und Ziele der Datenverarbeitung bekannt und nachweisbar. Verantwortliche sollten daher auf eine angemessene Dokumentation aller Aspekte der von ihnen durchgeführten Datenverarbeitung achten.

F.3. Bundesgerichtshof ergänzt Rechtsprechung zur Einschränkung des Auskunftsrechts durch die Rechte anderer Personen

Nachdem der Bundesgerichtshof (BGH) sich bereits im Jahr 2021 zum Umfang des Rechts auf Auskunft nach Artikel 15 DS-GVO geäußert hatte (Urteil vom 15. Juni 2021, VI ZR 576/19)[1], ergänzte das Gericht in diesem Jahr seine Rechtsprechung zum Auskunftsrecht in Bezug auf die Berücksichtigung von Rechten anderer Personen (Urteil vom 22. Februar 2022, VI ZR 14/21).

Das Recht auf Auskunft der betroffenen Person ist gemäß Artikel 15 Absatz 4 DS-GVO durch die Rechte und Freiheiten anderer Personen beschränkt. Ist anzunehmen, dass eine (vollständige) Auskunft andere Personen in ihren Rechten beeinträchtigt, ist die Pflicht zur Auskunft entsprechend eingeschränkt. Nach Erwägungsgrund 63 fallen unter den Begriff der Rechte anderer insbesondere Geschäftsgeheimnisse, Rechte des geistigen Eigentums und das Urheberrecht an Software. Auch Datenschutzrechte anderer Personen stellen im Sinne des Artikel 15 Absatz 4 DS-GVO Rechte anderer Personen dar.

Recht auf Auskunft versus Hinweisgeberschutz

Der BGH hatte in letzter Instanz über die Anwendung der Regelung zur Einschränkung des Auskunftsrechts nach Artikel 15 Absatz 4 DS-GVO zu entscheiden. Im verhandelten Fall hatte sich ein Mieter bei seinem Vermieter über vermeintliche anhaltende Geruchsbelästigungen und mutmaßlichen Ungezieferbefall in einer Nachbarwohnung beschwert. Nach Vorhaltung der Beschwerde gegenüber dem betroffenen Mieter verlangte dieser Auskunft gemäß Artikel 15 Absatz 1 DS-GVO über den Namen des Hinweisgebers. Der Vermieter verweigerte diese Auskunft mit Verweis auf die Beeinträchtigung der Rechte des Hinweisgebers gemäß Artikel 15 Absatz 4 DS-GVO. In seinem Urteil wog der BGH das berechtigte Interesse des angezeigten Mieters als betroffene Person, Kenntnis zu erlangen über die Identität der Person, welche ihn bei seinem Vermieter angezeigt hatte, ab mit dem Interesse des meldenden Mieters, unerkannt zu bleiben.

1 Siehe 27. Tätigkeitsbericht (2021).

Im vorliegenden Fall sah der BGH im Ergebnis keine Pflicht zur Einschränkung des Auskunftsrechts, da das Interesse des Hinweisgebers an einer Geheimhaltung seiner Identität jedenfalls nicht das Auskunftsinteresse des Betroffenen überwiege. Das Recht auf Auskunft über die Herkunft personenbezogener Daten solle nämlich die betroffene Person gerade in die Lage versetzen, mögliche Rechte auch gegen die Person oder Stelle geltend zu machen, von der die (möglicherweise unrichtigen oder zu Unrecht weitergegebenen) Daten herrühren. Allein der Einwand des Verantwortlichen (hier des Vermieters), einem Hinweisgeber Vertraulichkeit zugesichert zu haben oder der pauschale Verweis auf das Schutzbedürfnis eines Hinweisgebers, genügten nicht zur Verweigerung der entsprechenden Auskunft gegenüber der betroffenen Person. Vielmehr seien die Rechte der Betroffenen im Einzelfall abzuwägen, wobei die Richtigkeit oder Unrichtigkeit der mitgeteilten personenbezogenen Daten eine maßgebliche Rolle spiele. Der Verantwortliche trage die Darlegungs- und Beweislast für die Umstände, die im Rahmen der gebotenen Interessenabwägung die Verweigerung der begehrten Auskunft über die Person des Hinweisgebers rechtfertigen sollen. Im vorliegenden Fall musste der BGH als Revisionsinstanz davon ausgehen, dass die Information über den Mieter unrichtig war, was folgerichtig eine uneingeschränkte Auskunft über die Herkunft dieser Information zur Folge hätte. Im Ergebnis hat der BGH die Sache an die Vorinstanz zurückverwiesen.

Die Frage, ob das Recht auf Auskunft gemäß Artikel 15 Absatz 4 DS-GVO durch die Rechte anderer beeinträchtigt ist und ob als Folge eine (vollständige) Auskunft unterbleiben muss, ist im jeweiligen Einzelfall unter Abwägung der jeweiligen Interessen und Beeinträchtigungen zu entscheiden. Der BGH stellt mit seinem Urteil klar, dass der einfache Verweis auf eine Schutzbedürftigkeit einer anderen Person zur Verweigerung der Auskunft jedenfalls nicht genügt.

F.4. Vorratsdatenspeicherung verstößt gegen europäisches Recht

Am 20. September 2022 hat der Europäische Gerichtshof (EuGH) sein inzwischen drittes Urteil zur Vorratsdatenspeicherung gefällt. In meinem Tätigkeitsbericht 2020 hatte ich bereits darauf hingewiesen, dass die Entscheidung des EuGHs zu § 113 a Abs. 1 i.V.m. § 113 b Telekommunikationsgesetz alte Fassung (TKG aF), der die Pflicht von Telekommunikationsdienstleistern zur Vorratsdatenspeicherung in Deutschland statuiert, noch aussteht. Mit dem Begriff Vorratsdatenspeicherung wird das vor allem von Strafverfolgungsbehörden und Geheimdiensten immer wieder beschworene Instrument beschrieben, dass Anbieter von Telekommunikationsdiensten ohne Anlass und Differenzierung verpflichtet werden sollen, personenbezogene Kommunikationsdaten über ihre Kunden für längere Zeiträume zu speichern und zur Ermittlung und Verfolgung von Straftaten zur Verfügung zu stellen. Der EuGH bestätigt in dem jüngsten Urteil seine Grundsatzentscheidungen aus den Jahren 2014 und 2020. Erwartungsgemäß hat der EuGH auch die deutschen Vorschriften zur anlass- und unterschiedslosen Speicherung von Kommunikationsdaten auf Vorrat für die Zwecke der allgemeinen Verbrechensbekämpfung oder zur Wahrung der nationalen Sicherheit als Verstoß gegen europäisches Recht gewertet.

Tätigkeitsbericht 2020, S. 52 ff..

Hintergrund der Entscheidung[1] sind zwei Gerichtsverfahren zwischen der Bundesrepublik Deutschland, vertreten durch die Bundesnetzagentur (BNetzA) für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, auf der einen Seite und der SpaceNet AG (Rs. EUGH Aktenzeichen C-793/19) bzw. der Telekom Deutschland GmbH auf der anderen Seite. In den Verfahren wird die Rechtmäßigkeit der gesetzlichen Pflicht zur Vorratsdatenspeicherung auf der Grundlage der genannten TKG-Vorschriften überprüft. Die SpaceNet AG war als Internetzugangsprovider zur Speicherung von IP-Adressen auf Vorrat verpflichtet worden. Die Telekom Deutschland GmbH bietet zusätzlich öffentlich zugängliche Telefondienste an, sodass sich die Pflicht zur Speicherung der Kommunikationsdaten ihrer Kunden auch auf die Telefonie bezieht.

1 Die Entscheidung ist im Volltext abrufbar unter: https://t1p.de/EuGH_SpaceNet.

Kernaussagen der EuGH-Entscheidung

Allgemeine und unterschiedslose Pflicht zur Vorratsspeicherung grundsätzlich europarechtswidrig

Im Einklang mit seiner bisherigen Rechtsprechung stellt der EuGH erneut ausdrücklich fest, dass nationale Rechtsvorschriften, durch die präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorgesehen ist, grundsätzlich europarechtswidrig sind. Darüber hinaus konkretisiert er die Grenzen und Anforderungen für zulässige und unzulässige Vorratsdatenspeicherungen. Der EuGH differenziert einerseits sehr detailliert zwischen verschiedenen Zwecken, für die eine Vorratsdatenspeicherung in Betracht gezogen wird. Dies sind in abgestufter Reihenfolge

- der Schutz der nationalen Sicherheit,
- die Bekämpfung schwerer Kriminalität und Verhütung schwerer Bedrohungen der öffentlichen Sicherheit sowie
- die Bekämpfung der Kriminalität und der Schutz der öffentlichen Sicherheit.

Andererseits wird zwischen den Daten unterschieden, die von der Vorratsspeicherung erfasst sein sollen. Es werden unterschiedliche Maßstäbe für Verkehrs- und Standortdaten, IP-Adressen und Daten, die die Identität der Nutzer elektronischer Kommunikationsmittel betreffen, definiert.

Demnach wäre eine allgemeine und unterschiedslose Vorratsdatenspeicherung mit dem Unionsrecht grundsätzlich vereinbar, von

- Verkehrs- und Standortdaten nur, wenn sie dem Schutz der nationalen Sicherheit dient und sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht,
- IP-Adressen zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit nur für einen auf das absolut Notwendige begrenzten Zeitraum und
- Daten über die Identität der Nutzer elektronischer Kommunikationsdienste.

Eine gezielte Vorratsspeicherung – diese betrifft eine begrenzte Personenzahl – von Verkehrs- und Standortdaten wäre mit dem Unionsrecht grundsätzlich vereinbar, wenn sie dem Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit dient und anhand objektiver Kriterien personell oder geografisch sowie zeitlich auf das absolut Notwendige begrenzt ist. Sie ist im Einzelfall auch in Bezug auf Personen zulässig, zu denen zumindest eine indirekte Verbindung zur verfolgenden Tat besteht.

Vorschriften zur Vorratsdatenspeicherung im TKG müssen angepasst werden.

Darüber gestatten die Bekämpfung schwerer Kriminalität und der Schutz der nationalen Sicherheit die Betreiber elektronischer Kommunikationsdienste anzuweisen, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern.

Jegliche Maßnahme muss bezogen auf Anlass, personellen und zeitlichen Umfang sowie alternative Ermittlungsmaßnahmen verhältnismäßig und daher auf das absolut Notwendige beschränkt sein. Der EuGH greift umfassend die Bewertungsmaßstäbe und Anforderungen auf, die er insbesondere in der Entscheidung aus 2020 formuliert hat.

Konsequenzen für Deutschland

Die EuGH-Entscheidung bezieht sich auf einen Rechtsstreit, dem die §§ 113 a und 113 g TKG aF zugrunde liegen. Mittlerweile wurde das Telekommunikationsgesetz modernisiert. Die Regelung zur Vorratsdatenspeicherung wurde weitgehend unverändert in die §§ 175 bis 181 TKG übernommen. Die Bundesregierung wollte die Entscheidung des EuGH abwarten und anschließend die Regelungen zur Vorratsdatenspeicherung so gestalten, dass „Daten rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können". Wie die §§ 175 bis 181 TGK nun anzupassen sind, lässt sich sehr klar und deutlich aus der EuGH-Entscheidung ableiten. Ich hoffe sehr, dass der Gesetzgeber nun zeitnah der Zusage aus dem aktuellen Koalitionsvertrag Taten folgen lässt und die TKG-Vorschriften angepasst werden.

F.5. Schutz des Beschwerdeführers bei Akteneinsicht

Das Verwaltungsgericht (VG) Hannover befasste sich mit der Frage, ob die Herausgabe des Namens der Beschwerde führenden Person an den Verantwortlichen gerechtfertigt ist. Ähnlich wie in dem vom BGH entschiedenen Fall zum Auskunftsrecht (siehe F.3., S.62) geht es auch hier um eine Abwägung verschiedener Interessen und letztlich um die Frage, wie weit der Schutz von Informanten reicht.

Ein Mitarbeiter hatte bei mir eine Beschwerde nach Art. 77 DS-GVO wegen Datenschutzverstößen in seinem Unternehmen eingelegt. Das verantwortliche Unternehmen hatte hierauf bei mir Akteneinsicht nach § 29 Verwaltungsverfahrensgesetz (VwVfG) beantragt mit dem erklärten Ziel, Kenntnis zu erlangen über die Identität des Informanten aus dem Unternehmen. Ich entschied mich jedoch, zum Schutz des Mitarbeiters vor arbeitsrechtlichen Konsequenzen die entsprechenden personenbezogenen Angaben zu schwärzen und insofern eine nur begrenzte Einsicht in die Verwaltungsakte zu gewähren.

Rechtsprechung des VG Hannover mit Blick auf den Informantenschutz

Das VG Hannover setzt mit seinem Urteil vom 03. August 2022 (10 A 1307/20) seine frühere Rechtsprechung fort, in welcher sich insgesamt nun eine deutliche Tendenz zum Schutz von Informanten zeigt.

Tätigkeitsbericht 2020, S. 80.

Nach Ansicht des Gerichts ist die Herausgabe des Namens eines Beschwerdeführers im Rahmen eines Antrags auf Akteneinsicht nach § 29 VwVfG zu verweigern, wenn keine Anhaltspunkte dafür bestehen, dass der Beschwerdeführer die Aufsichtsbehörde wider besseres Wissen oder leichtfertig falsch informiert hat. Entscheidend sind hier die Ausschlusstatbestände des § 29 Absatz 2 Alternative 3 und 4 VwVfG: Eine Akteneinsicht kann verweigert werden, soweit Inhalte wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheim gehalten werden müssen. Die Entscheidung über die Herausgabe bestimmter Inhalte einer Akte muss abgewogen werden zwischen dem Geheimhaltungsinteresse der anderen Personen und dem Auskunftsinteresse des Antragstellers. Das VG Hannover lässt hierbei insbesondere behördlichen Informanten einen besonderen Schutz zukommen. Im hier entschiedenen Fall waren nach Ansicht des Gerichts keine Anhaltspunkte zu erkennen, dass der Informant wider besseres Wissen oder leichtfertig falsche Behauptungen aufgestellt hat, da die Angaben des Beschwerdeführers zu Pflichtverletzungen des Verantwortlichen konkret und nachvollziehbar waren und das verantwortliche Unternehmen letztlich sogar selbst die eigene Datenverarbeitung nach Kenntnis der Beschwerde umgestellt hatte. Meine Rechtsauffassung, wonach der Name des Beschwerdeführers hier zu schwärzen war, wurde also vom Gericht bestätigt.

F.6. Selbständige Evangelisch-Lutherische Kirche (SELK) unterliegt der Datenschutzaufsicht durch die LfD

Mit Urteil vom 30. November 2022 (Az. 10 A 1195/21) hat das Verwaltungsgericht Hannover meine Sichtweise bestätigt, dass die SELK an die DS-GVO gebunden ist und meiner Aufsicht unterliegt. Bei dem Urteil handelt es sich um die erste Grundsatzentscheidung zur Auslegung des Art. 91 DS-GVO.

Pressemitteilung des VG Hannover (Kurzlink): https://t1p.de/SELK

Der Rechtsstreit zwischen der SELK und meiner Behörde begann bereits im Jahr 2020. Nachdem eine außergerichtliche Klärung nicht möglich gewesen war, erhob die SELK im Frühjahr 2021 Klage gegen meine Behörde. Die Klage zielte auf eine Feststellung ab, dass die SELK im Zeitpunkt des Inkrafttretens der DS-GVO umfassende Datenschutzregelungen angewandt hat oder jedenfalls nach Inkrafttreten der DS-GVO umfassende Regelungen im Sinne des Art. 91 DS-GVO erlassen durfte und weiter anwenden darf. Weiter wurde Feststellung beantragt, dass die SELK berechtigt sei, eine spezifische Aufsichtsbehörde einzurichten und deshalb nicht meiner Aufsicht unterliege. Fragen zur Auslegung des Art. 91 DS-GVO sollten dem EuGH im Wege eines Vorabentscheidungsverfahren vorgelegt werden.

Zur Vorgeschichte: Tätigkeitsbericht 2020, S. 191.

Das Verwaltungsgericht Hannover urteilte zunächst, dass die SELK kein eigenes Datenschutzrecht anwenden dürfe, weil die Kirche am maßgeblichen Stichtag 24. Mai 2016 keine umfassenden Regeln im Sinne von Art. 91 DS-GVO angewandt hatte. Im Zusammenspiel mit Art. 99 Abs. 1 DS-GVO werde deutlich, dass Art. 91 DS-GVO auf den Zeitpunkt des Inkrafttretens der DS-GVO am 24. Mai 2016 abstelle. Die Sichtweise der Klägerin, dass es genüge, wenn im Zeitpunkt des Geltungsbeginns der DS-GVO am 25. Mai 2018 umfassende Regelungen vorgelegen hätten, würde die Wortlautgrenze der Auslegung überschreiten.

Auslegung des Begriffs „umfassend" in Art. 91 DS-GVO

Weiter urteilte das Gericht, dass die SELK am Tag des Inkrafttretens der DS-GVO keine umfassenden Datenschutzregelungen angewendet habe, weil die Regelungsdichte der Datenschutzrichtlinie aus dem Jahr 1993 zu gering gewesen sei. Unter „umfassend" sei zu verstehen, dass die Datenschutzregeln

der Religionsgemeinschaft vollständig seien und nicht durch staatliche Regelungen ergänzt werden müssten. Der Begriff „umfassend" beziehe sich auf das Gesamtwerk der Regelungen und nicht lediglich auf Einzelregelungen. Bei einer Akzeptanz von Teilregelungen bei gleichzeitiger Schließung der Lücken durch Rückgriff auf die DS-GVO bestünde die Gefahr der Zersplitterung des kirchlichen Datenschutzrechts, welche einen Zustand begründe, der unter dem Gesichtspunkt der Rechtssicherheit nicht zuträglich sei.

DSK-Beschluss zur spezifischen Aufsicht (Kurzlink): https://t1p.de/spez-aufsicht

Ferner folgte die Kammer der Sichtweise, die zuvor auch schon die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) vertreten hatte, dass es sich bei Art. 91 DS-GVO um eine abschließende Bestandsschutzregelung handele. Diese Auslegung ergebe sich sowohl aus dem Wortlaut der Überschrift („bestehende" Datenschutzvorschriften) als auch dem Wortlaut von Abs. 1 („zum Zeitpunkt des Inkrafttretens dieser Verordnung", „weiter angewandt"). Neu- bzw. Erstregelungen, die erst nach dem Stichtag erlassen wurden oder werden, fielen daher nicht unter die Ausnahmevorschrift des Art. 91 DS-GVO.

Verweis auf EuGH, Urt. v. 10.07.2018, C-25/17 – Jehovan todistajat

Diese Auslegung des Art. 91 DS-GVO verstoße auch nicht gegen höherrangiges Recht. Die DS-GVO sei ein „für alle geltendes Gesetz" im Sinne von Art. 140 GG i.V.m. Art. 137 Abs. 3 Satz 1 der Weimarer Reichsverfassung (WRV). Ebenso habe der EuGH in ständiger Rechtsprechung festgehalten, dass Kirchen und religiöse Gemeinschaften dem Datenschutzrecht als allgemeinem Gesetz unterlägen. Unter Verweis auf die Zeugen-Jehovas-Entscheidung des EuGH verwies die Kammer auf die für jedermann geltende Pflicht, die Vorschriften des Unionsrechts zum Datenschutz einzuhalten, welche nicht als Eingriff in die organisatorische Autonomie der Religionsgemeinschaften angesehen werden könne. Darüber hinaus begründe Art. 17 AEUV keine justiziablen subjektiven Rechte der von ihm erfassten Institutionen.

Keine Ungleichbehandlung von Glaubensgemeinschaften

Abschließend verneinte das Gericht nachvollziehbar auch eine Ungleichbehandlung von Glaubensgemeinschaften, die erst jetzt den Status der Körperschaft des öffentlichen Rechts erhielten, im Vergleich zu den etablierten Glaubensgemeinschaften. Zweck des Art. 91 DS-GVO sei es gewesen, bereits bestehende Datenschutzvorschriften der beiden großen Kirchen weiterhin Geltung zu verschaffen, nicht aber jeder Religionsgemeinschaft die Schaffung eigener Datenschutzvorschriften zu ermöglichen. Selbst wenn eine bereits vorhandene Religionsgesellschaft und eine neu hinzutretende Religionsgesellschaft als wesentlich gleich anzusehen wären, würde die Ungleichbehandlung auf dem sachlichen Grund des Bestandsschutzes beruhen.

Das Verwaltungsgericht Hannover urteilte weiter, dass die SELK nicht berechtigt gewesen sei, eine unabhängige Aufsichtsbehörde spezifischer Art gemäß Art. 91 Abs. 2 DS-GVO einzurichten. Art. 91 Abs. 2 DS-GVO beziehe sich nur auf Religionsgemeinschaften, die Datenschutzregeln anwenden, die alle Voraussetzungen des Art. 91 Abs. 1 DS-GVO erfüllten. Dies treffe auf die SELK nicht zu. Folglich sei meine Behörde für die Aufsicht über die SELK zuständig. Die Zuständigkeit folge aus Art. 55 DS-GVO und einer unionsrechtskonformen Auslegung und Anwendung der für die Aufsicht über juristische Personen des Privatrechts geltenden Zuständigkeitsregelungen in § 40 BDSG und § 22 NDSG auch auf Religionsgesellschaften, die nach Art. 140 GG i.V.m. Art. 137 Abs. 5 WRV den Status einer Körperschaft des öffentlichen Rechts haben.

SELK durfte keine spezifische Aufsichtsbehörde einrichten

Der von der SELK überdies beantragten Vorlage von Auslegungsfragen zu Art. 91 DS-GVO an den EuGH kam die Kammer nicht nach. Eine Vorlage an den EuGH sei nicht erforderlich, zumal die Kammer keine Zweifel an der Auslegung des Art. 91 DS-GVO habe. Die Berufung wurde aber aufgrund der grundsätzlichen Bedeutung zugelassen.

Aus meiner Sicht ist es sehr zu begrüßen, dass diese Vielzahl an wichtigen Auslegungsfragen zu Art. 91 DS-GVO nun erstmals gerichtlich entschieden wurde. Ich gehe davon aus, dass dieses Urteil über den konkreten Einzelfall hinaus auch für andere (Frei-)Kirchen oder Religionsgemeinschaften in anderen Bundesländern Bedeutung haben könnte. Allerdings bleibt zunächst noch die weitere Entwicklung der Rechtsprechung abzuwarten. Die SELK hat zwischenzeitlich Berufung beim Niedersächsischen Oberverwaltungsgericht in Lüneburg eingelegt.

SELK hat Berufung zum OVG beantragt

G. Beteiligung an Gesetzgebungsverfahren

G.1. Übersicht begleiteter Rechtssetzungsvorhaben

Die Begleitung von Rechtssetzungsvorhaben ist ein bedeutender Teil meiner Arbeit und nimmt dementsprechend viel Raum ein. Die folgende Übersicht soll das verdeutlichen, bevor ich anschließend auf einige Verfahren näher eingehe.

Gesetze

- Änderung Niedersächsisches Datenschutzgesetz (NDSG)
- Änderung Niedersächsisches Kommunalabgabengesetz (NKAG)
- Änderung Niedersächsisches Verwaltungsvollstreckungsgesetz (NVwVG)
- Änderung Niedersächsisches Krankenhausgesetz (NKHG)
- Entwurf Niedersächsisches Gesetz über die oder den Landesbeauftragten für Opferschutz (NLfOG)
- Änderung Niedersächsisches Ausführungsgesetz zum Bundesmeldegesetz (Nds. AG BMG)
- OZG-Umsetzungen / Gesetz zur Änderung des Niedersächsischen Verwaltungsvollstreckungsgesetzes und anderer Gesetze
- Entwurf eines Gesetzes zur Änderung des Niedersächsischen Finanzausgleichsgesetzes (NFAG), Aufnahmegesetzes und Niedersächsischen Ausführungsgesetzes zum Zweiten Buch des Sozialgesetzbuchs (SGB II)
- Änderung Niedersächsisches Justizgesetz (NJG)

Verordnungen

- Diverse Änderungen der Corona-VO Nds
- Diverse Änderungen der Niedersächsischen Corona-Absonderungs-VO
- Entwurf einer VO Ethikkommission Pflege

- Änderung Niedersächsische Meldeverordnung (NMeldVO)
- Entwurf MantelVO Förderung von Pflegeeinrichtungen
- Notverordnung zum Niedersächsischen Gesetz über Kindertagesstätten und Kindertagespflege (NKiTaG) – Ukraine
- Änderung Durchführungsverordnung Baugesetzbuch (DVO-BauGB)
- Änderung Durchführungsverordnung zum Niedersächsischen Gesetz über Kindertagesstätten und Kindertagespflege (NKiTaG)
- Entwurf einer Verordnung zur Förderung von Ombudsstellen nach § 9 a des Achten Buches des Sozialgesetzbuches (SGB VIII)
- Änderung Klinisches Krebsregister DatenbestimmungsVO
- VO zur Änderung der Verordnung über die Berechnung der Finanzhilfe für Schulen in freier Trägerschaft (FinHVO)
- Niedersächsische Verordnung zur elektronischen Aktenführung bei den Gerichten (Nds. eAktGerVO)
- Verordnung über die Bestellung von Beschäftigten des beliehenen Trägers einer Einrichtung des Maßregelvollzugs zu Verwaltungsvollzugsbeamtinnen und Verwaltungsvollzugsbeamten (VollzBeaMVollzVO)
- Verordnung zur Änderung der Wahlordnung für die Personalvertretungen im Land Niedersachsen (WO-Pers)
- Änderung der Spielordnung für die öffentlichen Spielbanken in Niedersachsen (NSpielO)
- Niedersächsische Verordnung über die maschinelle Führung der Schiffsregister und der Schiffsbauregister (Nds. MSchRegV)

Verwaltungsvereinbarungen

- Entwurf einer Verwaltungsvereinbarung zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen zur Durchführung des Staatsvertrages im Bereich Europäischer Garantiefonds für die Landwirtschaft (EGFL) und Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER)
- Entwurf einer Verwaltungsvereinbarung zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen zur Durchführung des Staatsvertrages im Bereich des ökologischen Landbaus

Verwaltungsvorschriften

- Information der Personal verwaltenden Dienststellen über Pfändungs- und Überweisungsbeschlüsse, Pfändungs- und Einziehungsverfügungen, Abtretungserklärungen sowie Verbraucherinsolvenzverfahren, Runderlass des Niedersächsischen Finanzministeriums
- Entwurf der Neufassung der Richtlinien zur gleichberechtigten und selbstbestimmten Teilhabe schwerbehinderter und ihnen gleichgestellter Menschen am Berufsleben im öffentlichen Dienst (Schwerbehindertenrichtlinien – SchwbRl)

G.2. Die Novellierung des Onlinezugangsgesetzes: Auf dem Weg zum „OZG 2.0“

Das Onlinezugangsgesetz (OZG) vom 14.8.2017 stellte bereits einen wichtigen Schritt in Richtung Digitalisierung der Verwaltung dar. Im Rahmen der Umsetzung kamen diverse Fragestellungen – auch solche datenschutzrechtlicher Natur – auf, die die bisherige Gesetzeslage nicht beantworten konnte. Zudem wurde immer klarer, dass die gesetzliche Umsetzungsfrist auf Grund diverser Faktoren nicht eingehalten werden kann. Dies machte eine Gesetzesanpassung in der Form eines „OZG 2.0“ notwendig.

„Einer für Alle"-Prinzip wird kodifiziert.

Meine Behörde ist Mitglied der Kontaktgruppe „OZG 2.0“ der Datenschutzkonferenz und begleitet in dieser Funktion den Gesetzgebungsprozess mit. In datenschutzrechtlicher Hinsicht ist dabei die Regelung des „Einer-für-Alle"-Prinzips hervorzuheben. Dabei setzt eine Behörde eine Online-Verwaltungsleistung (z. B. die Online-Beantragung eines Schwerbehindertenausweises; lesen Sie hierzu mehr in Kap. J.6.4) um und stellt diese den anderen Behörden zur Nutzung zur Verfügung. Auf diese Weise soll vermieden werden, dass mehrere Behörden verschiedene Anwendungen für ein und dieselbe Leistung entwickeln (lassen) müssen. Die bereitstellende Behörde erhebt dabei personenbezogene Daten der Antragstellenden über ein Online-Formular und leitet diese Daten weiter an die zuständige Fachbehörde, die den Antrag inhaltlich bearbeitet. Im Rahmen des OZG 2.0 wird angestrebt, eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die bereitstellende Behörde zu schaffen und dieser die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung zuzuweisen. Hiervon unberührt bleibt die datenschutzrechtliche Verantwortlichkeit für die Antragsbearbeitung bei der für den Antrag zuständigen Fachbehörde.

Der Entwurf des OZG 2.0 umfasst in Artikel 2 auch eine Änderung des E-Government-Gesetzes. Hierbei ist besonderes Augenmerk auf die Once-Only-Regelung zu richten (siehe auch Kapitel E.7., S.45).

Die Betroffenen im Mittelpunkt!

Im Gesamtgefüge zwischen der reinen Digitalisierung der Verwaltungsleistungen (OZG) und der Modernisierung der Register (RegModG/ID-NrG) einschließlich des Once-Only-Nachweisabrufs darf die Transparenz für die Betroffenen nicht aus den Augen verloren werden. Es ist von zentraler Bedeutung, dass sich die Betroffenen in jedem Stadium eines Verwaltungsverfahrens Klarheit darüber verschaffen können, mit welcher Behörde sie gerade kommunizieren und bei welchem Verantwortlichen sie ihre Rechte geltend machen können. Auch das ist und bleibt mein Anliegen bei der weiteren Begleitung dieses spannenden Themas.

G.3. Änderung des Niedersächsischen Krankenhausgesetzes – Die Landesbeauftragte für den Datenschutz ist auch ohne offizielle Beteiligung wachsam

Lt.-Drs. 18/10578 (Kurzlink): https://t1p.de/EntwurfNKHG

Bei der routinemäßigen Durchsicht der Landtagsdrucksachen bin ich in den Drucksachen vom 18.01.2022 auf einen Gesetzentwurf für ein neues Niedersächsisches Krankenhausgesetz (NKHG) von den Fraktionen der SPD und der CDU gestoßen. Mit § 31 NKHG-E sollten erstmals umfangreiche Datenverarbeitungsbefugnisse des Ministeriums für Soziales, Gesundheit und Gleichstellung (MS) in das Gesetz aufgenommen werden.

Unzureichende Regelungen

Im Rahmen der Neufassung des NKHG sollte mit § 31 NKHG-E eine umfassende allgemeine Datenübermittlungsbefugnis zwischen dem für Gesundheit zuständigen Fachministerium (MS) und den Verwaltungs-, Polizei- und Strafverfolgungsbehörden eingeführt werden. Neben den Daten des Krankenhausträgers, des Krankenhauspersonals, den Patientenfürsprechern und den Demenzbeauftragten des Krankenhauses wurden auch Daten von Patientinnen und Patienten explizit benannt. Es war unklar, wie und auf welcher Rechtsgrundlage das MS Patientendaten aus den Einrichtungen erhält und zu welchen Zwecken es diese verarbeiten sollte.

Unabhängig davon stellte § 31 NKHG-E keine auch nur im Ansatz hinreichende Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten (Art. 4 Nr. 15 i.V.m. Art. 9 Abs. 1 DS-GVO) dar.

Keine Beteiligung der LfD

Laut dem Kurzbericht des Ausschusses für Soziales, Gesundheit und Gleichstellung (154. – öffentliche – Sitzung am 20. Januar 2022) hat dieser die Einbringung des Gesetzentwurfs entgegengenommen und kam überein, zu dem Gesetzentwurf eine schriftliche Anhörung durchzuführen. Die von den Fraktionen benannten Anzuhörenden sollten mit einer Frist bis zum 16. Februar

2022 um eine schriftliche Stellungnahme gebeten werden. Da mir der Gesetzentwurf jedoch bis zum 07.02.2022 nicht vorgelegt wurde, musste ich davon ausgehen, dass ich im Rahmen der Anhörung nicht beteiligt werden sollte. Ich habe daher die von mir festgestellten Mängel gegenüber dem Vorsitzenden des Ausschusses sowie gegenüber allen im Landtag vertretenen Fraktionen schriftlich gerügt – mit Erfolg.

Kritik wurde umgesetzt

Eine offizielle Beteiligung meiner Behörde oder eine Rückmeldung seitens der Fraktionen oder des Ausschusses hat weiterhin nicht stattgefunden. Aus der Tagesordnung für die Plenarsitzung vom 28.06.2022 habe ich die im späteren Verlauf verabschiedete Fassung des Niedersächsischen Krankenhausgesetzes entnommen.

Der aktuellen Beschlussempfehlung (Drs. 18-11357) sowie dem schriftlichen Bericht (Drs. 18-11398) ist zu entnehmen, dass meine Intervention sehr erfolgreich gewesen ist:
Die entsprechende Vorschrift wurde unter Hinweis auf die „umfassende Kritik der LfD in der Anhörung grundlegend geändert" und entspricht nunmehr den datenschutzrechtlichen Vorgaben. Im schriftlichen Bericht wird rechtlich zutreffend auf viereinhalb Seiten auf die datenschutzrechtlichen Hintergründe der neuen Regelung eingegangen.

Muster für zukünftige Gesetzgebungsverfahren

Für zukünftige Gesetzgebungsverfahren, welche die Verarbeitung von besonderen Kategorien personenbezogener Daten umfassen sollen, können als Muster neben den oben genannten Ausführungen im schriftlichen Bericht auch die Gesetzgebungsmaterialien zur Änderung des § 31 Niedersächsisches Schulgesetzes (Lt.-Drs. 18/5416 vom 17.12.2019) und hier insbesondere die Ausführungen des Gesetzgebungs- und Beratungsdienstes in der Vorlage 12 vom 22.11.2019 zur Lt.-Drs. 18/4471 auf Seite 13 herangezogen werden.

Datenschutzexpertise frühzeitig nutzen

Bei Gesetzentwürfen der Landesregierung ist die Beteiligung der LfD in § 9 der Gemeinsamen Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen verpflichtend geregelt.

Gesetzentwürfe einer oder mehrerer Fraktionen unterfallen nicht dieser Vorschrift. Im Interesse der von einer Gesetzesänderung betroffenen Bürgerinnen und Bürger bietet es sich jedoch an, dass gerade, wenn die Regierungsfraktionen einen Gesetzentwurf einbringen, auch diese die LfD im Vorfeld beteiligen.

G.4. Änderungen der Niedersächsischen Corona-Verordnungen

Zur Bekämpfung des Coronavirus SARS-CoV-2 und Eindämmung der Krankheit COVID 19 wurden etliche gesetzliche und untergesetzliche Regelungen geschaffen und geändert. So waren im Jahr 2022 alleine jeweils zwölf verschiedene Versionen der Niedersächsischen Corona-Verordnung und des diese legitimierenden Infektionsschutzgesetzes in Kraft. Viele (Neu-)Regelungen waren in einem datenschutzrechtlichen Kontext zu bewerten.

Beteiligung meiner Behörde

Siehe 27. Tätigkeitsbericht der LfD, Abschnitt J.1.1, Seite 96

Im Gegensatz zu den beiden vorherigen Berichtszeiträumen wurde meine Behörde 2022 bei allen wesentlichen Änderungen der Niedersächsischen Corona-Verordnung beteiligt, was ich als positive Veränderung gegenüber den zurückliegenden Berichtszeiträumen hervorheben möchte. Dabei gehe ich davon aus, dass auch zukünftig eine frühzeitige Einbindung meiner Behörde bei entsprechenden Regelungsvorhaben erfolgt. Nur so kann eine umfassende und effiziente datenschutzrechtliche Beratung sichergestellt werden.

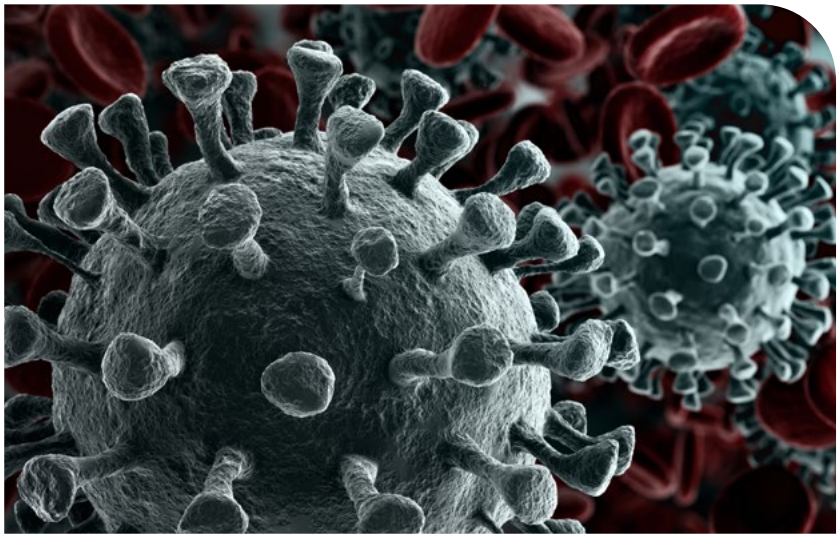
Materiell-rechtliche Änderungen

Inhaltich waren die Änderungen von der sich im Laufe des Jahres entspannenden Pandemielage geprägt. So konnten etliche Beschränkungen, wie etwa die allgemein gültige Zugangskontrolle zur Arbeitsstätte oder zu Freizeiteinrichtungen, aufgehoben werden. Die mit den Beschränkungen einhergehenden Datenverarbeitungsbefugnisse wurden aufgehoben. Dieses ist aus datenschutzrechtlicher Sicht sehr zu begrüßen.

Erledigung von Kritikpunkten

In diesem Zusammenhang verweise ich auf zwei – auf meine Anregung hin – erfolgte Klarstellungen in der Begründung zur aktuellen Niedersächsischen Corona-Verordnung vom 30. September 2022.[1] Für eine datenschutzkonforme Umsetzung der Verordnung ist Folgendes zu beachten:

1 Niedersächsisches Gesetz- und Verordnungsblatt, Nummer 34/2022 vom 10. Oktober 2022, Seite 617



Einfaches Attest zur Befreiung von der Pflicht zum Tragen einer Mund-Nase-Bedeckung (MNB)

Sofern in einzelnen Bereichen noch die Pflicht zum Tragen einer MNB besteht, ist nach § 2 Absatz 2 Nummer 2 der Verordnung eine Befreiung aus gesundheitlichen Gründen möglich. In der Vergangenheit war bei einem Beschäftigtenverhältnis streitig, ob zur Befreiung von der MNB-Pflicht der Betroffene ein qualifiziertes Attest vorlegen muss. In der Begründung der Verordnung wird nunmehr klargestellt, dass – im Beschäftigungsverhältnis – zur Befreiung von der MNB-Pflicht ein einfaches Attest ohne Angaben konkreter Gesundheitsdaten der betroffenen Person ausreichend ist.

Keine Befugnis zur Weiterverarbeitung bei „Vorlage“ eines 3G-Nachweises

Im Zusammenhang mit 3G-Daten wird in der Verordnung in § 4 Satz 1, § 5 Satz 1, § 7 Absatz 3 Satz 1 und Satz 3 sowie § 7 Absatz 4 Satz 1 und Satz 2 der Begriff „vorlegen“ verwendet. Zu dessen Auslegung stellt die Begründung klar, dass auf die „Vorlage“ keine personenbezogenen Daten der Beschäftigten, etwa für Dokumentations- beziehungsweise Nachweiszwecke weiterverarbeitet werden dürfen.

G.5. Gesetz über die Landesbeauftragte oder den Landesbeauftragten für Opferschutz

Am 23. September 2022 ist das Gesetz über die Niedersächsische Landesbeauftragte oder den Niedersächsischen Landesbeauftragten für den Opferschutz (NLfOG) in Kraft getreten. Die oder der Landesbeauftragte für den Opferschutz (LfO) dient als zentrale Anlaufstelle für die Opfer von Straftaten und ihnen nahestehenden Personen.

Siehe 27. Tätigkeitsbericht 2021, Abschnitt G 5, Seite 68

Wie bereits im letzten Tätigkeitsbericht dargestellt, stand meine Behörde bereits im Jahr 2021 auf Referentenebene mit dem Niedersächsischen Justizministerium im intensiven Austausch. Im Jahr 2022 erfolgten mehrere weitere Abstimmungen mit dem Niedersächsischen Justizministerium zum Referentenentwurf.

Erkennbare Orientierung am Datenschutz

Im darauffolgenden parlamentarischen Gesetzgebungsverfahren wurde meine Behörde schließlich Mitte 2022 im Rahmen der Verbandsbeteiligung zur schriftlichen Anhörung im Ausschuss für Rechts- und Verfassungsfragen des Niedersächsischen Landtags aufgefordert. Aufgrund des sehr konstruktiven vorangegangenen Austauschs zum Referentenentwurf musste ich lediglich wenige Empfehlungen geben. Diese bezogen sich insbesondere darauf, das Einwilligungserfordernis bei der Verarbeitung von Daten der Betroffenen durch den LfO an verschiedenen Stellen des Gesetzesentwurfs deutlicher herauszustellen.

Im in Kraft getretenen NLfOG sind verschiedene Änderungen des Gesetzentwurfs vorgenommen worden. So darf der LfO lediglich die Polizeibehörden um Übermittlung der Betroffenendaten ersuchen. Zuvor war eine „autonome“ Verpflichtung der Polizeibehörden gegenüber dem LfO zur Datenübermittlung vorgesehen. Auch war die Möglichkeit für den LfO enthalten, andere öffentliche sowie nicht-öffentliche Stellen um Auskunft zu ersuchen. Dies ist letztlich nicht in die aktuelle Fassung eingegangen. Die Verantwortlichkeit für eine Datenübermittlung der Polizei trägt nun die übermittelnde Polizeibehörde und nicht – wie zuvor vorgesehen – der LfO. Vor dem Hintergrund, dass die jeweils erforderliche Einwilligung der Betroffenen in die Datenverarbeitung von der Polizei eingeholt werden muss, erscheint diese klare Ausgestaltung sinnvoll.

Bedauerlicherweise wurde die ursprünglich vorgesehene und von mir angeregte Regelung zur Datenlöschung gestrichen. Diese sah vor, Daten Betroffener spätestens nach einem Jahr zu löschen, sofern die weitere Verarbeitung nicht für eine Beratung durch den LfO erforderlich war. Hierdurch sollte einer Datenverarbeitung über das erforderliche Maß hinaus mit einer eindeutigen Regelung begegnet werden.

Insgesamt ist das NLfOG in Anbetracht des gewählten Einwilligungserfordernisses für die Datenverarbeitung Betroffener deutlich erkennbar an den Maßgaben des Datenschutzes orientiert. Diese datenschutzfreundliche Ausgestaltung sowie die frühe und konstruktive Abstimmung im Vorfeld möchte ich ausdrücklich positiv hervorheben.

Die Opfer von Straftaten haben es selbst in der Hand, ob sie die Unterstützung des oder der LfO in Anspruch nehmen wollen. Eine „aufgedrängte" Hilfe unter Inkaufnahme eines behördenseitigen Eingriffs in das Recht auf informationelle Selbstbestimmung wird vermieden.

G.6. Änderung des Niedersächsischen Justizvollzugsgesetzes

Siehe 27. Tätigkeitsbericht 2021, Abschnitt G.3, Seite 65 folgende

Das novellierte Niedersächsische Justizvollzugsgesetz (NJVollzG) ist am 1. Juli 2022 in Kraft getreten. Im Rahmen des bereits seit dem Jahr 2018 laufenden Gesetzgebungsverfahrens hatte meine Behörde zu verschiedenen Stadien des Gesetzentwurfs Stellungnahmen abgegeben; zuletzt im Rahmen einer Anhörung gegenüber dem zuständigen Ausschuss des Landtages im Sommer 2021.

Im Jahr 2022 hat das parlamentarische Verfahren seinen Abschluss gefunden. Mit großem Interesse erwartet wurde der, aus datenschutzrechtlicher Sicht kritisch betrachtete, geplante umfassende Einsatz von künstlicher Intelligenz (KI) bei der Videoüberwachung in den Justizvollzugsanstalten. Konkret geplant war der Einsatz einer Video-KI zur Situationserkennung, um Suizide vermeiden zu helfen und die Sicherheit und Ordnung innerhalb der Anstalt aufrechtzuhalten.

Zunächst kein umfassender Einsatz von KI

In die aktuelle Gesetzesfassung hat dieser umfangreiche Einsatz von KI letztlich doch nicht Einzug gehalten. Dieser weite Anwendungsbereich war von mir im Rahmen der Anhörung scharf kritisiert worden. Er stellt sich als ein unverhältnismäßiger Eingriff in die Grundrechte der Gefangenen dar. Nunmehr ist positiv zu vermerken, dass eine „automatische Verarbeitung" von Bildübertragungen und -aufzeichnungen auf den eng begrenzten Zweck der Abwehr einer Lebensgefahr in besonders gesicherten Hafträumen beschränkt worden ist (Suizidprävention). Letzteres entspricht einer meiner Forderung im Rahmen der Anhörung. Diese begrenzte Zweckbestimmung wird dem Grundsatz der Verhältnismäßigkeit gerecht.

Die (normale) Videoüberwachung der Justizvollzugsanstalten oder – wie im Gesetzestext formuliert – die „Bildübertragungen und -aufzeichnungen mittels optisch-elektronischer Einrichtungen" wird nun in § 79 a NJVollzG geregelt. Positiv fällt dabei auf, dass die Überwachung auf bestimmte Bereiche der Anstalt mit Ausnahme von Hafträumen und medizinischen Behandlungsräumen beschränkt wurde. Zuvor war eine weitaus umfassendere Überwachung vorgesehen, die sich auf das Anstaltsgelände sowie das Innere der Anstaltsgebäude erstreckte. Lediglich im Rahmen der §§ 81, 81 a NJVollzG besteht die Möglichkeit, einzelne Gefangene im Rahmen einer besonderen Sicherungsmaßname in besonders dafür vorgesehenen Räumen oder besonders gesicherten Hafträumen zu beobachten.

Ob es im Laufe der jetzigen Legislaturperiode einen erneuten Vorstoß zur Erweiterung der aktuellen Regelung zum Einsatz von KI bei der Videoüberwachung in Justizvollzugsanstalten geben wird, bleibt abzuwarten.

H. Aufklärung und Öffentlichkeitsarbeit

H.1. „Autos und ihre Daten – so fährt die Zukunft“ – eine Veranstaltung der LfD Niedersachsen

Ein modernes Auto besteht aus viel mehr als aus Reifen, Karosserie und Motor. Es ist auf Wunsch des Kunden mit dem Internet verbunden, kommuniziert mit anderen Fahrzeugen und fährt bisweilen ganz ohne menschliches Zutun. Bei alledem generieren Fahrzeuge heute eine Menge Daten. In einem Symposium diskutierte ich mit Experten, welche Herausforderungen und Chancen daraus entstehen.

Im Vergleich zu anderen Debatten, die rund um das Automobil geführt werden, ist die Diskussion um Autos und ihre Daten noch vergleichsweise wenig emotionsgeladen. Dabei hat das Thema durchaus Sprengkraft: Durch den permanenten Datenstrom generiert ein Fahrzeug heute Datenmengen im Gigabyte-Maßstab. Mit der Weiterentwicklung hin zum autonomen und vernetzen Fahren wachsen die Datenmengen weiter. Damit ist das moderne Auto nicht mehr der Rückzugsort, an dem die Insassen noch ganz für sich sein können.

Daher war es aus meiner Sicht an der Zeit, mit Experten aus Forschung und Wirtschaft zu beleuchten, wie es um die Datenverarbeitung und den Datenschutz in modernen Fahrzeugen bestellt ist.

Denn längst wecken die Fahrzeugdaten Begehrlichkeiten bei den Automobilherstellern, Diensteanbietern und zahlreichen weiteren Akteuren: Die Palette reicht von Versicherern mit diversen Telematik-Tarifen und den Strafverfolgungsbehörden für die Rekonstruktion von Unfällen bis hin zu Content-Anbietern im Allgemeinen und Unternehmen mit vielfältigen Marketingzwecken.

Für den Datenschutz ist die aktuelle Entwicklung im Automobilsektor, wie überhaupt die gesamte Entwicklung zu mehr Digitalisierung, Connectivity und smarten Alltagsgegenständen eine große Herausforderung. Ohne Frage bieten die Daten, die durch das vernetzte und autonome Fahren entstehen, umfangreiche gesellschaftliche Chancen und Potenziale. Durch die Echtzeitauswertung von Verkehrsdaten können Fahrzeuge z. B. helfen, Staus zu vermeiden und die Steuerung freier Parkräume zu verbessern. Fahrassistenzsysteme machen den Straßenverkehr sicherer.

Aus meiner Sicht ist neben allen positiven Effekten auch Skepsis angebracht. Die transformierende Wirkung des „automatisierten Fahrens“ auf Technologie, Gesellschaft und Recht ist weder abschließend erfasst noch bewertet. Neben den Befürchtungen im Hinblick auf die Sicherheit und

Verlässlichkeit der Technik, der sich die Nutzer zunehmend ausliefern, gibt es zahlreiche rechtliche Fragen zu klären. Das können zivilrechtliche Haftungsfragen sein, die strafrechtliche Verantwortung und nicht zuletzt Fragen des Datenschutzes.

Der Datenschutz kommt immer dann als Regulativ ins Spiel, wenn personenbezogene oder personenbeziehbare Daten erhoben, übermittelt oder verarbeitet werden. Ist dies der Fall, müssen die entsprechenden Rechtsgrundlagen beachtet und die Grundsätze des Datenschutzes umgesetzt werden. Die Bewertung dieser Fragen und die Umsetzung der Anforderungen waren in der Vergangenheit nicht unumstritten und sind nach wie vor Gegenstand eines intensiven Austauschs der Datenschutzaufsichtsbehörden mit den Automobilherstellern und dem Verband der Automobilindustrie (VDA).

Das Symposium bot die Möglichkeit, das Thema aus unterschiedlichen Blickwinkeln zu betrachten. Während ich den Standpunkt des Datenschutzes aus Sicht der Aufsichtsbehörden beleuchtete, stellte der Konzerndatenschutzbeauftragte der Volkswagen AG, Dr. Oliver Draf, dar, wie Fahrzeughersteller den Datenschutz sicherstellen wollen.

Aus der wissenschaftlichen Perspektive heraus erläuterte Prof. Dr. Volker Lüdemann von der Hochschule Osnabrück den Teilnehmerinnen und Teilnehmern datenbasierte Geschäftsmodelle rund um das selbstfahrende Auto, wie sie inzwischen Internetkonzerne wie Google oder Apple verfolgen.

Bastian Lampe von der RWTH Aachen wagte zum Abschluss des Symposiums einen Blick auf die Technologien der Zukunft, bei denen Daten mehr denn je im Zentrum des automatisierten und vernetzten Fahrens stehen werden.

Ich selbst empfinde es als eine Bereicherung, dass Veranstaltungen vor Ort und der persönliche Kontakt und Austausch mit der Datenschutz-Community inzwischen wieder möglich sind. Besonders gefreut hat es mich daher, dass es mir noch im Jahr 2022 gelungen ist, selbst eine Veranstaltung zu einem Thema zu veranstalten, das den Datenschutz noch über Jahre hinaus umtreiben wird.

H.2. Vorträge der Landesdatenschutzbeauftragten

Nachdem ich meine ersten Vorträge im Jahr 2022 bedingt durch die Corona-Pandemie weiterhin online halten musste, entspannte sich die allgemeine Situation im weiteren Jahresverlauf. Glücklicherweise konnte ich wieder verstärkt vor Fachleuten sowie Zuhörerinnen und Zuhörern vor Ort vortragen und in den direkten Austausch gehen.

Ein Schwerpunkt meiner Vorträge lag gleich zum Jahresanfang 2022 auf dem neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), welches zum Ende des Jahres 2021 in Kraft getreten war und für einige Aufregung bei den Betreibern von Webseiten und Apps gesorgt hatte (siehe dazu auch J.7.3 ab S. 171). Der Grund war die nun vorgenommene europarechtskonforme Umsetzung der „Cookie-Regelung" der ePrivacy-Richtlinie. Der Einsatz von Cookies und anderen Trackingtechnologien sowie die Einbindung von Drittdiensten ist schon seit Jahren ein datenschutzrechtlicher Dauerbrenner. Daher hatten Verantwortliche und das Fachpublikum ein großes Interesse, Informationen und eine Einschätzung der Datenschutzaufsicht zum TTDSG zu erhalten.

Regeln zu Cookies und Tracking im TTDSG

Datenverarbeitung nach Schrems II

Wie bereits in den vorangegangenen zwei Jahren war auch die Datenverarbeitung nach Schrems II häufig ein Topthema in diversen Veranstaltungen. Bei mehreren Gelegenheiten konnte ich hierzu über die Fortsetzung meiner anlasslosen Kontrolle zur Umsetzung der Anforderungen des Schrems II-Urteils und die gewonnenen Erkenntnisse berichten (siehe dazu auch Kapitel D. ab S. 30). Die datenschutzkonforme Datenübermittlung in die USA wird als Thema sicherlich auch im Jahr 2023 erhalten bleiben, nachdem Mitte Dezember 2022 von der Europäischen Kommission ein Entwurf für einen neuen Angemessenheitsbeschluss für die USA veröffentlicht wurde.

Alle FAQ im Überblick: https://t1p.de/faq-ueberblick

Tätigkeiten der LfD und Bußgeldbemessung

Ebenfalls von großem Interesse waren 2022 die Vorstellung meiner aktuellen Tätigkeiten und hierbei insbesondere die von mir verhängten Bußgelder (siehe dazu auch Kapitel I.3. ab S. 99). In diesem Zusammenhang erläuterte ich bei verschiedenen Gelegenheiten auch das Konzept der Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (Datenschutzkonferenz, DSK) zur Bußgeldzumessung in Verfahren gegen Unternehmen. Dieses Thema wird perspektivisch noch wichtiger werden, da der Euro-

Symposium zum „Connected Car"

päische Datenschutzausschuss inzwischen eigene Leitlinien zur Berechnung von Geldbußen vorgestellt hat (siehe dazu Kapitel C.2., Seite 17). Dies wird sich auch auf meine Sanktionspraxis auswirken.

Die zum Jahresende zunehmend gelockerten Veranstaltungsauflagen nutzte ich zudem, um eigene Akzente in einem für den Datenschutz zunehmend wichtigen Feld zu setzen: Der vernetzten Mobilität. In einem Symposium „Autos und ihre Daten – so fährt die Zukunft" brachte ich Fachleute und Fachpublikum in Hannover zusammen, um gemeinsam die Chancen und Herausforderungen zu diskutieren, die sich aus den Datenschätzen ergeben, die von modernen Fahrzeugen generiert werden (siehe dazu auch H.1. ab S. 84).
Dabei hat sich gezeigt, wie wichtig bei allen technischen Meeting-Möglichkeiten auch der direkte fachliche Austausch ist und bleibt. Er ist meiner Ansicht nach unabdingbar dafür, die Belange des Datenschutzes nachdrücklich und nachvollziehbar zu kommunizieren.

H.3. Veröffentlichung von Informationsmaterial

Wie in den vergangenen Jahren auch habe ich mit der Bereitstellung von Informationsmaterialien auf aktuelle Ereignisse, Themen oder Anregungen reagiert, um den Informationsbedürfnissen von Verantwortlichen sowie Bürgerinnen und Bürgern gerecht zu werden. Eine Auswahl wichtiger Veröffentlichungen stelle ich an dieser Stelle vor.

Eckpunktepapier zum Einsatz digitaler Lernplattformen

Nicht erst seit den massiven Einschränkungen des Unterrichts durch die Corona-Pandemie werden an den niedersächsischen Schulen digitale Lernplattformen eingesetzt. Dieser Trend hat sich durch die Pandemie jedoch deutlich beschleunigt. Durch die Bereitstellung und Organisation digitaler Lerninhalte werden oftmals vielfältige elektronische Kommunikationsmöglichkeiten zwischen den Lernenden und Lehrenden eröffnet. Dabei wird eine Vielzahl von personenbezogenen Daten der Schülerinnen und Schüler verarbeitet. Aus diesem Grund habe ich ein Eckpunktepapier für den datenschutzkonformen Einsatz von digitalen Lernplattformen in den niedersächsischen Schulen veröffentlicht. Darin gebe ich u. a. Informationen, wie das Gebot der Datensparsamkeit umgesetzt werden kann, wie eine Auftragsverarbeitung ausgestaltet werden sollte, und wie geeignete technisch-organisatorische Maßnahmen bei der Nutzung digitaler Lernplattformen umgesetzt werden.

Eckpunktepapier zum Download (Kurzlink): https://t1p.de/Eckpunkte-Lernplattformen

Gestaltung von Consent-Layern auf Webseiten

Wenn wir das Internet nutzen begegnen uns mittlerweile vermehrt aufwändige Consent-Fenster (auch Consent-Banner oder Consent-Layer genannt), die Nutzerinnen und Nutzern erstens detaillierte Informationen über den Einsatz von Cookies und die Einbindung von Drittdiensten und zweitens echte Entscheidungs- und Wahlmöglichkeiten geben. Entsprechend aufwändiger ist die Gestaltung und die Umsetzung von Consent-Layern geworden. In einer Handreichung habe ich daher zusammengefasst, welche Anforderungen an die datenschutzkonforme Gestaltung von Consent-Layern gestellt werden.

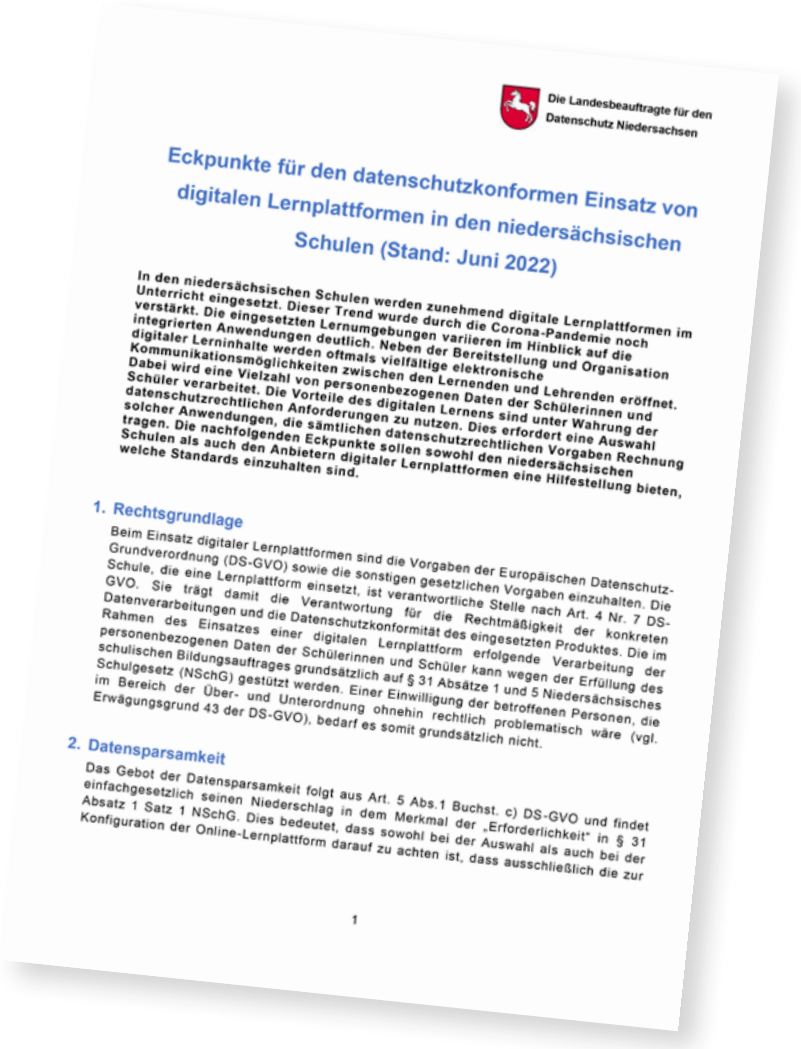
Handreichung zu Consent-Layern als Download (Kurzlink): https://t1p.de/HandreichungConsent-Layer

Hinweise zur Datenverarbeitung im Krankheitsfall

Über eine bevorstehende Änderung der rechtlichen Grundlagen für die Vorlage von Arbeitsunfähigkeitsbescheinigungen von Arbeitnehmerinnen und

Hinweise zum Download (Kurzlink): https://t1p.de/HinweiseDatenverarbeitungImKrankheitsfall

Arbeitnehmern im Krankheitsfall zum 1. Januar 2023 habe ich mit umfangreichen Hinweisen informiert. Denn im Rahmen des Prüfverfahrens zur Feststellung der Arbeitsunfähigkeit sowie zur Festsetzung der Entgeltfortzahlung im Krankheitsfall werden sowohl personenbezogene Daten der Beschäftigten wie zum Beispiel Kontaktdaten der Betroffenen oder nähere Informationen zu deren Krankenversicherung (gesetzlich oder privat), als auch besondere Kategorien von personenbezogenen Daten wie Gesundheitsdaten verarbeitet. Die Hinweise sollen sowohl Verantwortlichen als auch den Betroffenen einen Überblick verschaffen, welche datenschutzrechtlichen Vorgaben zu beachten sind.



Die Landesbeauftragte für den Datenschutz Niedersachsen

Eckpunkte für den datenschutzkonformen Einsatz von digitalen Lernplattformen in den niedersächsischen Schulen (Stand: Juni 2022)

In den niedersächsischen Schulen werden zunehmend digitale Lernplattformen im Unterricht eingesetzt. Dieser Trend wurde durch die Corona-Pandemie noch verstärkt. Die eingesetzten Lernumgebungen variieren im Hinblick auf die integrierten Anwendungen deutlich. Neben der Bereitstellung und Organisation digitaler Lerninhalte werden oftmals vielfältige elektronische Kommunikationsmöglichkeiten zwischen den Lernenden und Lehrenden eröffnet. Dabei wird eine Vielzahl von personenbezogenen Daten der Schülerinnen und Schüler verarbeitet. Die Vorteile des digitalen Lernens sind unter Wahrung der datenschutzrechtlichen Anforderungen zu nutzen. Dies erfordert eine Auswahl solcher Anwendungen, die sämtlichen datenschutzrechtlichen Vorgaben Rechnung tragen. Die nachfolgenden Eckpunkte sollen sowohl den niedersächsischen Schulen als auch den Anbietern digitaler Lernplattformen eine Hilfestellung bieten, welche Standards einzuhalten sind.

1. Rechtsgrundlage

Beim Einsatz digitaler Lernplattformen sind die Vorgaben der Europäischen Datenschutz-Grundverordnung (DS-GVO) sowie die sonstigen gesetzlichen Vorgaben einzuhalten. Die Schule, die eine Lernplattform einsetzt, ist verantwortliche Stelle nach Art. 4 Nr. 7 DS-GVO. Sie trägt damit die Verantwortung für die Rechtmäßigkeit der konkreten Datenverarbeitungen und die Datenschutzkonformität des eingesetzten Produktes. Die im Rahmen des Einsatzes einer digitalen Lernplattform erfolgende Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler kann wegen der Erfüllung des schulischen Bildungsauftrages grundsätzlich auf § 31 Absätze 1 und 5 Niedersächsisches Schulgesetz (NSchG) gestützt werden. Einer Einwilligung der betroffenen Personen, die im Bereich der Über- und Unterordnung ohnehin rechtlich problematisch wäre (vgl. Erwägungsgrund 43 der DS-GVO), bedarf es somit grundsätzlich nicht.

2. Datensparsamkeit

Das Gebot der Datensparsamkeit folgt aus Art. 5 Abs.1 Buchst. c) DS-GVO und findet einfachgesetzlich seinen Niederschlag in dem Merkmal der „Erforderlichkeit" in § 31 Absatz 1 Satz 1 NSchG. Dies bedeutet, dass sowohl bei der Auswahl als auch bei der Konfiguration der Online-Lernplattform darauf zu achten ist, dass ausschließlich die zur

1

H.4. Datenschutzinstitut – Fortbildung auf hohem Niveau

Bereits seit vielen Jahren bietet das Datenschutzinstitut Niedersachsen (DsIN) meiner Behörde verschiedene Schulungen für Datenschutzbeauftragte im öffentlichen Bereich an. Im Jahr 2022 wurden Schulungen sowohl im Online-Format als auch in Präsenz durchgeführt und erstmalig auch eine Schulung zum Beschäftigtendatenschutz für Teilnehmende aus Unternehmen durchgeführt.

Im Jahr 2022 wurden die unter den Bedingungen der Pandemie eingeführten Online-Schulungsangebote weiter fortgesetzt und fanden regen Zuspruch. Das Online-Format bietet dabei für die Teilnehmenden und Dozenten durchaus Vorteile, die insbesondere in der Verringerung von Reisezeiten und einer potenziell größeren Reichweite der Veranstaltung zu sehen sind. Als besonderen Erfolg werte ich die neu von mir ins Programm aufgenommene Grundlagenschulung zu „Datenschutz im Verein". Ziel dieses Angebotes ist es, den meist ehrenamtlich tätigen Amtsträgern datenschutzrechtliches Grundlagenwissen für die Arbeit im Verein zu vermitteln. Um die unmittelbare praktische Anwendbarkeit der Inhalte zu gewährleisten, werden typische Beispiele aus dem Vereinsleben besprochen. Mit über 30 Teilnehmenden war die Veranstaltung ausgebucht. Umfang und Themenauswahl stießen auf durchweg positive Resonanz und somit habe ich die Schulung als festen Bestandteil in das Jahresprogramm unseres Schulungsinstitutes aufgenommen.

Eine weitere Neuerung war ein Kursangebot zum Thema „Grundlagen des Beschäftigtendatenschutzes". Der Kurs richtete sich an Mitarbeitende und Verantwortliche aus kleinen und mittleren Unternehmen (KMU), da aus dem Bereich KMU häufig Beratungsanfragen zum Beschäftigtendatenschutz an mich gerichtet werden. Es ist mir naturgemäß nicht immer möglich, in solchen Einzelfällen eine umfassende Beratung anzubieten. Die Resonanz auf dieses besondere Schulungsangebot war ausgesprochen gut. Insgesamt 17 Teilnehmende von niedersächsischen KMU nahmen an dem neuen Kursangebot teil.

Nicht alle Seminarinhalte sind gleichermaßen für das Online-Format geeignet und so wurden im Rahmen der Möglichkeiten, die die pandemische Lage eröffnet hat, auch wieder Schulungen in Präsenz durchgeführt. Dies betraf zum Beispiel den Kurs zu datenschutzfreundlichen Technologien und technisch-organisatorischen Maßnahmen, der mit praktischem Anschauungsmaterial arbeitet.

In der Gesamtschau wurde so das Angebot des Datenschutzinstitutes nochmals deutlich flexibler und in seiner neuen Vielfalt gefestigt. Dem Auftrag der DS-GVO, neben Aufsicht und Kontrolle auch Beratung, Aufklärung und Information zu gewährleisten, kann meine Behörde damit in besonderer Weise Rechnung tragen.

H.5. Veröffentlichung von personenbezogenen Daten im Internet wegen persönlicher Streitigkeiten

Im Berichtszeitraum war ein deutlicher Trend zur Veröffentlichung von personenbezogenen Daten nach der Eskalation von Auseinandersetzungen zwischen Konfliktparteien im Internet zu beobachten. Dies zeigt sich an zahlreichen Beschwerden Betroffener, die Beiträge auf Bewertungsportalen, Social-Media-Kanälen oder privaten Blogs beanstandeten. Grundsätzlich hat der Verantwortliche bei der Veröffentlichung von personenbezogenen Daten eine Rechtsgrundlage dafür nachzuweisen und den Verhältnismäßigkeitsgrundsatz einzuhalten.

Die vielseitigen Beschwerdesachverhalte richteten sich etwa gegen Unternehmensinhaber, welche auf vermeintlich unzutreffende Kundenbewertungen mit der Veröffentlichung der Kontaktdaten des jeweiligen Kunden auf Rezensionsplattformen reagiert hatten. In Einzelfällen veröffentlichten Bürger aus Unzufriedenheit mit der Arbeit öffentlicher Stellen vollständige Verfahrensakten von Gerichten oder Behörden, aus welchen sich Namen und Kontaktdaten zahlreicher Beteiligter entnehmen ließen.

Informationsschreiben abrufbar unter (Kurzlink): https://t1p.de/digitaleRacheakte

Die rechtlichen Überprüfungen haben ergeben, dass in den häufigsten Fällen keine Rechtsgrundlage für die Veröffentlichung der Datensätze vorlag und gegen die DS-GVO verstoßen worden ist.

Vor dem Hintergrund dieser Entwicklung habe ich ein Informationsschreiben auf meiner Webseite veröffentlicht, welches u. a. auf die Notwendigkeit einer Rechtsgrundlage für die Veröffentlichung von personenbezogenen Daten im Internet hinweist. Ich möchte auf diesem Weg zur Sensibilisierung der Öffentlichkeit sowie zur Vermeidung der beschriebenen Datenschutzverstöße beitragen.

I. Aufsicht und Vollzug

I.1. Zahlen und Fakten

Um einen schnellen Überblick über die Arbeit meiner Behörde zu ermöglichen, veröffentliche ich an dieser Stelle ausgewählte statistische Werte und Kennzahlen. Dies soll dazu beitragen, meine Tätigkeit transparent zu machen. Allerdings ist damit keine Aussage über die qualitative Ausprägung der hier aufgeführten Aufgabenbereiche getroffen.

Beschwerden

Die Zahl der Beschwerden gemäß Art. 77 DS-GVO ging mit 2058 im Jahr 2022 um 480 Fälle leicht zurück. Ob damit die bereits im Jahr 2022 erhoffte Verstetigung auf einem hohen Niveau erreicht ist, wird sich meiner Meinung nach erst mit Ablauf des Jahres 2023 bewerten lassen. Zudem muss ich betonen, dass dieser geringfügige Rückgang kaum eine spürbare Entlastung im Tagesgeschäft meiner Behörde bedeutet.

Gemeldete Datenschutzverletzungen

Die gemäß Art. 33 DS-GVO gemeldeten Datenschutzverletzungen sind 2022, und damit erstmals seit Geltung der DS-GVO, im Vorjahresvergleich zurückgegangen. Die Zahl sank um 524 Meldungen auf eine Gesamtzahl von 1149. Für den Rückgang in diesem Bereich gibt es eine relativ einfache Erklärung: 2021 erreichten mich knapp 500 Meldungen zu Sicherheitslücken in Microsoft Exchange Servern (sogenannter Hafnium Hack), die 2022 keine Rolle mehr gespielt haben. Lässt man diese Meldungen unbeachtet, ist die Zahl der übrigen Meldungen zwischen 2021 und 2022 auf fast demselben Niveau geblieben.

Abhilfemaßnahmen nach DS-GVO

Ich habe im Jahr 2022 90 Warnungen (Art. 58, Abs. 2 lit. a DS-GVO), 9 Anweisungen und Anordnungen (Art. 58, Abs. 2 lit. c-h und j) sowie 305 Verwarnungen (Art. 58, Abs. 2 lit. b DS-GVO) ausgesprochen. Zudem habe ich 51 Bußgeldbescheide erlassen (siehe I.3, S. 99). Die Gesamthöhe der verhängten Bußgelder betrug rund 2,2 Millionen Euro.

Gerichtsverfahren

Insgesamt wurden im vergangenen Jahr 23 neue Klage- und Antragsverfahren eröffnet, in denen meine Behörde Partei war. In knapp der Hälfte der Fälle (10) wurde dabei die Abweisung einer Beschwerde moniert. Zudem wurden in 12 Fällen meine Abhilfemaßnahmen angefochten.

Entschieden wurden im Berichtszeitraum 10 Klage- und Antragsverfahren, in 5 Fällen wurden Klagen und Anträge zurückgenommen, genauso oft wurden sie als unbegründet abgelehnt.

Beratungen

Im Jahr 2022 erreichten mich knapp 1.000 schriftliche Beratungsanfragen (per Post oder E-Mail), was gegenüber dem Vorjahr einem Rückgang um rund 600 Anfragen entspricht. Meine Mitarbeiterinnen und Mitarbeiter bemühen sich weiterhin auch in konkreten Einzelfällen Unterstützung zu leisten, wann immer es ihre Zeit zulässt. Leider ist das aufgrund der nach wie vor dünnen Personaldecke meines Hauses nicht immer möglich.

Europäische Verfahren

Im Jahr 2022 war mein Haus in folgendem Umfang mit europäischen Verfahren befasst:

1. Verfahren mit Betroffenheit (Art. 56): 91 Fälle
2. Verfahren mit Federführung (Art. 56): 3 Fälle
3. Verfahrensschritte gem. Kap VII DS-GVO (Art. 60 ff.):
   a. Die LfD hat als betroffene Aufsichtsbehörde einen Beschlussentwurf erhalten: 249 Fälle
      Die LfD hat als betroffene Aufsichtsbehörde einen überarbeiteten Beschlussentwurf erhalten: 13 Fälle
   b. Der LfD wurde als betroffener Aufsichtsbehörde ein finaler Beschlussentwurf vorgelegt: 211 Fälle
   c. Verfahren mit Federführung (Art. 60): 2 Fälle

Ressourcen der Behörde

Jahr	Budget in Tsd. Euro	Beschäftigungsvolumen
2017	3.581	45,25
2018	3.917	50,25
2019	4.117	51,17
2020	4.271	53,17
2021	4.381	56,17
2022	4.381	56,17

I.2. Beschwerden und Meldungen von Datenschutzverletzungen

Erstmals seit Geltung der Datenschutz-Grundverordnung (DS-GVO) ist die Zahl der Beschwerden und der Meldungen von Datenschutzverletzungen im Vorjahresvergleich nicht weiter gestiegen. Bei den Beschwerden ist sogar ein leichter Rückgang zu verzeichnen. Dennoch liegen die Zahlen weiterhin auf einem hohen Niveau, wobei die Gründe für Beschwerden und die Auslöser von Datenschutzverletzungen auch im zurückliegenden Jahr wieder vielfältig waren.

Die Zahl der Beschwerden gemäß Art. 77 DS-GVO ging mit 2058 im Jahr 2022 um 480 Fälle leicht zurück. Ob damit die bereits im Jahr 2022 erhoffte Verstetigung auf einem hohen Niveau erreicht ist, wird sich meiner Meinung nach erst mit Ablauf des Jahres 2023 bewerten lassen. Zudem muss ich betonen, dass dieser geringfügige Rückgang kaum eine spürbare Entlastung im Tagesgeschäft meiner Behörde bedeutet.

Schwerpunkte von Beschwerden

Videoüberwachung

Die Videoüberwachung blieb, wie schon in den Vorjahren, auch im Jahr 2022 ein Dauerthema. Sowohl im privaten Bereich wie auch beim Einsatz durch Unternehmen erhielt ich erneut zahlreiche Beschwerden wegen unzulässiger Videoüberwachungen. Im privaten Bereich lag der Schwerpunkt dabei auf der Überwachung der Nachbarschaft, teilweise verbunden mit der unzulässigen Überwachung des öffentlichen bzw. gemeinschaftlich genutzten Raumes.

Im Bereich der Videoüberwachung durch Unternehmen war oftmals eine unzureichende oder gänzlich fehlende Kennzeichnung der Auslöser für Beschwerden.

Aus der Menge der Beschwerden im unternehmerischen Bereich stechen zwei Fälle besonders heraus, in denen Fahrschulen rechtswidrig Fahrstunden mit Bild und Ton im Internet gestreamt haben (siehe J. 8.3., S. 179).

Für den Austausch mit Unternehmen muss ich feststellen, dass sich die Zusammenarbeit verschlechtert hat. Verantwortliche äußern sich oft aggressiv in ihrer Wortwahl. Der Wille, eine datenschutzkonforme Ausgestaltung einer Videoüberwachung zu erreichen, nimmt ab. In der Vergangenheit hat sich die

Hinzuziehung einer anwaltlichen Vertretung oft positiv ausgewirkt, da bestenfalls von deren Seite die Rechtsauffassung der LfD bestärkt wurde, zumindest aber der Verantwortliche bei der Erfüllung der ihm obliegenden Verpflichtungen unterstützt wurde. Mittlerweile entwickeln aber auch die Rechtsanwälte eine zunehmende Verweigerungshaltung, auch bereits auf die Bitte um Auskunftserteilung. Auskünfte werden auch nach gewährter Fristverlängerung und Erinnerung zum Teil nur unvollständig erteilt. Der Aufwand für die Fallbearbeitung wird dadurch deutlich erhöht.

Auskunft, ein schwieriges Unterfangen

Im Bereich der Betroffenenrechte bezogen sich erneut zahlreiche Beschwerden auf das Auskunftsrecht gemäß Art. 15 DS-GVO. Betroffen hiervon waren alle Bereiche im öffentlichen und nicht-öffentlichen Bereich. Auch war das Recht auf Auskunft erneut Gegenstand einer höchstrichterlichen Befassung (siehe F.3., S. 62).

In vielen Fällen, die einer Beschwerde im nicht-öffentlichen Bereich zugrunde lagen, wurde auf eine Bitte um Auskunft durch das verantwortliche Unternehmen nicht reagiert oder die Auskunft ist unvollständig gewesen. So beobachte ich, dass Verarbeitungszwecke und/oder Datenweiterleitungen nur formelhaft benannt werden, aber letztlich dazu entgegen Art. 15 DS-GVO keine Auskunft gegeben wird. Vielfach genügte in den Fällen der fehlenden Antwort ein Hinweis meiner Behörde an das verantwortliche Unternehmen, damit das Auskunftsbegehren beantwortet wurde.

Ungeachtet dessen hatten betroffene Personen in einigen Fällen falsche Vorstellungen von den Betroffenenrechten. So versuchen immer wieder betroffene Personen bei zivilrechtlichen Streitigkeiten um den Ausgleich einer Zahlungsforderung das Recht auf Löschung nach Art. 17 DS-GVO geltend zu machen, um der Forderung zu entgehen. Sie übersehen dabei jedoch, dass das Recht auf Löschung erst dann besteht, wenn die Voraussetzungen von Art. 17 Abs. 1 DS-GVO erfüllt sind. So besteht das Recht dann nicht, wenn die personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind, weshalb solche Beschwerden im Regelfall erfolglos sind.

Dauerärgernis Werbung

Werbepost von unbekannten Unternehmen

Auch im Jahr 2022 ist Werbung ein Dauerärgernis für Bürgerinnen und Bürger gewesen. So haben vor allem Newsletter sowie persönlich gestaltete Werbeanschreiben von Unternehmen, zu denen die betroffenen Personen keinen Geschäftskontakt hatten, zu Beschwerden geführt. Dies vor allem in den Fällen, bei denen die Unternehmen auf Anfrage der betroffenen Person nicht darlegen konnten, von wem sie die (E-Mail-)Adresse erhalten haben. Vielfach wurden die Bürgerinnen und Bürger, die ihr Recht auf Auskunft nach Art. 15 DS-GVO gegenüber dem werbenden Unternehmen geltend gemacht haben,

diesbezüglich an andere Unternehmen verwiesen. Auffällig ist, dass die Unternehmen häufig ihren Sitz außerhalb der EU haben und letztlich die Herkunft der Adressdaten nicht aufklärbar ist. Gegen Unternehmen mit ungewöhnlich hohem Beschwerdeaufkommen habe ich Verfahren eingeleitet und die Sachverhalte näher untersucht. Soweit die Untersuchungen abgeschlossen werden konnten, habe ich in einigen Verfahren Verstöße gegen die DS-GVO festgestellt und Maßnahmen nach Art. 58 Abs. 2 DS-GVO ergriffen. Dabei fällt auf, dass teilweise mehrere Unternehmen involviert sind und in diesen Fällen der Verlauf der personenbezogenen Daten und die datenschutzrechtliche Beurteilung der Verantwortlichkeit sowie der Datenverarbeitung sich sehr aufwändig gestalten. Ein Teil der Untersuchungen konnte im Jahr 2022 noch nicht abgeschlossen werden.

Darüber hinaus erreichen mich im Bereich der Werbung weiterhin viele Beschwerden, denen die Nichtbeachtung von Werbewidersprüchen zugrunde liegt. In diesen Fällen genügt zumeist ein Hinweis auf die Rechtslage an das Unternehmen, um Abhilfe zu schaffen.

Neugierige Beschäftigte

Im Jahr 2022 konnte ich einen Anstieg von Beschwerden, aber vor allem von Datenpannenmeldungen beobachten, denen eine Kompetenzüberschreitung der beschäftigten Person, ein sogenannter Mitarbeiterexzess, zugrunde lag. Immer wieder können offenbar beschäftigte Personen dem „Angebot" an personenbezogenen Daten Dritter bei ihrem Unternehmen nicht widerstehen und sehen diese ein, obwohl die Daten keinen Bezug zu ihrem Tätigkeitsfeld haben. In diesen Fällen ist regelmäßig bereits ein Verstoß der beschäftigten Person gegen die organisatorischen Maßnahmen des verantwortlichen Unternehmens gegeben. Schwerer wiegen jedoch die Fälle, bei denen die personenbezogenen Daten verwendet oder sogar gegenüber weiteren Personen offenbart werden. Hier fehlt es an einem datenschutzrechtlichen Bewusstsein. Die Rechtswidrigkeit ihres Handelns wird den beschäftigten Personen vielfach erst im Nachgang bewusst, wenn Maßnahmen des Arbeitgebers und/oder meiner Behörde drohen oder ergriffen werden. Richtig ist in diesen Fällen, dass Unternehmen bei einem sogenannten Mitarbeiterexzess von einer Datenpanne im Sinne von Art. 33 DS-GVO ausgehen und diese entsprechend meiner Behörde melden.

Schwerpunkt der Meldung von Datenschutverletzungen

Eine Datenschutzverletzung, die ein Risiko für die Rechte und Freiheiten der Betroffenen bedeuten könnte, muss durch Verantwortliche innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden. So schreibt es Art. 33 der DS-GVO vor. Auch in diesem Bereich konnte ich im Jahr 2022, zumindest auf den ersten Blick, einen leichten Rückgang der Meldezahlen verzeichnen, und zwar um 524 Meldungen auf eine Gesamtzahl von 1149. Für den Rückgang in diesem Bereich gibt es eine relativ einfache Erklärung. 2021 erreichten die LfD knapp 500 Meldungen zu Sicherheitslücken in Microsoft Exchange Servern (sogenannter Hafnium Hack), die 2022 keine Rolle mehr gespielt haben. Lässt man diese unberücksichtigt, ist die Zahl der übrigen Meldungen 2021 und 2022 annähernd gleichgeblieben.

Offenlegung von Mitarbeiterdaten

Im Bereich des Beschäftigtendatenschutzes meldeten mir etliche Verantwortliche im öffentlichen und nicht-öffentlichen Sektor die unzulässige Offenlegung von Daten ihrer Mitarbeiterinnen und Mitarbeitern gegenüber unbefugten Dritten durch Fehlversand, Verlust oder auch Diebstahl. Die zahlreichen Negativbeispiele im Bereich des Beschäftigtendatenschutzes geben der Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (kurz Datenschutzkonferenz, DSK) Anlass zu zunehmender Besorgnis. Aus diesem Grund hat die DSK die Schaffung eines Beschäftigtendatenschutzgesetzes gefordert (Siehe E.3., S. 39).

Ransomeware und kein Ende

Die Anzahl an Datenpannenmeldungen wegen Ransomware-Angriffen auf IT-Netze von Unternehmen hat im vergangenen Jahr zugenommen. Hier zeigt sich eine der augenfälligsten Verschränkungen zwischen Datenschutz und IT-Sicherheit. Es werden zumindest die Daten auf den Rechnern verschlüsselt, sodass auf sie nicht mehr zugegriffen werden kann. Alternativ oder zusätzlich werden Daten und damit auch personenbezogene Daten ausgeleitet. Diese Taten sind als Diebstahl zu werten.

Dabei sind die Angriffsszenarien unterschiedlich, neben der Ausnutzung von Softwarelücken sind es vielfach sogenannte Phishing-Mails, die den Angreifern den Zugang zum dem IT-Netz ermöglichen.

Auch wenn eine IT-Sicherheit nicht vollständig gewährleistet werden kann, sollten gleichwohl vor allem die IT-Systeme aktuell und ein Backup-System vorhanden sein. Ein wirksamer Schutz ist zudem die Verschlüsselung der Daten durch das Unternehmen selbst. Weiter müssen die Beschäftigten wiederholt geschult werden. Und im Falle eines Falles sollten die Geschäftspartner und Kunden informiert werden. In verschiedenen Fällen sind die erbeuteten Daten u. a. für die Erstellung von falschen Rechnungen und/oder die Generierung neuer Phishing-Mails für Angriffe auf die IT-Systeme von Geschäftspartnern und Kunden verwendet worden. Diese Mails sehen häufig täuschend echt aus und nehmen Bezug auf bisherigen Mailverkehr oder bestehende Aufträge. So werden unaufmerksame Empfänger schnell dazu verleitet, auf einen Link in der Mail zu klicken oder einen Anhang zu öffnen, wodurch Malware auf den Rechner gelangt. Dies birgt nicht nur erhebliche Risiken für personenbezogene Daten, sondern kann auch Geschäfts- und Kundenbeziehungen nachhaltig stören.

I.3. Überblick über bearbeitete Bußgeldverfahren

Im Jahr 2022 habe ich Bußgelder in Höhe von rund 2,2 Millionen Euro verhängt, die überwiegend auf zwei ausgesprochene Einzelfälle zurückzuführen sind. Die Mehrzahl der verhängten Geldbußen betraf erneut die unzulässige Videoüberwachung.

Im Jahr 2022 habe ich insgesamt 97 neue Fälle auf eine mögliche Geldbuße geprüft. Im gleichen Zeitraum habe ich 51 Erstbescheide in Bußgeldsachen erlassen, die sich zum Teil auf Fälle bezogen, die bereits in den Vorjahren eingeleitet wurden. Von diesen Bescheiden sind 45 rechtskräftig geworden, da die Adressaten entweder keinen Einspruch eingelegt haben oder weil sie ihre Einsprüche vor einer Sachentscheidung des Gerichts zurückgenommen haben. Die nicht mit Bußgeldern abgeschlossenen Verfahren sind entweder anhängig, waren nicht bußgeldwürdig, wurden eingestellt oder wurden an andere zuständige Stellen abgegeben.

Höhe und Adressaten von Geldbußen

Mit Erstbescheiden wurden Geldbußen in Höhe von rund 2,2 Millionen Euro festgesetzt. Die Bescheide wurden gegenüber Verantwortlichen aus den Bereichen Gastgewerbe, Handel, Industrie, Finanzdienstleistungen, sonstige Dienstleister sowie gegen natürliche Personen erlassen. Die natürlichen Personen haben die Verstöße teilweise als Inhaberinnen bzw. Inhaber von Unternehmen begangen.

Geahndet wurden Verstöße gegen die Artikel 5, 6, 10, 13, 14, 15, 17, 21, 25, 28, 30, 32, 35 sowie 83 Abs. 5 lit. e Datenschutz-Grundverordnung (DS-GVO) und § 26 Bundesdatenschutzgesetz (BDSG). Dabei handelte es sich um Verstöße gegen

- die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage,
- die Informations-, Auskunfts- und Löschpflicht,
- die Pflicht zur Beachtung von Widersprüchen gegen die Verarbeitung,
- die Pflicht zum Abschluss von Auftragsverarbeitungsverträgen,
- die Führung bzw. Vorlage von Verzeichnissen der Verarbeitungstätigkeit,
- technische Maßnahmen,
- Anfertigungspflicht einer Datenschutzfolgenabschätzung sowie gegen
- behördliche Anweisungen.

Gerichtliche Entscheidungen

Im Jahr 2022 wurden durch die Gerichte neun Entscheidungen zu Bußgeldverfahren getroffen. Die Bußgeldadressaten haben die Verstöße in der Sache überwiegend eingeräumt und ihre Einsprüche zumeist auf die Rechtsfolgenseite beschränkt. Bei solch einer Beschränkung wird die Feststellung des Verstoßes durch meine Behörde unmittelbar rechtskräftig, sodass das Gericht nur noch über die Höhe der Geldbuße zu entscheiden hat. Zwei Einsprüche wurden zurückgenommen, bevor es zu einer gerichtlichen Entscheidung in der Sache kommen konnte.

Weitere gerichtliche Entscheidungen wegen Bußgeldbescheiden meiner Behörde werden für das Jahr 2023 erwartet.

Einzelne Fallkonstellationen

Europäische Zusammenarbeit

In einem Fall hatte ich über die Festsetzung einer Geldbuße als federführende Aufsichtsbehörde im Kooperationsverfahren nach Art. 60 DS-GVO zu entscheiden. In einem anderen Mitgliedstaat der Europäischen Union war den dortigen Behörden ein Fahrzeug mit Kameratechnik aufgefallen. Bei meiner Untersuchung habe ich festgestellt, dass die datenschutzrechtlich Betroffenen nicht informiert wurden, dass ein erforderlicher Auftragsverarbeitungsvertrag nicht geschlossen worden war, dass die technischen und organisatorischen Schutzmaßnahmen nicht im Verzeichnis der Verarbeitung erläutert wurden und dass die notwendige Datenschutzfolgenabschätzung nicht erfolgt war. Nach Abschluss des europäischen Verfahrens über die Zusammenarbeit habe ich eine Geldbuße in Höhe von 1.100.000 Euro für die vier Verstöße festgesetzt. Das Unternehmen hat den Bußgeldbescheid akzeptiert.

Profilbildung zu Werbezwecken

Ein Kreditinstitut hat vorhandene personenbezogene Daten aktiver und ehemaliger Kundinnen und Kunden ausgewertet und deren digitales Nutzungsverhalten analysiert. Ziel war es, Kundinnen und Kunden mit einer erhöhten Neigung für digitale Medien zu identifizieren und diese adressatengerecht für vertragsrelevante oder werbliche Zwecke verstärkt auf elektronischen Kommunikationswegen anzusprechen. Die mit dieser Auswertung verbundene Zweckänderung und der konkrete Umfang der Auswertung war von den Kundinnen und Kunden vernünftigerweise nicht zu erwarten. Das Unternehmen konnte sich daher nicht auf Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage stützen. Ich habe eine Geldbuße in Höhe von 900.000 Euro festgesetzt, die inzwischen rechtskräftig ist.

Übermittlung von Krankentagen an Führungskräfte

Kenntnis nicht erforderlich

Anlässlich einer jährlichen Beurteilung wurde vom Personalbereich eines Unternehmens eine Liste von Beschäftigten zusammengestellt, die auffällig viele Krankheitstage bzw. Kurzerkrankungen über mehrere Kalenderjahre aufwiesen. Da vor allem ständige Kurzerkrankungen den betrieblichen Ablauf erheblich störten, wurde erwogen, solchen Beschäftigten bestimmte freiwillige Zulagen ggf. nicht mehr zu gewähren. Die eigentliche Auswertung durch den Personalbereich war nicht zu beanstanden, da sie auch für andere – zulässige – arbeitsrechtliche Maßnahmen nötig gewesen wäre. Unzulässig war, dass die Liste mit Namen und Krankheitstagen per E-Mail an einen Verteiler aller höherrangigen Führungskräften versendet wurde. Die Empfänger erhielten damit Kenntnis davon, welche Beschäftigten in fremden Bereichen in diese Gruppe fielen, ohne dass diese Kenntnis erforderlich im Sinne von § 26 Abs. 1 Satz 1 BDSG gewesen wäre. Wegen dieser unzulässigen Übermittlungen habe ich im Jahr 2022 eine Geldbuße in Höhe von 25.000 Euro festgesetzt, die akzeptiert wurde.

Unzureichende technische Maßnahmen

Newsletter und Betroffenenrechte

Einem im Jahr 2022 sanktionierten Fall lag eine technische Störung zugrunde. Ein Unternehmen betrieb ein E-Mail-Newslettersystem, das über einen relevanten Zeitraum keine Abmeldungen zuließ. Da das Unternehmen Newsletter in relativ hoher Frequenz versendet hatte, führte dies bei einzelnen datenschutzrechtlich Betroffenen zu einer erheblichen Zahl unerwünschter E-Mails. Einige Betroffene versuchten sich durch Geltendmachung ihrer Betroffenenrechte auf anderem Wege zu helfen. Abmeldungen vom Newsletter über Service-Mitarbeitende des Unternehmens waren allerdings ebenfalls erfolglos, sodass Werbewidersprüche im Ergebnis nicht beachtet wurden. In zumindest einem Fall wurde darüber hinaus auch die vom Betroffenen verlangte Auskunft nicht erteilt. Ich habe eine Geldbuße in Höhe von 50.000 Euro festgesetzt, die akzeptiert wurde.

Kundendatenbank im Internet

In einem anderen sanktionierten Fall war eine Kundendatenbank mit zehntausenden Einträgen im Internet zugänglich. Der Zugriffsschutz bestand aus einer besonders langen Adresse mit augenscheinlich zufälliger Zeichenkombination. Eine darüberhinausgehende Hürde, z.B. in Form von Nutzername und Passwort, bestand nicht. Der Verantwortliche setzte im Ergebnis darauf, dass die lange Adresse nicht bekannt wird. Da die Adresse von den (berechtigten) Anwendern typischerweise unverschlüsselt aufgerufen wurde, konnte sie allerdings verhältnismäßig leicht in falsche Hände geraten. Hintergrund ist, dass beim Aufruf unverschlüsselter Internetseiten die komplette Adresse über alle Netzknotenpunkte unverschlüsselt übertragen wird, während bei verschlüsselten aufgerufenen Seiten (https) typischerweise nur die Adresse bis zur Third-Level-Domain sowie der Port unverschlüsselt übertragen werden (müssen). Der restliche Pfad wird grundsätzlich verschlüsselt an den Zielserver übertragen,[1] sodass ein Mitschneiden der zum Zugriff nötigen vollständigen Adresse durch externe Angreifer deutlich erschwert wäre. Unter Berücksichtigung besonderer Umstände des Einzelfalles (teilweise Unternehmensaufgabe) habe ich eine Geldbuße in Höhe von 8.900 Euro festgesetzt, die akzeptiert wurde.

1 Beispiel: Beim Aufruf von https://lfd.niedersachsen.de:443/startseite/infothek/faqs_zur_ds_gvo/ wird der Teil „https://lfd.niedersachsen.de:443“ unverschlüsselt übertragen. Der dahinterliegende Pfad wird bereits TLS-verschlüsselt übertragen.

Durchsuchung wegen mangelnder Kooperation

In einem Fall hat ein Unternehmen mir über seinen Bevollmächtigten die Auskunft verweigert und sich dabei auf das Auskunftsverweigerungsrecht berufen. Dieses Recht bestand nach meiner Auffassung jedenfalls nicht im geltend gemachten Umfang.

Aufgrund des Hinweises einer anderen Behörde bestanden hinreichende Anhaltspunkte dafür, dass Beschäftigte unzulässig mit Kameras überwacht wurden. Nachdem ich einen Beschluss des zuständigen Ermittlungsrichters erwirkt hatte, erfolgte mit Beamtinnen und Beamten der zuständigen Polizeidienststelle eine Durchsuchung der Liegenschaft. Im Rahmen der Durchsuchung wurde ein Speichersystem sichergestellt, auf dem Videoaufzeichnungen zu vermuten waren.

Vor Ort waren die Vertreter des Unternehmens kooperativ, was aufgrund des Schriftverkehrs mit dem bevollmächtigten Rechtsanwalt nicht zu erwarten war. Das Verfahren ist noch nicht abgeschlossen.

Videoüberwachung und Dashcams

FAQ zu Dashcams (Kurzlink): https://t1p.de/faq-dashcam

Viele Fälle betrafen auch im Jahr 2022 den Bereich der Videoüberwachung. Dabei lag ein Schwerpunkt auf Verfahren, in denen Arbeitgeber ihre Beschäftigten sowie Kundinnen und Kunden per Video überwachen. Mein Vorgehen gegen Videoüberwachung am Arbeitsplatz habe ich bereits in den vergangenen drei Tätigkeitsberichten ausführlich vorgestellt.[2]

Zahlreiche Bußgeldentscheidungen entfielen zudem erneut auf Dashcams, die anlasslos Videosequenzen aufzeichneten und damit von den Verantwortlichen unzulässig eingesetzt wurden. Zu Dashcam-Geldbußen habe ich bereits im Tätigkeitsbericht 2019 ausführlich berichtet[3] und im Oktober 2020 zusätzlich einen umfangreichen Fragen-Antworten-Katalog für Betreiberinnen und Betreiber von Dashcams veröffentlicht.

Nachstellungsähnliche Personenfotografie

Keine Haushaltsausnahme

In einer Innenstadt wurde eine männliche Person durch die Polizei kontrolliert, nachdem diese von weiblichen Jugendlichen angezeigt worden war. Hintergrund war, dass die Jugendlichen den Eindruck hatten, von der männlichen Person verfolgt und fotografiert zu werden. Die Kontrolle ergab, dass sich auf dem Smartphone der männlichen Person einige Fotografien der Anzeigeerstatterinnen befanden, die kurz zuvor im öffentlichen Raum der Innenstadt aufgenommen wurden. Nach dem Eindruck der Polizeibeamten waren die Ju-

2 Siehe Tätigkeitsbericht für das Jahr 2019 ab Seite 173, Tätigkeitsbericht für das Jahr 2020 ab Seite 82 und Tätigkeitsbericht für das Jahr 2021 ab Seite 173.

3 Siehe Tätigkeitsbericht 2019 ab Seite 105

gendlichen nicht nur Beiwerk der Aufnahmen, sondern gezielt im Fokus der Aufnahmen.

Die sogenannte Haushaltsausnahme nach Art. 2 Abs. 2 Buchst. c DS-GVO zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten griff nicht. Die Regelung umfasst kein Recht, in der Öffentlichkeit eigenmächtig gezielt Fotografien von fremden Personen zu fertigen. Fremde Personen, die sich in der Öffentlichkeit bewegen, können nicht durch das Anfertigen von Fotografien zu persönlichen Zwecken in die Privatsphäre der- oder desjenigen „hineingezogen" werden, die bzw. der solche Fotos fertigt.

Interessenabwägung

Die Anwendbarkeit des Datenschutzrechts führt nicht automatisch zu einer Unzulässigkeit des Fotografierens oder Filmens. Bei Aufnahmen, die den menschlichen Körper in den Mittelpunkt stellen, fehlt es jedoch an einer Rechtsgrundlage. Datenschutzrechtlich Verantwortliche können sich insbesondere nicht auf Art. 6 Abs. 1 Buchst. f DS-GVO berufen, da sie über keine berechtigten Interessen verfügen, die mindestens gleichwertig zu den Interessen der aufgenommenen Personen sind. Dies gilt insbesondere, wenn es sich bei den datenschutzrechtlich betroffenen Personen um Kinder im Sinne der DS-GVO handelt. Diese müssen auf den besonderen Schutz durch die Rechtsordnung vertrauen können. Kinder sind häufig noch nicht in der Lage, zwischen Privatsphäre und Sozialsphäre adäquat zu unterscheiden, sodass sie sich nicht durchgehend an die jeweilige Sphäre angepasst verhalten. Mit Einschränkungen gilt dies auch für Jugendliche. In der DS-GVO ist für junge Menschen bis zu einem Alter von 16 Jahren eine besondere Schutzbedürftigkeit angelegt.

Der Verstoß wurde mit einer Geldbuße in Höhe von 500 Euro geahndet, die akzeptiert wurde.

Über vergleichbare Fälle hat bereits die Aufsichtsbehörde der Freien und Hansestadt Hamburg mehrfach und ausführlich berichtet.[4]

4 Siehe Tätigkeitsbericht Datenschutz 2020 des Hamburgischen Beauftragten für den Datenschutz und die Informationsfreiheit (HmbBfDI) ab Seite 120 und Tätigkeitsbericht Datenschutz 2021 des HmbBfDI ab Seite 71

J. Aktuelle Themen

J.1. Polizei

1.1 Abschluss der Prüfung der Polizei-Leitstellen

In mehreren Tätigkeitsberichten über die vergangenen fünf Jahre hatte ich bereits ausführlich über die Verarbeitung sehr sensibler Daten in den Leitstellen der Polizei berichtet. Es wird jede Mitteilung an die Leitstelle mit personenbezogenen Daten, dem Sachverhalt und allen Einzelheiten der Meldung in einer Erfassungssoftware verarbeitet. Für diese Daten müssen besondere Schutzmaßnahmen ergriffen werden, was jedoch nicht immer der Fall war.

Fehlender Vertrag zur Auftragsverarbeitung

Schutzstufenkonzept der LfD (Kurzlink): https://t1p.de/schutzstufen

Eine Leitstelle wurde von mir beanstandet, weil es der zuständigen Polizeidirektion nicht gelungen war, mit dem Auftragnehmer einen Vertrag zur Auftragsverarbeitung abzuschließen. Ein solcher Vertrag ist gesetzlich vorgeschrieben. Die Servicetechnikerinnen und -techniker des Auftragnehmers haben im Fall der Fernwartung einen Zugriff auf personenbezogene Daten bis zur Schutzstufe E meines Schutzstufenkonzeptes.

Fehlender Nachweis erfolgter Fernwartungszugriffe

Der Polizeidirektion war es außerdem nicht möglich, einen Nachweis darüber zu erbringen, ob und wann Fernwartungszugriffe erfolgt sind und ob auch tatsächlich ein Zugriff auf die enthaltenen personenbezogenen Daten stattgefunden hat. Ich habe auch diesen Umstand formell beanstandet und zwischenzeitlich eine ausführliche Stellungnahme durch das Niedersächsische Innenministerium erhalten.

Ergriffene Maßnahmen durch das Innenministerium

In seiner Stellungnahme führte das Ministerium aus, dass die betroffene Polizeidirektion mittlerweile einen Vertrag zur Auftragsverarbeitung mit dem Auftragnehmer geschlossen hat und alle Technikerinnen und Techniker nach dem Verpflichtungsge-

setz verpflichtet worden sind. Diese Verpflichtung führt dazu, dass im Fall einer unbefugten Offenlegung erlangter sensibler personenbezogener Daten im Rahmen der Fernwartung eine Bestrafung wie bei einem Amtsträger, mit bis zu einem Jahr Freiheitsstrafe oder einer Geldstrafe, stattfindet.

Da bereits bei einem anderen Dienstleister der Polizei eine Protokollierung der Zugriffe im Rahmen der Fernwartung zur Sicherstellung beziehungsweise Beobachtung der geschalteten Leitungswege aus technischen Gründen durchgeführt wird, konnte eine Vereinbarung getroffen werden, diese Protokollierung zusätzlich für den Zweck des tatsächlichen Nachweises stattgefundener Zugriffe (wann, durch welche Person und für welchen Zeitraum) zu nutzen. Die Protokolldaten werden der Datenschutzbeauftragten der Polizeidirektion nun regelmäßig zur Nachweisführung übermittelt.

In den weiteren Ausführungen verweist das Innenministerium auf die bevorstehende Umstellung der gesamten Leitstellenanwendungen in Niedersachsen. Bei der Planung und Auswahl der neuen Leitstellensoftware war ich von Beginn an eingebunden. Ich konnte mich davon überzeugen, dass die datenschutzrechtlichen Notwendigkeiten bisher beachtet wurden.

Vorhandenes Restrisiko

Das Innenministerium ist sich bewusst, dass die ergriffenen Maßnahmen aus datenschutzrechtlicher Sicht keinen optimalen Umsetzungsgrad erreicht haben und weiterhin ein entsprechendes Restrisiko bei der Verarbeitung der sensiblen personenbezogenen Inhalte vorliegt. Dieses wird jedoch durch die Verantwortlichen der Polizei für eine Übergangsfrist verantwortet.

Ausblick

Ich gehe derzeit davon aus, dass spätestens nach der erfolgten Umstellung auf die neue Software in den einzelnen Leitstellen der Polizei eine rechtskonforme Datenverarbeitung stattfinden wird. In diesem Zusammenhang erwarte ich, dass die verantwortlichen Polizeibehörden ihrer nach § 39 des Niedersächsischen Datenschutzgesetzes obliegenden Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung vor Inbetriebnahme der neuen Software nachkommen. Da die Polizei bei der aktuell eingesetzten Software die entsprechenden Pflichten nicht erfüllt hat, werde ich diesen Punkt weiterverfolgen.

1.2 TKÜ-Zentrum im Nordverbund weiter im Verzug

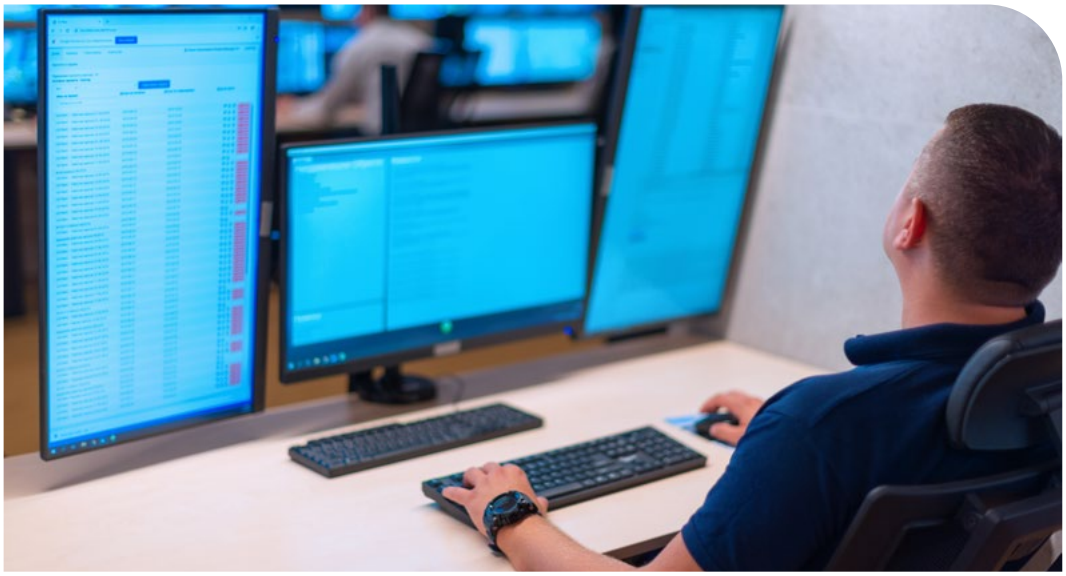
Maßnahmen der Telekommunikationsüberwachung (TKÜ)[1] zur Ermittlung von schweren Straftaten und zur Gefahrenabwehr stellen einen erheblichen Eingriff in die Rechte und Freiheiten der betroffenen Personen dar. Dieser Tatsache war sich der Gesetzgeber bewusst und hat entsprechende rechtliche Hürden zur Eindämmung und Eingrenzung der Eingriffe gesetzt. Das Datenschutzrecht verlangt daher auch erhebliche technische und organisatorische Maßnahmen zum Schutz vor Verletzungen der Persönlichkeits- und Freiheitsrechte, ohne dass dabei die TKÜ wirkungslos wird. Das seit Jahren geplante gemeinsame „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer" (RDZ-TKÜ) ist mit dem angestrebten rechtskonformen Aufbau und Betrieb erneut erheblich in Verzug geraten. Das von mir bereits im Jahr 2017 beanstandete Altverfahren des Landeskriminalamtes (LKA) Niedersachsen wird daher faktisch solange weiter betrieben, bis das Fünfländer-Nachfolgeverfahren im Produktivbetrieb starten kann. Inzwischen ist dies der siebte Beitrag zu diesem Thema in einem Tätigkeitsbericht.

Zuletzt habe ich in meinem 27. Tätigkeitsbericht für das Berichtsjahr 2021 über die offenen datenschutzrechtlichen und technisch-organisatorischen Fragen zur Verfahrensprojektierung für ein gemeinsames RDZ-TKÜ berichtet (siehe Kapitel J.2.2, ab Seite 116). Bei diesem Projekt der Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein sollen in einer Kooperation an einem Standort Synergieeffekte für die Länderpolizeien erzielt werden. Die ersten Planungen für eine Modernisierung der vorhandenen Lösung wurden bereits im Jahr 2011 aufgenommen und in den Folgejahren für eine Mehr-Länder-Kooperation fortgesetzt. Seither sind auch die Datenschutzaufsichtsbehörden der fünf beteiligten Länder in gemeinsamer Abstimmung mit der Beratung der Projektleitung befasst. Ziel des im August 2016 hierfür in Kraft getretenen Staatsvertrages[2] ist eine neu zu entwickelnde und von allen fünf Ländern gemeinschaftlich nutzbare TKÜ-Anlage mit einem einheitlichen Verfahren in einem gemeinsamen RDZ-TKÜ. Dieses soll unter einer gemeinsamen fachlichen Leitung mit Sitz in Hannover gesteuert werden.

Daten von 1258 Betroffenen abgerufen

1 Laut Statistik des Bundesamtes für Justiz vom August 2022 wurden 2020 in Niedersachsen 417 TKÜ-Maßnahmen angeordnet. Niedersachsen liegt damit im bundesweiten Mittelfeld.

2 Der Nds. Landtag verabschiedete als Nds. Ratifizierungsgesetz zum Staatsvertrag das Gesetz zu dem Staatsvertrag zwischen der Freien Hansestadt Bremen, der Freien und Hansestadt Hamburg, dem Land Mecklenburg-Vorpommern, dem Land Niedersachsen und dem Land Schleswig-Holstein über die Einrichtung und den Betrieb eines Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer vom 08.06.2016, Nds. GVBl. Nr. 7/2016, Seite 110.



Bei der Beratung war rechtlich bereits im Jahr 2018 die Umsetzung der sogenannten JI-Richtlinie im zweiten Teil des neuen Niedersächsischen Datenschutzgesetzes (NDSG) zu bewerten. Zusätzlich mussten gleichberechtigt die mitunter abweichenden Bestimmungen der Landesdatenschutzgesetze der anderen vier beteiligten Länder berücksichtigt werden.

Anforderungen seit Jahren nicht umgesetzt

Die TKÜ sollte unter der Betreuung des RDZ-TKÜ nach erheblichen Verzögerungen im ersten Quartal 2022 in Betrieb gehen. Durch Verzögerungen bei der Beschaffung, Personalfluktuation in der Projektgruppe, Anpassungsaufwände beim Dienstleister, haushaltsrechtliche Hindernisse, Verzögerungen in einigen der Partnerländer sowie erschwerte Gremienbefassungen kam es nach Angaben der Projektleitung zu weiteren Abweichungen vom Zeitplan.

Die letzten Beratungsergebnisse durch die fünf Datenschutzaufsichtsbehörden stammen aus dem Jahr 2019. Im Berichtszeitraum wurden neue technisch orientierte Fragen durch das Fachgebiet Datenschutz der Projektgruppe RDZ-TKÜ an meine Behörde herangetragen, die sich erst in den letzten Monaten ergeben hatten. Diese wurden erörtert und durch meine Behörde bewertet und anschließend mit den anderen vier Datenschutzaufsichtsbehörden abgestimmt. Eine Reihe von inhaltlichen Hinweisen zu diesen Fragen erhielt die Projektleitung in Hannover schriftlich im Juni 2022. Zu diesem Zeitpunkt wurde mir eine Fertigstellung der Risikobewertung und einer Datenschutz-Folgenabschätzung (DSFA) frühestens ab Juli 2022 in Aussicht gestellt.

TKÜ-Altverfahren im LKA Niedersachsen für Niedersachsen und Bremen läuft weiterhin mit Mängeln

Erneut habe ich auf die Tatsache hingewiesen, dass das TKÜ-Altverfahren im LKA Niedersachsen für Niedersachsen und Bremen, das seit 2012 in Betrieb ist, bereits im September 2017 (mit sieben Hauptpunkten und 44 Unterpunkten) von mir beanstandet wurde. Ich wies zudem darauf hin, dass diese Beanstandung weiterhin Bestand habe, weil das Verfahren faktisch noch immer

mit Mängeln und Rechtsverstößen betrieben werde. Jede Verzögerung eines Neuverfahrens verlängert diesen nicht hinnehmbaren Zustand, solange der Dienstleister nicht mit den notwendigen Abhilfemaßnahmen zum Altverfahren beauftragt wird.

Zeitplan obsolet: Verzögerung durch Beschaffungs- und Finanzierungsstau

Im November 2022 erfuhr ich von der Projektleitung auf Nachfrage, dass sich der zwischenzeitlich für den 10.10.2022 geplante Start erneut verschieben werde. Als Gründe hierfür wurden mir folgende Faktoren genannt:

- Die Beschaffung einer seit 2017 rechtlich verpflichtend einzusetzenden Komponente habe sich unvorhergesehen um einen erheblichen Betrag verteuert und sei bisher finanziell nicht abgedeckt gewesen.
- Seit Januar 2022 liefen die o. g. Gremienbefassungen, die offenbar aufgrund der Finanzierungslücke und der aktuell schwierigen Haushaltslage der Länder erforderlich geworden seien. Bis Anfang Dezember 2022 seien zudem die Länderkabinette von zwei Ländern eingebunden. Erst danach könne der Umlaufbeschluss zur Finanzierung durch den zuständigen Arbeitskreis der Innenminister der Norddeutschen Länder erfolgen.
- Erst ab Januar 2023 könne die Beschaffung der Hard- und Software für die Lösung mit der genannten Komponente über einen Rahmenvertrag starten; die Lieferung werde voraussichtlich erst im Herbst 2023 erfolgen.
- Der Aufbau der Komponenten sowie die Implementierung und der Test durch die Dienstleistungsfirmen würden dementsprechend im Anschluss erfolgen. Die hierfür nötigen externen Personaleinsätze könnten aufgrund der unklaren Lieferzeiten nicht geplant werden.

In der Folge sei der Starttermin für den Wirkbetrieb durch die Projektleitung aufgrund der zahlreichen Unwägbarkeiten noch nicht neu bestimmbar.

Informationssicherheit muss verifiziert werden

Der parallel weiter zu bearbeitende Bereich des BSI-Grundschutz-Checks für die Gesamtanlage und das Verfahren sowie die noch zu erarbeitende DSFA würden laut Projektleitung zu Kapazitätsbindungen im Technik-Bereich der Projektgruppe führen. Es wurde zugesagt, dass die DSFA rechtzeitig vor dem Wirkbetrieb den Aufsichtsbehörden vorgelegt werde.

Die Gesamtverzögerung bis zum Wirkbetrieb beträgt nach meiner letzten Einschätzung dieser Berichte absehbar inzwischen fast drei Jahre.

1.3 Abschluss der Prüfung des polizeilichen Messengers NIMes

In meinen Tätigkeitsberichten der vergangenen zwei Jahre hatte ich bereits ausführlich über die flächendeckende Einführung des Niedersachsen-Messengers (NIMes) für die Polizei und die damit verbundenen Gefahren für die Verarbeitung der personenbezogenen Daten berichtet. Im Rahmen meines Prüfverfahrens und der anschließenden Beanstandung gegenüber dem Innenministerium hatte ich festgestellt, dass die genannten Gefahren durch den Umstand der Nutzung privater mobiler Endgeräte entstehen, die bislang nur in einem geringen Umfang gegen dienstliche Endgeräte ersetzt worden sind.

Maßnahmen des Innenministeriums

Mittlerweile wurden ungefähr 3.800 dienstliche Smartphones und Tablets beschafft und ausgegeben, die alle über ein sogenanntes Mobile Device Management (MDM) verfügen, welches eine komplette sicherheitstechnische Behandlung der Geräte aus der Ferne ermöglicht. Für das Jahr 2023 ist die Anschaffung von bis zu 10.000 mobilen Endgeräten vorgesehen.

Zusätzlich plant das Innenministerium die Ausgabe der kommenden Generation des sogenannten Polizei-Clients (PoC 2.0) ab September 2023. Dieses würde in der Endausbaustufe bedeuten, dass ungefähr 25.000 neue Endgeräte als Arbeitsplatzausstattung vorhanden wären. Da NIMes auch als Desktop-Anwendung seit seiner Einführung landesweit zur Verfügung steht, könnte der Messenger dann ab dem Herbst 2023 von allen Beschäftigten der Polizei Niedersachsen auf den mobilen dienstlichen Endgeräten und dem PoC 2.0 genutzt werden.

Das Innenministerium hat bereits im Jahr 2022 verfügt, dass die Nutzung von NIMes auf privaten Geräten nur dann gestattet ist, wenn kein dienstliches Gerät zur Verfügung gestellt wird. Die aufgeführten 25.000 Endgeräte des PoC 2.0 und die hohe Anzahl der mobilen Geräte könnten somit zukünftig gewährleisten, dass die Nutzung privater Endgeräte auf wenige Ausnahmefälle beschränkt wird.

Vorhandenes Restrisiko

Die geplanten Ausstattungen mit dienstlichen Geräten dürften erst im Laufe des Jahres 2023 dazu führen, dass nur noch wenige private Endgeräte genutzt werden. Das bis dahin bestehende erhöhte und danach verbleibende Restrisiko muss durch die Verantwortlichen in den Reihen der Polizei in Kauf genommen werden.

1.4 Gut gemeint, aber dennoch rechtswidrig – Verwarnung des Landeskriminalamts Niedersachsen

Die Verarbeitung von Daten muss sich stets auf eine rechtliche Grundlage stützen lassen können. Dieser rechtsstaatliche Grundsatz gilt umso mehr, wenn es sich um hoch sensible Daten aus Strafverfahren handelt, die an Dritte übermittelt werden sollen.

Das Forschungsvorhaben

Die Universität Kassel trat 2019 mit der Bitte um Unterstützung für ein Forschungsprojekt zu dem Thema „Die Strafverfolgung der Vergewaltigung in Niedersachsen" an das Landeskriminalamt Niedersachsen (LKA) heran.

Der wissenschaftliche Zweck der Forschung lag im Wesentlichen darin, ein umfassendes Bild über die Sachbehandlung der Verfahren nach einer bereits erfolgten und der Polizei angezeigten Vergewaltigung zu erhalten. Auch sollten mögliche Gründe einer geringeren Verurteilungsquote von Tätern im Vergleich zu anderen Bundesländern ermittelt werden. Eine Methode der Untersuchung stellte die Befragung von Vergewaltigungsopfern mittels eines sehr detaillierten und umfangreichen Fragebogens dar. Entgegen der sonst üblichen Verfahrensweise wurden die Fragebögen den Betroffenen jedoch ohne ihr Wissen und ohne vorherige Zustimmung zugesandt. Für den Versand selektierte das LKA Niedersachsen vorab in dem polizeilichen Vorgangsbearbeitungssystem NIVADIS fast 3500 weibliche Personen nach bestimmten Kriterien. Der Versand der von der Universität Kassel erstellten Fragebögen an diese Personen wurde durch das LKA Niedersachsen im Jahre 2021 veranlasst. Als Absender wurde die Universität Kassel vermerkt. Dadurch wurden unzustellbare Schreiben durch den Postdienstleiter mit den Namen der Betroffenen an die Universität Kassel rückversandt.

Rechtsgrundlage der Verarbeitung aus Sicht des Landeskriminalamts

Die Verarbeitung der personenbezogenen Daten im Rahmen der Selektierung und des Versands wurde durch das LKA auf die Rechtsgrundlage des § 39 Absatz 7 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) gestützt. Dabei sei eine Abwägung zugunsten der Unterstützungsleistung aufgrund der Relevanz der Forschungsfrage sowie der zu erwartenden wissenschaftlichen Erkenntnisse getroffen worden. Die Risiken, welche durch die Zusendung der Fragebögen für die Opfer bestanden, zum Beispiel einer Retraumatisierung oder einer möglichen unerwünschten Offenlegung der Opfereigenschaft gegenüber Dritten, seien dabei bekannt ge-

wesen. Auch der Ethikrat der Universität Kassel habe dieses Risiko als hinnehmbar bewertet.

Leider trat eine solche Retraumatisierung bei mehreren angeschriebenen Personen ein, von denen eine den Mut aufbrachte, sich in Form einer Beschwerde an meine Behörde zu wenden.

Verwarnung des Landeskriminalamts

Im Rahmen meines daraufhin eingeleiteten Prüfverfahrens habe ich im Ergebnis datenschutzrechtliche Verstöße festgestellt und abschließend gegenüber dem LKA in 2022 eine Verwarnung ausgesprochen. Für die Selektion, den Versand der Fragebögen sowie die Übermittlung der Daten an die Universität Kassel, welche der Rückversand der unzustellbaren Postsendungen darstellte, lag keine Rechtsgrundlage vor. § 39 Absatz 7 NPOG kann nur für eigene wissenschaftliche Vorhaben der Polizei dienen. Forschungsvorhaben von Dritten sind nicht vom Anwendungsbereich der Norm umfasst. Doch selbst wenn die Norm zur Anwendung hätte gebracht werden können, wäre auch die erforderliche Interessensabwägung als Tatbestandsvoraussetzung zugunsten der Betroffenen zu treffen gewesen.

Wissenschaftliche Zwecke in der Güterabwägung

Auch ein bedeutender wissenschaftlicher Zweck darf nicht zu unbegrenzten Datenverarbeitungen führen. Bei der Gegenüberstellung der betroffenen Grundrechtspositionen, hier einerseits die Forschungsfreiheit und andererseits das Recht auf informationelle Selbstbestimmung, musste beachtet werden, dass durch die Verarbeitung von personenbezogenen Daten (pbD) besonderer Kategorien, welche hier die Opfereigenschaft darstellte, dem Recht auf informationelle Selbstbestimmung zunächst ein vergleichbar höherer Schutzgedanke als „normalen" pbD zuzuordnen war. Weitaus wichtiger und letztendlich der entscheidende Faktor für ein offensichtliches Überwiegen der Rechte der Betroffenen war jedoch die Tatsache, dass auch das Grundrecht der Betroffenen auf körperliche Unversehrtheit betroffen war. Dies ergab sich aus dem hohen Risiko jedes Einzelnen, durch das Anschreiben eine Retraumatisierung zu erleiden. Dieses Risiko lag allein durch die hohe Zahl der angeschriebenen Betroffenen offenkundig vor und ist letztendlich leider auch eingetreten.

Mein datenschutzrechtlicher Beitrag

Zukünftig muss unbedingt vermieden werden, dass Opfer von Straftaten, die bereits allein durch die erlittene Tat mit den psychischen Folgen zu kämpfen haben, durch staatliches Handeln zum zweiten Mal zum Opfer werden. Hierzu hat meine Behörde hoffentlich beigetragen.

1.5 Prüfung des Schengener Informationssystems der zweiten Generation (SIS II)

Bereits in meinem letzten Tätigkeitsbericht habe ich ausführlich über die Prüfung der Ausschreibungen von Personenfahndungen zur verdeckten Kontrolle der polizeilichen und justiziellen Zusammenarbeit in Strafsachen oder zur Gefahrenabwehr nach Artikel 36 Absatz 2 SIS II-Beschluss berichtet. Der Schwerpunkt der Prüfung lag darin, ein Gesamtbild über die Nutzung dieses Instrumentes und der damit verbundenen datenschutzrechtlichen Probleme zu erhalten. Zugleich wurde die Rechtmäßigkeit solcher Ausschreibungen in einer Stichprobe kontrolliert.

Siehe 27. Tätigkeitsbericht der LfD, Abschnitt 2.5, Seite 117

Prüfergebnis

In drei Polizeidirektionen wurden insgesamt 52 gespeicherte Ausschreibungen zur Personenfahndung gemäß Artikel 36 Absatz 2 SIS II-Beschluss – mithin 78 Prozent des prüfrelevanten Speicherbestandes der niedersächsischen Polizei – gesichtet. Die Ausschreibungen erfolgten sowohl repressiv als auch präventiv sowie zur Führungsaufsicht.

In 50 von 52 Fällen konnte die Rechtmäßigkeit der Ausschreibungen festgestellt werden. In zwei Fällen lagen jedoch die Voraussetzungen der nationalen Rechtsgrundlage nicht (mehr) vor; beide Ausschreibungen wurden unverzüglich gelöscht. In einem der beiden Fälle hätte die (repressive) Personenausschreibung mangels einer Verlängerung des richterlichen Beschlusses bereits zwei Jahre zuvor gelöscht werden müssen. In dem weiteren Fall lag ein richterlicher Beschluss für die über einen Zeitraum von fast vier Jahren andauernde (repressive) Personenausschreibung zu keinem Zeitpunkt vor. Die die Ausschreibung veranlassende Behörde war in diesem Fall eine Staatsanwaltschaft.

Hinsichtlich der Anordnungen der Ausschreibungen zur polizeilichen (präventiven) Beobachtung durch Dienststellenleitungen beziehungsweise Amtsgerichte konnte in insgesamt sechs Fällen eine zeitliche Lücke zwischen zwei Ausschreibungszeiträumen von zumeist wenigen Tagen festgestellt werden. Dies betraf jedoch vorrangig Ausschreibungszeiträume der Jahre 2017 bis 2019; darauffolgende Anordnungszeiträume gingen regelmäßig taggenau ineinander über.

Gegenüber den Verantwortlichen wurden infolge der durchgeführten Prüfung sowie in Vorbereitung künftiger aufsichtsbehördlicher Kontrollen zum SIS II Handlungsempfehlungen ausgesprochen.

Bewertung und Ausblick

Zusammenfassend ließ die Prüfung eine erste, grundlegende Beurteilung des Speicherverhaltens der niedersächsischen Polizeibehörden im SIS II zu. Diese Erkenntnisse bilden sodann die Grundlage für die nächste turnusmäßige Überprüfung des SIS II spätestens im Jahre 2025.

1.6 Prüfung der Datenerhebung durch die Verwendung von Vertrauenspersonen

Gemäß § 48 Absatz 2 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) kontrolliert meine Behörde die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung von personenbezogenen Daten, die nach den §§ 17 c und 32 Absatz 2 sowie den §§ 33 a bis 37 a NPOG erhoben wurden. Gegenstand meiner Prüfung war im Berichtszeitraum die Datenerhebung durch die Inanspruchnahme von Vertrauenspersonen gemäß § 36 NPOG, also von Privatpersonen, deren langfristig angelegte Zusammenarbeit mit der Polizei Dritten nicht bekannt ist.

Prüfergebnis

Im Zuge meiner aufsichtsbehördlichen Tätigkeit wurden sämtliche Verwendungen von Vertrauenspersonen gemäß § 36 NPOG in den Polizeibehörden des Landes Niedersachsen geprüft.

In allen geprüften Verfahren lagen die materiellen Rechtmäßigkeitsvoraussetzungen des § 36 Absatz 1 Satz 1 NPOG in Verbindung mit § 34 Absatz 1 Satz 1 NPOG vor. Die Anordnungen erfolgten gemäß § 36 Absatz 4 Satz 1 NPOG durch das Amtsgericht Hannover; Anordnungen durch die Polizei bei Gefahr im Verzug gemäß § 36 Absatz 5 Satz 1 NPOG erfolgten nicht.

Hinsichtlich der engen Voraussetzungen zur Auswahl der Vertrauensperson gemäß § 36 Absatz 2 NPOG sowie der Verbote zu Einsatzmethoden gemäß § 36 Absatz 3 NPOG konnte auf umfangreiche landesweite Vorgaben zurückgegriffen werden. Die Vorgaben des § 48 NPOG hinsichtlich der Dokumentation der Datenerhebung sowie Datenlöschung wurden in allen Fällen beachtet.

In einem Fall gingen zwei richterliche Beschlüsse für die Anordnung der Maßnahme nicht taggenau ineinander über, sodass für einen Zeitraum von insgesamt 24 Stunden kein richterlicher Beschluss für die polizeiliche Eingriffsmaßnahme vorlag.

Bei fast allen abgeschlossenen Verfahren erfolgte die befristete Zurückstellung der Unterrichtung des von der Eingriffsmaßnahme Betroffenen gemäß § 30 Absatz 5 NPOG. In einem Verfahren fand eine Benachrichtigung des Betroffenen gemäß § 30 Absatz 4 NPOG statt. Eine unter den engen Voraussetzungen des § 30 Absatz 7 NPOG mögliche endgültige Zurückstellung erfolgte in keinem Fall.

In drei Fällen erfolgte die Einholung des richterlichen Beschlusses für die Zurückstellung der Unterrichtung des von der verdeckten Maßnahme Betroffenen nicht innerhalb des gemäß § 30 Absatz 5 Satz 2 NPOG gesetzlich vorgeschriebenen Zeitrahmens. In allen drei Fällen lag aber zum Prüfungszeitpunkt ein richterlicher Beschluss für die befristete Zurückstellung der Unterrichtung des von der Eingriffsmaßnahme Betroffenen vor.

In zwei weiteren Fällen lag der erforderliche richterliche Beschluss für die befristete Zurückstellung der Benachrichtigung indes nicht vor. Diesbezüglich wurde die sofortige Einholung des Beschlusses durch die zuständige Behörde angeregt.

Bewertung und Ausblick

Bei den zuständigen Polizeibehörden herrschte grundsätzlich ein hohes Maß an Sorgfalt und Sensibilität im Zusammenhang mit den Datenerhebungen selbst sowie der Zuarbeit zu den Prüfungen durch meine Behörde. Die Prüfung sämtlicher Datenerhebungen durch die Inanspruchnahme von Vertrauenspersonen gemäß § 36 NPOG ließ eine erste Beurteilung datenschutzrechtlich relevanter Aspekte in diesem Themenfeld zu. Die gewonnenen Erkenntnisse bilden die Grundlage für eine mögliche nächste Überprüfung im Jahre 2024.

J.2. Justiz

2.1 Aufsichtsrechtliche Lücke – besondere Stellen im Justizsystem fehlen noch immer

Die Lücke bei der Datenschutzaufsicht im Justizbereich, auf die ich bereits in meinen letzten Tätigkeitsberichten hingewiesen habe, besteht weiterhin. „Besondere Stellen im Justizsystem", wie sie Erwägungsgrund 20 zur Datenschutz-Grundverordnung (DS-GVO) vorsieht, sind bislang weder in Niedersachsen oder anderen Bundesländern noch auf Bundesebene eingerichtet.

Siehe 27. Tätigkeitsbericht der LfD, Abschnitt J.3.1, Seite 122

Schreiben der Datenschutzkonferenz

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) hat sich im März 2022 an die Justizministerkonferenz gewandt, um auf die aufsichtsrechtliche Lücke aufmerksam zu machen und für das Thema zu sensibilisieren. In ihrem Antwortschreiben aus dem August 2022 teilte die Justizministerkonferenz die Einschätzung der DSK, dass die Zuständigkeitsausnahme der Datenschutzaufsichtsbehörden für den Bereich justizieller Tätigkeit gemäß Artikel 55 Absatz 3 DS-GVO nicht dazu führen dürfe, dass die Datenschutzrechte der Betroffenen unzureichend gewährleistet würden. Zugleich betont sie aber auch, dass die Unabhängigkeit der Justiz nicht beeinträchtigt werden dürfe. Nicht zuletzt bedürfe das Thema auch im Hinblick auf die Frage der Gesetzgebungskompetenz einer weitergehenden Diskussion im Länderkreis.

Weiteres Vorgehen

Durch die Justizministerkonferenz war beabsichtigt, eine Erörterung innerhalb einer Zentralabteilungsleitertagung der Landesjustizverwaltungen zu führen. Da eine entsprechende Sachstandsmitteilung aktuell noch aussteht, werde ich die Entwicklungen weiter beobachten und das Thema in meinem nächsten Tätigkeitsbericht erneut aufgreifen.

2.2 Aufsicht über Staatsanwaltschaften – Beanstandung einer Generalstaatsanwaltschaft

Siehe 26. Tätigkeitsbericht 2020, Seite 139 und 27. Tätigkeitsbericht 2021, Seite 124

Im Fall einer Datenverarbeitung durch eine Generalstaatsanwaltschaft (GenStA) hat meine Behörde eine Beanstandung ausgesprochen. Entgegen der Auffassung der GenStA sah meine Behörde sich als zuständig für die Aufsicht an. Zu diesem Thema habe ich bereits in den beiden vorangegangenen Tätigkeitsberichten im Allgemeinen sowie zuletzt auch zu einem konkreten Einzelfall berichtet.

Bei mir ging eine Meldung ein, wonach eine GenStA eine höchstrichterliche Entscheidung in nicht anonymisierter Form an öffentliche Stellen in Niedersachsen übermittelt habe sollte. Dies wurde durch die betreffende GenStA bestätigt. Eine der GenStA zuzuordnende Stelle hatte einen Beschluss des Bundesgerichtshofs zur Kenntnisnahme an niedersächsische Staatsanwaltschaften weitergeleitet. Die in dem Beschluss enthaltenen personenbezogenen Daten der betroffenen Person waren zuvor nicht anonymisiert worden.

Zuständigkeit der LfD

Die GenStA brachte gegenüber meiner Behörde im Rahmen des Verwaltungsverfahrens in einer Stellungnahme sowie im weiteren Schriftverkehr wiederholt zum Ausdruck, dass sie die Zuständigkeit meiner Behörde ausdrücklich nicht anerkenne. In diesem Zusammenhang argumentierte sie, dass es sich bei ihren Datenverarbeitungen generell um „justizielle Tätigkeiten" handele. Insofern sei sie „wie die Gerichte" zu betrachten und von meiner Aufsicht ausgenommen.

Diese Auffassung habe ich ausdrücklich zurückgewiesen. Meine Aufsicht über die erfolgte Datenverarbeitung der GenStA – hier in Form der Übersendung einer Gerichtsentscheidung – war vorliegend auch nicht durch die Regelung des § 57 Absatz 3 Satz 1 des Niedersächsischen Datenschutzgesetzes (NDSG) eingeschränkt. Danach ist meine Aufsicht über die Staatsanwaltschaften „erst nach Abschluss des Strafverfahrens zulässig". Diese Vorschrift kam in dem zugrunde liegenden Fall nicht zur Anwendung.

Selbst unter Zurückstellung von Bedenken, ob diese Regelung angesichts der Weisungsgebundenheit der Staatsanwaltschaften gegenüber dem Landesjustizministerium überhaupt mit europäischem Recht vereinbar ist[1] sowie Bedenken hinsichtlich des Wortlauts, der lediglich die Erhebung von Daten von der Aufsicht ausnimmt, lagen die Voraussetzungen des § 57 Absatz 3 Satz

1 Siehe EuGH, Urteil vom 27. Mai 2019, Az. C-508/18.

1 NDSG hier nicht vor. Ausweislich des Gesetzestexts („nach Abschluss des Strafverfahrens", „bei der Ermittlung, Aufdeckung oder Verfolgung von Straftaten") muss die betreffende Datenverarbeitung im Rahmen eines konkreten Strafverfahrens erfolgen, um einen Ausschluss meiner Zuständigkeit auszulösen.

Meine Ermittlungen ergaben jedoch, dass der GenStA der betreffende Gerichtsbeschluss ohne konkreten Einzelfallbezug im Rahmen eines bundesweiten Austauschs zur Verfügung stand. Diesen hat die GenStA wiederum ohne Bezug zu einem konkreten Strafverfahren an niedersächsische Staatsanwaltschaften weitergegeben.

Insbesondere angesichts des Umstands, dass neben der obigen Diskussion um meine Zuständigkeit im vorliegenden Fall die Weitergabe der personenbezogenen Daten der betroffenen Person aus dem gerichtlichen Beschluss nicht erforderlich war, sprach ich eine Beanstandung aus. Diese erfolgte gemäß § 57 Absatz 5 Satz 2 NDSG gegenüber dem Niedersächsischen Justizministerium (MJ) als für die GenStA zuständige oberste Landesbehörde. Die Stellungnahme des MJ hierzu stand zum Ende des Berichtszeitraums noch aus.

2.3 Prüfung der Niedersächsischen Justizvollzugsanstalten

Die Grundrechte der Gefangenen sind in besonderer Weise eingeschränkt. Jedoch sind diese Beschränkungen nicht grenzenlos zulässig. Deshalb hat meine Behörde begonnen, die Verarbeitungen von Daten der Gefangenen durch die Niedersächsischen Justizvollzugsanstalten im Rahmen einer anlasslosen Prüfung in den Fokus zu nehmen. Im Vordergrund stehen dabei Fragen aus der täglichen aufsichtsbehördlichen Praxis.

Regelmäßig erreichen meine Behörde Beschwerden von Inhaftierten aus den Niedersächsischen Justizvollzugsanstalten. Gegenstand der Beschwerden sind dabei etwa die Beschilderung von Hafträumen, die Einsehbarkeit von Räumlichkeiten, wie Büros mit vertraulichen Unterlagen, die Abwicklung des Brief- und Schriftverkehrs sowie die Entsorgung von Dokumenten, die personenbezogene Daten enthalten. Die Prüfung soll einen Überblick über die jeweiligen Verfahrensweisen in den Justizvollzugsanstalten schaffen und zeigen, an welchen Stellen Verbesserungsbedarf besteht.

Zunächst schriftliches Verfahren

Die Prüfung wurde aus Kapazitätsgründen auf insgesamt sieben der 13 Justizvollzugsanstalten in Niedersachsen begrenzt. In einem ersten Schritt wurden diese stichprobenartig ausgewählten Anstalten (jeweils begrenzt auf die jeweilige Hauptanstalt) aufgefordert, einen schriftlichen Fragenkatalog zu beantworten. Die ausgewerteten (vorläufigen) Ergebnisse des schriftlichen Teils der Prüfung liegen inzwischen vor. Dabei wurden bei einzelnen Punkten – wie etwa der Gestaltung der Haftraumbeschilderung – diverse Unterschiede deutlich. Auch zu weiteren Aspekten, zum Beispiel hinsichtlich der Entsorgung von Dokumenten, wird es im weiteren Fortgang der Prüfung noch verschiedene Rückfragen geben.

In einem zweiten Schritt werden nun in einigen der Justizvollzugsanstalten Vor-Ort-Termine folgen. Diese sollen unter anderem der Klärung noch offener Rückfragen dienen. Zudem bietet sich hierdurch die Möglichkeit, sich einen unmittelbaren Eindruck von der Praxis vor Ort zu verschaffen. Eine abschließende Bewertung folgt im kommenden Berichtszeitraum.

J.3. Kommunen und Landesverwaltung

3.1 Einsatz von Microsoft 365 im öffentlichen Bereich

Wie bereits im letzten Berichtszeitraum macht der Einsatz von Microsoft 365 weiterhin Schlagzeilen und ist häufig Gegenstand von Beratungsanfragen sowohl im nicht-öffentlichen als auch im öffentlichen Bereich.

Tätigkeitsbericht 2021, Kapitel E.6, S. 43.

Was hat sich im Berichtszeitraum getan?

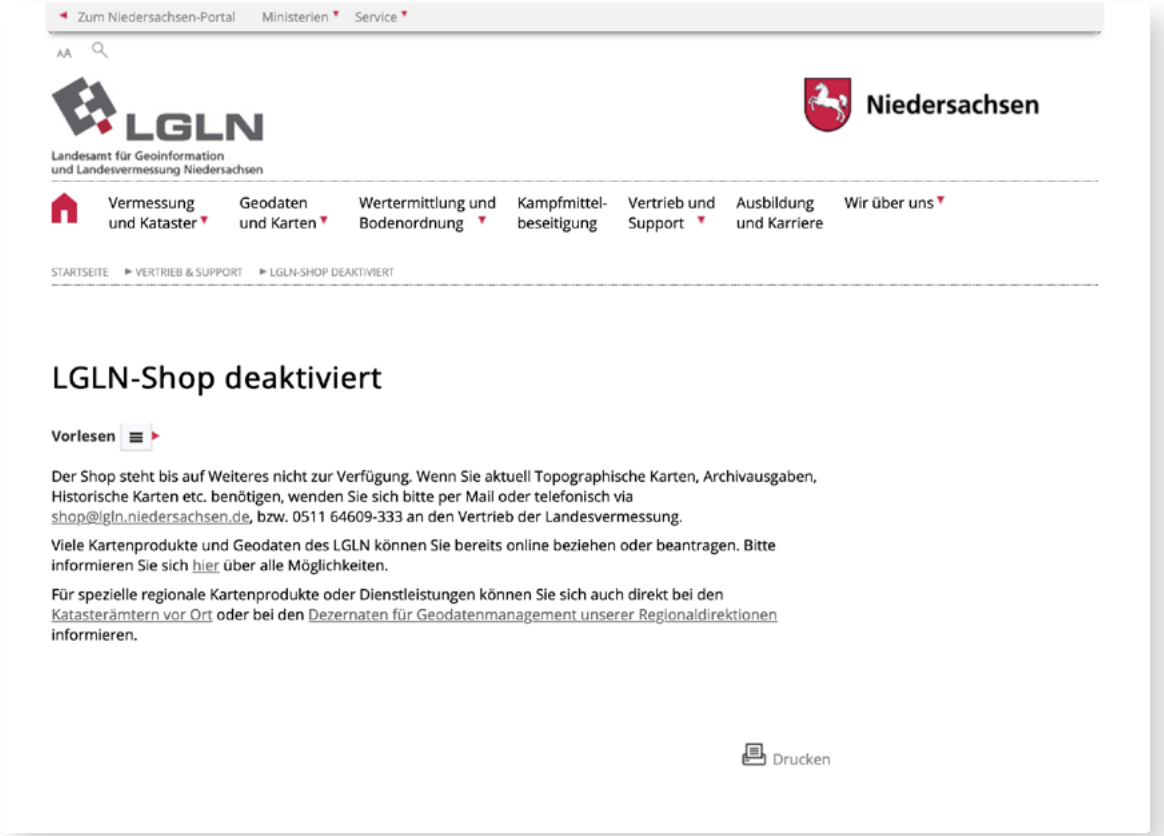
Die Datenschutzkonferenz (DSK) hat ihre Gespräche mit Microsoft fortgeführt. Dabei ging es sowohl um die Mängel des Datenschutznachtrags von Microsoft („Data Protection Addendum – DPA") als auch die Auswirkungen des Schrems II-Urteils des Europäischen Gerichtshofs auf den internationalen Datenverkehr. Auf der Grundlage der Befunde, die die DSK bereits im Jahr 2020 veröffentlichte, wurden umfangreiche, weitere Verhandlungsrunden mit Microsoft zu den aufgezeigten Defiziten durchgeführt. Der Abschlussbericht der DSK vom 02.11.2022 hat deutlich gezeigt, dass Microsoft auch die im diesem Berichtszeitraum geführten Gespräche leider nicht dazu genutzt hat, die Mängel des DPA in der am 15.9.2022 veröffentlichten Neufassung vollständig zu beheben. Wie die DSK in ihrer Festlegung vom 25.11.2022 festgestellt hat, kann der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten DPA vom 15. September 2022 nicht geführt werden. Damit können Verantwortliche durch den Abschluss der Standardvertragsunterlagen von Microsoft ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nicht nachkommen.

Und jetzt?

Ich werde mich im kommenden Berichtszeitraum sowohl mit dem zum 01.01.2023 aktualisierten DPA als auch mit den Entwicklungen im Bereich des internationalen Datenverkehrs befassen und den Verantwortlichen im öffentlichen Bereich auch beratend zur Seite stehen. Die Verantwortlichen sehe ich weiterhin in der Pflicht, die Datenschutzkonformität als unabdingbares Kriterium im Rahmen der IT-Beschaffungsprozesse einzusetzen.

3.2 Datenpannenmeldung des Landesamtes für Geoinformation und Landesvermessung

Ende des Jahres 2021 meldete mir das niedersächsische Landesamt für Geoinformation und Landesvermessung (LGLN) eine Datenschutzverletzung gemäß Art. 33 DS-GVO für den hauseigenen Online-Shop. Drei Kunden des LGLN hatten das Landesamt zuvor darauf aufmerksam gemacht, dass sie nach einer Bestellung in dessen Online-Shop Phishing-E-Mails erhalten hatten. Die gleichen E-Mails wurden auch an einzelne mit dem Online-Shop betraute Beschäftigte des LGLN versendet.



Durch einen Programmierfehler in der Struktur des Online-Shops war es einem Angreifer möglich gewesen, mittels einer sogenannten SQL-Injection auf die Datenbank der Kunden des Online-Shops Zugriff zu nehmen. Hierdurch konnten personenbezogene Daten wie Klarnamen, Anschriften, E-Mail-Adressen sowie zum Teil Telefonnummern von bis zu 25.000 Personen abgerufen werden. Die Schwachstelle wurde zügig geschlossen, indem der Online-Shop abgeschaltet wurde. Die betroffenen Kunden wurden sicherheitshalber über den Vorfall informiert.

Für Webanwendungen, die über das Internet kommunizieren, gelten besonders hohe Anforderungen, um die Vertraulichkeit der personenbezogenen Daten zu gewährleisten. Oftmals wird der Absicherung durch technische und organisatorische Maßnahmen gegen ungewollte Zugriffe oder Angriffe über das Internet zu wenig Beachtung geschenkt. Ein qualifiziertes Datenschutzkonzept auf der Grundlage eines entsprechenden IT-Sicherheitskonzeptes kann der verantwortlichen Stelle Klarheit über die Risiken und die erforderlichen Maßnahmen zu deren Eindämmung verschaffen. Auf diese Weise wird der Verantwortliche seiner Pflicht zur Einhaltung der Sicherheit der Verarbeitung gemäß Art. 5 Abs. 1 lit. f DS-GVO gerecht.

Die sogenannte SQL-Injection stellt einen der bekanntesten und häufigsten Angriffsvektoren auf Webanwendungen dar und findet sich regelmäßig unter den TOP 10 der häufigsten Sicherheitsrisiken für Webanwendungen des Online Web Application Project (OWASP). Vor dem Hintergrund, dass der Vorfall durch eine vollständige Umsetzung der für die Programmiersprache PHP geltenden Empfehlungen vermeidbar gewesen wäre, wurde eine Verwarnung gemäß Art. 58 Abs. 2 lit. b) DS-GVO ausgesprochen.

3.3 Prüfung von Windows 10 im kommunalen Bereich

Wie in meinem letzten Tätigkeitsbericht angekündigt, habe ich die Prüfung des Einsatzes des Betriebssystems Windows 10 im Hinblick auf die Telemetriedatenübertragung auf den kommunalen Bereich ausgeweitet. Zuvor habe ich die kommunalen Spitzenverbände über die anstehende Prüfung informiert.

Wie schon in der Landesverwaltung wurde die Prüfung bei fünf Verantwortlichen initiiert.

Kernanforderungen wurden von den meisten Verantwortlichen erfüllt.

Zum Zeitpunkt der Prüfung setzten die meisten geprüften Verantwortlichen die „Enterprise"-Edition von Windows 10 ein und hatten die Telemetriestufe „security" eingestellt. Durch weitere technische Maßnahmen konnten sie die Übermittlung von personenbezogenen Telemetriedaten an Microsoft unterbinden. Lediglich eine Kommune verwendete noch die „Professional"-Edition und konnte keine Unterbindung der Telemetriedatenübertragung nachweisen.

In mehreren Fällen zeigte sich Nachbesserungsbedarf bei der Dokumentation der getroffenen Maßnahmen. Auf entsprechende Hinweise hin wurde eine überarbeitete Dokumentation vorgelegt.

Mit dem Abschluss der Prüfung rechne ich noch im 1. Halbjahr 2023.

3.4 Abschluss der datenschutzrechtlichen Prüfung von 50 niedersächsischen Kommunen

In meinem vorhergehenden Tätigkeitsbericht (J 4.4) habe ich über die Fortführung der Kommunalprüfung berichtet. In die anlassunabhängige Prüfung einbezogen wurden vier Landkreise, drei kreisfreie Städte, drei große selbständige Städte, 30 Städte und Gemeinden sowie zehn Samtgemeinden. Die Prüfung konnte im Jahr 2022 abgeschlossen werden.

Prüfung allgemeiner Pflichten

Im ersten Teil der Prüfung wurden erneut die allgemeinen Pflichten der Verantwortlichen abgefragt. Hierzu zählten Angaben zum Verzeichnis der Verarbeitungstätigkeiten (VVT), zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA), zum Umgang mit Datenschutzverletzungen und zur Bearbeitung von Auskunftsersuchen im Sinne von Art. 15 DS-GVO. Die Prüfung dieser Bereiche ermöglichte einen Vergleich mit den Ergebnissen der ersten Kommunalprüfung.

Hinzu kamen spezifische Fragen zum Wohngeld (bei den Landkreisen) bzw. zum Melderecht (bei den Städten und Gemeinden) sowie abschließend zum Umgang mit personenbezogenen Daten bei der Akteneinsicht (§ 29 Verwaltungsverfahrensgesetz). Das Melderecht wurde gewählt, da in diesem Bereich umfangreiche personenbezogene Daten der Einwohnerinnen und Einwohner von fast allen Kommunen verarbeitet werden. Da die Landkreise nicht als Meldebehörde tätig sind, wurde für diese der Bereich des Wohngeldes gewählt, um einen abgegrenzten Bereich mit sensiblen Sozialdaten einzubeziehen. Sowohl das Melderecht als auch das Wohngeldrecht boten Gelegenheit, die von den Kommunen definierten Verarbeitungstätigkeiten in diesen Bereichen abzugleichen. Die Frage zum Akteneinsichtsrecht wurde gewählt, da alle Kommunen auf Antrag Akteneinsicht gewähren und ich in der Vergangenheit Beschwerden zu diesem Thema erhalten habe.

Datenschutzrechtliche Wichtigkeit des VVT

Der Schwerpunkt lag auf dem VVT, da hier von den Kommunen Auszüge mit Bezug zum Wohngeld bzw. Melderecht angefordert wurden. Den Verantwortlichen sollte dadurch verdeutlicht werden, wie wichtig die Führung des VVT ist. Die gesetzliche Verpflichtung zur Führung eines VVT dient dazu, dass sich die Verantwortlichen für jede einzelne Verarbeitungstätigkeit Gedanken zum Schutz der personenbezogenen Daten machen. Unter Bezug auf die ein-

gesetzten Mittel der Verarbeitung ist eine Risikoanalyse durchzuführen und es sind geeignete Maßnahmen zu ergreifen, um ein potentielles Risiko zu minimieren oder bestenfalls auszuschließen. Ein sorgfältig und gewissenhaft geführtes VVT dient dem Schutz vor Datenschutzverletzungen.

Durch die Angaben in diesem Bereich und die Vorlage der Auszüge bin ich zu dem Ergebnis gekommen, dass der Begriff „Verarbeitungstätigkeit" von den Kommunen weitgehend einheitlich ausgelegt wird, auch wenn eine unterschiedliche Detailtiefe vorhanden ist.

Datenschutz-Folgenabschätzungen (DSFA)

Eng verbunden mit dem VVT und der Risikoanalyse ist die DSFA. Diese ist unter anderem bei allen Verarbeitungstätigkeiten erforderlich, die in der Liste nach Art. 35 Abs. 4 DS-GVO (sogenannte DSFA Muss-Liste) aufgeführt sind. Nicht allen Kommunen war diese Liste bekannt. Obgleich diese Liste die Verarbeitungstätigkeiten enthält, die der Prüfung zu Grunde lagen, haben die betroffenen Kommunen mit unnötigem Aufwand selbst den Bedarf für eine DSFA geprüft, ihn erkannt und anschließend eine DSFA erstellt.

Sofern diese noch nicht vorlag, wurde mir gegenüber in der weit überwiegenden Zahl der Fälle die Durchführung angekündigt und dargelegt, aus welchen Gründen eine DSFA noch nicht erfolgte. Insgesamt konnten im Vergleich mit der vorangegangenen Prüfung Verbesserungen festgestellt werden.

Interne Verfahren wurden etabliert

Für die Umsetzung der Meldung von Datenschutzverletzungen sowie des Auskunftsrechts haben fast alle der geprüften Kommunen interne Prozesse etabliert, um den gesetzlichen Anforderungen im erforderlichen Umfang und fristgerecht nachzukommen. Nur vereinzelt gibt es noch Nachholbedarfe.

Grundsätzlich schwärzen

Der letzte Prüfungsteil widmete sich der Durchführung einer datenschutzkonformen Akteneinsicht. In den letzten Jahren sind bei mir regelmäßig Beschwerden eingegangen, in denen vorgetragen wurde, dass personenbezogene Daten von verfahrensunbeteiligten Personen nicht ausreichend geschwärzt wurden. Aus diesem Grund sollten die Kommunen darlegen, wie sie mit Akteneinsichtsgesuchen im Verwaltungsverfahren umgehen und das Recht auf informationelle Selbstbestimmung Dritter umsetzen. In der Regel sind sich die Kommunen ihrer datenschutzrechtlichen Verpflichtung bewusst. Dennoch waren Unsicherheiten vorhanden. Aufgrund der unterschiedlichen Größe der

geprüften Kommunen rührten diese zum Teil daher, dass einige in der Vergangenheit sehr selten Akteneinsichtsgesuche im Sinne des Verwaltungsverfahrensgesetzes erhalten hatten. Dies habe ich zum Anlass genommen, die Kommunen für die Beachtung des Rechts auf informationelle Selbstbestimmung von Dritten zu sensibilisieren.

Fazit

Im Vergleich mit der vorhergehenden Kommunalprüfung gibt es deutliche Verbesserungen bei der Beachtung der datenschutzrechtlichen Anforderungen. Große Fortschritte gab es bei den Vorkehrungen zur Meldung von Datenschutzverletzungen. Des Weiteren sind die meisten Kommunen bei der Erstellung ihres VVT weit fortgeschritten. Lediglich im Bereich der DSFA sind weiterhin Schwierigkeiten vorhanden. Abschließend bleibt festzuhalten, dass die Größe einer Kommune nicht dafür ausschlaggebend ist, inwieweit sie ihre datenschutzrechtlichen Verpflichtungen erfüllt. Viel eher ist entscheidend, wie sehr sich die Verantwortlichen in den Kommunen mit der Umsetzung der datenschutzrechtlichen Vorgaben befassen und hierfür Ressourcen freihalten.

Ergebnisse der Kommunalprüfung 2018 (Kurzlink): https://t1p.de/bericht-kommunen

3.5 Zensus 2022 – erste Volkszählung unter Geltung der DS-GVO

Wie ist die datenschutzrechtliche Bilanz der verantwortlichen Stellen in Niedersachsen?

Im Jahr 2022 fand – nach elf Jahren – wieder eine europaweite Volkszählung statt. Der Fachbegriff hierfür ist Zensus. Der ursprünglich für das Jahr 2021 geplante Zensus war aufgrund der Corona-Pandemie um ein Jahr auf 2022 verschoben worden. Ich war bereits im Vorfeld von den verantwortlichen Stellen in Niedersachsen, insbesondere dem Landesamt für Statistik Niedersachsen (LSN), intensiv eingebunden worden.

Gegenstand des Zensus

Vorbefragung im Herbst 2021

Die Befragungen im Rahmen des Zensus 2022 begannen im Herbst 2021 mit der Vorbefragung zur Gebäude- und Wohnungszählung. Hierbei wurde im Vorfeld ein Teil der Eigentümer von Gebäuden bzw. Wohnungen vom LSN angeschrieben, um zu klären, ob die angeschriebene Person tatsächlich auskunftspflichtig ist. Die eigentlichen Zensusbefragungen begannen dann im Mai 2022. Hierbei fanden parallel verschiedene Teile des Zensus statt.

Beginn der Befragung im Mai 2022

Gebäude- und Wohnungszählung

Mit der Gebäude- und Wohnungszählung wurden die Eigentümer von Haus- oder Wohnungseigentum befragt. Es handelte sich um eine sogenannte Vollbefragung, d. h. befragt wurden sämtliche Eigentümer in Deutschland. Die Aufforderung zur Teilnahme erfolgte per Post.

Ein weiterer wichtiger Teil des Zensus war die sogenannte Haushaltebefragung. Hierbei wurden ca. 10 Prozent der Bevölkerung als Stichprobe befragt; diese Adressen wurden im Zufallsprinzip ermittelt. Hintergrund ist, dass auch Register wie das Melderegister zur Erstellung der anonymen Statistik herangezogen werden. Daher genügt eine ergänzende Stichprobenbefragung der Haushalte. Die Ergebnisse der Stichprobenbefragung werden dann auf ganz Deutschland mathematisch hochgerechnet. Die Haushaltebefragung dieser ausgewählten Haushalte erfolgte über Erhebungsbeauftragte, die sich mit einer Terminankündigungskarte im Briefkasten anmeldeten.

Wohnheime und Gemeinschaftsunterkünfte

Der dritte Teil des Zensus bezog sich auf Wohnheime und Gemeinschaftsunterkünfte. Hier fand ebenfalls eine Vollbefragung statt, d. h. die Befragung bezog sich jeweils auf alle Bewohner.

Wiederholungsbefragung

Schließlich fand im Zeitraum von Sommer bis Herbst 2022 die sogenannte Wiederholungsbefragung statt. Sie diente der Qualitätssicherung. Hierbei wurden bei einem kleinen Teil der aufgesuchten Haushalte einige der Fragen aus der Haushaltebefragung zu Überprüfungszwecken nochmals gestellt.

Die verantwortlichen Stellen in Niedersachsen

Gemeinsame Verantwortlichkeit

Der Zensus 2022 wurde vom Bund, den Bundesländern und den Erhebungsstellen in den Kommunen durchgeführt. Hierbei besteht in Niedersachsen folgende datenschutzrechtliche Verantwortlichkeit. Es besteht zum einen eine gemeinsame Verantwortlichkeit des Statistischen Bundesamts und des LSN. Zum anderen besteht eine gemeinsame Verantwortlichkeit des LSN und derjenigen niedersächsischen Kommunen, in denen Erhebungsstellen bestehen.

kommunale Erhebungsstellen

Der Ablauf des Zensus vor Ort wurde durch diese sogenannten örtlichen Erhebungsstellen organisiert. In Niedersachsen bestanden Erhebungsstellen in Gemeinden mit mindestens 30.000 Einwohnern; im Übrigen bei den Landkreisen. Damit bestanden in Niedersachsen rund 50 Erhebungsstellen. Die Erhebungsstellen bestellten und beaufsichtigten die Erhebungsbeauftragten und koordinierten die Befragung vor Ort. Die Erhebungsstellen waren nicht befugt, Auswertungen der erhobenen Daten selbst vorzunehmen oder durch Dritte vornehmen zu lassen.

Erhebungsbeauftragte

Die Erhebungsbeauftragten wurden von der örtlichen Erhebungsstelle mit der Befragung in einem konkreten Gebiet beauftragt. Die Erhebungsbeauftragten waren insofern Teil der örtlichen Erhebungsstelle. Soweit Erhebungsbeauftragte ehrenamtlich tätig waren, erhielten sie eine Aufwandsentschädigung.

3 Millionen Auskunftspflichtige in Niedersachsen

Die erforderliche Vorbereitung und Organisation des Zensus allein in Niedersachsen wird an folgenden Zahlen deutlich: Es wurden ca. 7000 niedersächsische Erhebungsbeauftragte beauftragt. Insgesamt, bezogen auf die oben dargestellten drei parallelen Teile des Zensus, gab es ungefähr 3 Millionen Auskunftspflichtige allein in Niedersachsen.

Datenschutzrechtliche Bilanz

Die Befragungen im Rahmen des Zensus 2022 sind am Ende des Berichtsjahres abgeschlossen gewesen. Die statistischen Ämter des Bundes und der Länder werden die Befragungen zu Statistiken umwandeln; diese Ergebnisse des Zensus werden im November 2023 erwartet. Wie ist nun also die datenschutzrechtliche Bilanz?

Ergebnisse liegen im November 2023 vor

Einhaltung des Rückspielverbots

Um es vorwegzunehmen: Der wichtigste Grundsatz des Zensus, nämlich das gesetzliche Verbot der Verwendung von erhobenen Zensusdaten zu allgemeinen Verwaltungszwecken, wurde eingehalten. Dieses sogenannte Rückspielverbot untersagt beispielsweise, das Melderegister mittels erhobenen Zensusdaten zu korrigieren oder erhobene Zensusdaten dem Finanzamt mitzuteilen. Anders ausgedrückt: Der Zensus 2022 erfolgt nur zur Erstellung von Statistiken. Die Statistiken sind anonym. Ein etwaiger Verstoß gegen das Rückspielverbot ist mir zu keinem Zeitpunkt bekannt geworden. Der wichtigste Grundsatz des Zensus ist damit eingehalten worden.

Keine Korrektur von Registern

Der Zensus dient nur anonymen Statistiken

Soweit im Rahmen der Zensuserhebung zunächst auch persönliche Identifikationsangaben, insbesondere Kontaktdaten und das konkrete Geburtsdatum, abgefragt worden sind, weise ich auf Folgendes hin: Hierbei handelt es sich lediglich um sogenannte Hilfsmerkmale, die nur der Durchführung des Zensusverfahrens dienen. Die Hilfsmerkmale werden zum frühestmöglichen Zeitpunkt von den abstrakten Antworten (sogenannte Erhebungsmerkmale) getrennt und nach Erreichen der statistischen Ziele gelöscht. Die Erhebung von Hilfsmerkmalen steht daher in Einklang mit dem einzigen gesetzlich erlaubten Ziel des Zensus, Statistiken zu erstellen.

nur zu statistischen Zwecken – Hilfsmerkmale werden gelöscht

Grundsätze des Zensus vom Bundesverfassungsgericht vorgegeben – bereits vor Geltung der DS-GVO

fachspezifische inländische Gesetze erforderlich

Ein weiterer Hinweis ist mir wichtig: Die Geltung der DS-GVO hat – neben geänderten Maßnahmenbefugnissen meiner Behörde – inhaltlich nicht den schon zuvor hohen datenschutzrechtlichen Standard bei der Durchführung des Zensus geändert. Dies beruht zum einen darauf, dass auch die DS-GVO bei staatlichem Tätigwerden stets ein bereichsspezifisches inländisches Gesetz verlangt, auf das die konkrete Datenverarbeitung gestützt werden kann. Diese bereichsspezifischen Gesetze des Bundes und des Landes Niedersachsen waren jeweils schon vor Geltung der DS-GVO aus Anlass des jeweiligen Zensus erlassen worden. Auch unter Geltung der DS-GVO bedurfte es daher dieser Spezialgesetze, um die Datenverarbeitung überhaupt vornehmen zu dürfen. Zudem ist der Zensus maßgebend durch das Volkszählungsurteil aus dem Jahr 1983 geprägt; die darin vom Bundesverfassungsgericht aufgestellten Grundsätze wiesen bereits vor Geltung der DS-GVO den höchsten datenschutzrechtlichen Standard auf. Hier ist namentlich das bereits genannte, vom Bundesverfassungsgericht vorgegebene Rückspielverbot zu nennen.

Im Rahmen von Beschwerden und Datenpannen war ich in folgenden Einzelfällen mit dem Zensus 2022 befasst.

Zwei Beschwerden

zu Unrecht zur Auskunft aufgefordert

Ich erhielt insgesamt zwei Beschwerden zu verantwortlichen Stellen in Niedersachsen. In beiden Fällen hat sich jeweils ein Bürger an mich gewandt, der zu Unrecht zu einer Auskunft im Rahmen des Zensus aufgefordert worden war. Diese Aufforderung bezog sich jeweils auf die Gebäude- und Wohnungszählung. Die Adresse, auf die sich das Aufforderungsschreiben bezog, war dem jeweiligen Bürger nicht bekannt. Die Ursache dieser Verwechslung war nicht aufklärbar. Gerade durch das bereits beschriebene Rückspielverbot, d. h. dem Verbot einer Rückmeldung von Zensusvorgängen in die allgemeine Verwaltung, wäre eine Korrektur etwaig fehlerhafter zugrundeliegender Register sogar unzulässig gewesen. Es war auch zu berücksichtigen, dass durch einfaches Ankreuzen im entsprechenden Fragebogen dem LSN als Rückantwort mitgeteilt werden konnte, dass man nicht Eigentümer eines Gebäudes unter der angefragten Anschrift ist. Ich habe in dieser Konstellation gegenüber dem LSN einen Hinweis erteilt.

Fünf Datenpannen aufgrund unbeabsichtigten menschlichen Fehlverhaltens

In fünf Fällen haben mir einzelne kommunale Erhebungsstellen Datenpannen gemäß Art. 33 DS-GVO gemeldet, die durch unbeabsichtigtes menschliches Fehlverhalten vorfielen.

In einem der Fälle stand die Zusendung eines einzelnen ausgefüllten Erhebungsbogens an einen dritten Auskunftspflichtigen im Raum. Allerdings war der Sachverhalt nicht aufklärbar, sodass keine aufsichtsbehördliche Maßnahme erlassen werden konnte.

In einem weiteren Fall bestanden widersprüchliche Angaben zu der Frage, ob ein Erhebungsbogen dem Erhebungsbeauftragten zugegangen oder noch beim Auskunftspflichtigen sei. Es stand

jedenfalls fest, dass der Erhebungsbogen keinem unbefugten Dritten zugegangen ist, sodass ein Fehlverhalten der kommunalen Erhebungsstelle – in Person des Erhebungsbeauftragten – nicht festgestellt werden konnte.

Fahrlässiges Fehlverhalten wird der kommunalen Erhebungsstelle zugerechnet

Ein anderer Fall wies einen groben Grad von Fahrlässigkeit auf. Hierbei hatte ein Erhebungsbeauftragter seine Tasche mit Erhebungsunterlagen bei einem kurzfristigen Zugwechsel in einer S-Bahn stehen gelassen. Betroffen waren die Erhebungsbögen von 65 Haushalten an 19 Adressen. Die Betroffenen sind von der kommunalen Erhebungsstelle informiert worden. Da das fahrlässige Fehlverhalten des Erhebungsbeauftragten der kommunalen Erhebungsstelle zugerechnet wird, habe ich gegenüber der Erhebungsstelle eine Verwarnung ausgesprochen.

Zwei Diebstähle aus Autos

Zwei der fünf Datenpannen betrafen den Diebstahl von Erhebungsunterlagen.

Diebstahl aus unverschlossenem Auto

In einem dieser beiden Fälle waren aus dem unverschlossenen privaten Kfz eines Erhebungsbeauftragten während einer Haushaltsbefragung die ausgefüllten Fragebögen von zwei Haushalten und einer gewerblich genutzten Adresse entwendet worden. Der Verlust ist aufgrund des deutlichen Fehlverhaltens des Erhebungsbeauftragten, der die Unterlagen in einem unverschlossenen Auto zurückgelassen hatte, der kommunalen Erhebungsstelle zuzurechnen. Ich habe daher gegenüber der Erhebungsstelle eine Verwarnung ausgesprochen.

Einbruch in verschlossenes Auto

In einem anderen Diebstahlsfall war das verschlossene private Auto eines anderen Erhebungsbeauftragten auf einem Parkplatz aufgebrochen worden. Hierbei wurde eine Tasche mit den Erhebungsbögen der Haushaltebefragung entwendet. Betroffen waren 42 Haushalte an 29 Adressen. In diesem Fall war aufgrund des verschlossenen Autos der Datenschutzverstoß, verursacht durch den Einbruchsdiebstahl eines Dritten, der kommunalen Erhebungsstelle nicht zurechenbar. Ich habe in diesem Fall die Erhebungsstelle gemäß Art. 57 Abs. 1 Buchstabe d) und Art. 58 Abs. 1 Buchstabe d) DS-GVO datenschutzrechtlich sensibilisiert und auf die Vorgaben der DS-GVO hingewiesen.

Umfangreiches FAQ zum Zensus

Zudem erreichten mich rund 20 Beratungsanfragen von Auskunftspflichtigen zur Rechtslage bzw. dem Ablauf des Zensus. Diese Fragen betrafen beispielsweise den gesetzlich nach Landesrecht vorgegebenen Ausschluss der Betroffenenrechte während des laufenden Zensus; insofern verweise ich auf meine Ausführungen im Tätigkeitsbericht 2021, Seite 132 ff. Weitere Fragen bezogen sich auf die Zulässigkeit von Auftragsverarbeitern im Rahmen des Zensus. Auch insofern verweise ich auf meinen Tätigkeitsbericht aus dem Jahr 2021.

Auch die Frage der Zulässigkeit der Erhebung von Hilfsmerkmalen wurde an mich herangetragen. Hierzu habe ich die Rechtslage oben bereits erläutert. Angesichts der ungefähr 3 Millionen Auskunftspflichtigen beim Zensus 2022 in Niedersachsen bin ich überzeugt, dass mein umfangreiches FAQ zum Zensus 2022 auf meiner Webseite erheblich dazu beigetragen hat, etliche Einzelfragen von zahlreichen Auskunftspflichtigen ohne individuellen E-Mail-Verkehr zu beantworten. In diesem FAQ habe ich in 60 Fragen und Antworten alle denkbaren Einzelfragen in kurzer und verständlicher Weise abstrakt für die niedersächsischen Bürgerinnen und Bürger beantwortet.

abstrakte Rechtsberatung

Fazit

Abschließend möchte ich anmerken, dass jede der genannten Datenpannen das Vertrauen berührt, das die Bürgerinnen und Bürger, die ja zur Auskunft verpflichtet sind, den zuständigen verantwortlichen Stellen im Rahmen des Zensus entgegenbringen. Allerdings sind diese vereinzelten Datenpannen, die auf menschlichem Fehlverhalten von teils ehrenamtlich tätigen Erhebungsbeauftragten beruhen, in Relation zu setzen zu der ordnungsgemäßen Tätigkeit von rund 7000 niedersächsischen Erhebungsbeauftragten und ungefähr 3 Millionen Auskunftspflichtigen in Niedersachsen. Daher ziehe ich das Resümee, dass die verantwortlichen Stellen in Niedersachsen das ihnen entgegengebrachte Vertrauen im Rahmen des Zensus 2022 gerechtfertigt haben.

verantwortliche Stellen in Niedersachsen gut aufgestellt

3.6 Prüfung in der allgemeinen Landesverwaltung

2022 habe ich anlassunabhängig die staatlichen Gewerbeaufsichtsämter (GAA) geprüft, um die Einhaltung der DS-GVO zu kontrollieren.

Ergänzend zur Kommunalprüfung – nun anlassunabhängige Prüfung in der allgemeinen Landesverwaltung

Nachdem bereits zahlreiche Kommunen von mir einer solchen Prüfung unterzogen worden waren, habe ich nun die anlassunabhängigen Prüfungen auf einen Teil der allgemeinen Landesbehörden ausgedehnt. Hintergrund der Auswahl war, dass in Landesbehörden wie den GAA in stärkerem Maß personenbezogene Daten von Bürgerinnen und Bürgern verarbeitet werden als in obersten Landesbehörden, in denen die einzelnen Vorgänge überwiegend auf Gesetzgebung, strukturelle Organisationsentscheidungen und abstrakte Rechtsfragen bezogen sind. Zudem besteht durch die sehr ähnliche Struktur der einzelnen GAA eine Vergleichbarkeit der geprüften Häuser; auf diese Weise lassen sich etwaige Verbesserungsbedarfe eindeutiger identifizieren. Geprüft wurden alle zehn niedersächsischen GAA.

Landesoberbehörden bewusst ausgewählt

Prüfung allgemeiner Pflichten sowie bereichsspezifischer Themen

Da die Pflichten der DS-GVO seit fast fünf Jahren gelten, stand bei der Prüfung nicht mehr die Durchführung der Umsetzungsphase, sondern die Einhaltung der nunmehr geltenden Pflichten im Vordergrund. Die Prüfung bestand im Wesentlichen aus einer Aufforderung, jeweils einen Fragebogen mit 16 Detailfragen zu beantworten. Hierbei habe ich in Teilbereichen die Einhaltung der datenschutzrechtlichen Pflichten zu den Themen Verzeichnis der Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung geprüft. Zudem bezog sich meine Prüfung auf organisatorische Vorkehrungen für den Fall etwaiger Datenschutzverletzungen und bei Auskunftsersuchen. Ein weiterer Prüfungsteil bezog sich bereichsspezifisch auf die Frage der Weitergabe personenbezogener Daten bei Nachbarschaftsbeschwerden und den Ablauf bei Akteneinsicht in Hinblick auf Daten beschwerdeführender Nachbarn. Hintergrund ist, dass ergänzend zu den Zuständigkeiten der GAA beispielsweise für Gefahrenprävention und Umweltschutz Beschwerderechte der Bürger bei den GAA bestehen. Daher bot sich als fachspezifisches Thema der datenschutzrechtliche

Umsetzungsphase der DS-GVO steht nicht mehr im Vordergrund

Umgang der GAA mit Nachbarschaftsbeschwerden, d. h. von Anwohnern an den Betrieben, an.

Die staatlichen Gewerbeaufsichtsämter sind datenschutzrechtlich gut aufgestellt

Die Auswertung der Antworten hat ergeben, dass die Gewerbeaufsichtsämter datenschutzrechtlich gut aufgestellt sind. Die datenschutzrechtlichen Vorgaben, soweit im Rahmen der Prüfung abgefragt, werden eingehalten. Aus der Auswertung geht zudem hervor, dass ein Datenschutzbewusstsein auf erfreulich hohem Niveau vorhanden ist. Es gab daher bei keinem der geprüften GAA einen Anlass zu einer Beanstandung.

Datenschutzbewusstsein auf erfreulich hohem Niveau

Ergänzende Vor-Ort-Prüfung

Im 1. Quartal 2023 werde ich zudem die schriftliche Prüfung durch Vor-Ort-Prüfungen ergänzen. Hierbei werde ich zufällig, d.h. unabhängig vom Ergebnis der schriftlichen Prüfung, ausgewählte GAA in Bezug auf die organisatorische Absicherung im Rahmen der Bearbeitung von Vorgängen vor Ort prüfen.

3.7 Transparenz ist Pflicht – Veröffentlichung von Corona-Beihilfen ist rechtmäßig

Während der Corona-Pandemie waren Beihilfezahlungen an Unternehmen eine wichtige Maßnahme, um Lockdown-Einschränkungen abzumildern. Diese Beihilfezahlungen durften veröffentlicht werden.

Im Berichtsjahr und im Jahr zuvor erreichten mich mehrere Anfragen, die sich auf eine Veröffentlichung von Corona-Beihilfen auf der Webseite der in öffentlicher Hand befindlichen niedersächsischen Investitions- und Förderbank (NBank) bezogen. Konkret waren zahlreiche Unternehmen aufgelistet, die staatliche Beihilfen zur Unterstützung während der Corona-Pandemie, namentlich zur Überbrückung während der Lockdown-Einschränkungen, erhalten hatten. Die Anfragenden waren durchweg nicht selbst betroffen. Sie richteten lediglich die Frage an mich, ob es datenschutzrechtliche Bedenken gegen die Veröffentlichung solcher Empfängerlisten durch eine öffentliche Stelle gibt.

Anfragende waren nicht selbst betroffen

Veröffentlichung stützt sich auf zwingende Pflicht gemäß Art. 6 Abs. 1 Buchstabe c DS-GVO

Im Zusammenhang mit den Unternehmensnamen sind teilweise auch personenbezogene Daten betroffen, beispielsweise als Teil des Unternehmensnamens. Allerdings waren die veröffentlichten Beihilfen an die Bedingungen geknüpft gemäß dem „Rahmen für staatliche Beihilfen zur Stützung der Wirtschaft angesichts des derzeitigen Ausbruchs von Covid-19“. Diese Rahmenvorgabe wurde umgesetzt in der „Vierten geänderten Bundesregelung Kleinbeihilfen 2020“ vom 12.02.2021, die in § 4 Abs. 4 eine solche Veröffentlichungspflicht ausdrücklich vorsieht. Diese Pflicht bezog sich auf Einzelbeihilfen von mehr als 100.000 Euro beziehungsweise von mehr als 10.000 Euro in den Bereichen Landwirtschaft und Fischerei. Die Veröffentlichungen der NBank hielten sich in diesem gesetzlichen Rahmen. Daher stützt sich die Veröffentlichung auf eine zwingende Pflicht nach Art. 6 Abs. 1 Buchstabe c DS-GVO. Ich habe den Anfragenden daher mitgeteilt, dass hinsichtlich der Veröffentlichung durch die NBank keine datenschutzrechtlichen Bedenken bestehen.

keine datenschutzrechtlichen Bedenken

3.8 Datenübermittlung durch Berufskammer – Amtshilfe ist keine Rechtsgrundlage

Mich erreichte eine Beschwerde, die sich auf die Übermittlung personenbezogener Daten durch eine Berufskammer an eine andere öffentliche Stelle bezog. Die Berufskammer berief sich hierbei auf Amtshilfe, welche jedoch keine ausreichende Rechtsgrundlage für die Übermittlung personenbezogener Daten darstellt.

Dass eine Berufskammer als öffentliche Stelle eine gesetzliche Übermittlungsbefugnis benötigt, um personenbezogene Daten an eine andere öffentliche Stelle zu übermitteln, verdeutlicht der folgende Praxisfall.

Kammermitglied stellt Rechnung aus

Ein Bürger hatte eine Rechnung von einem selbstständigen Rechtsberater, der Kammermitglied einer Berufskammer ist, erhalten. In einem sozialgerichtlichen Klageverfahren gegen eine Unfallkasse wollte der Bürger erreichen, dass diese ihm den Rechnungsbetrag erstattet. In diesem Klageverfahren hatte das Sozialgericht die Rechnung als überhöht bewertet und festgestellt, dass die Vorgaben zur Abrechnung nicht eingehalten wurden. Die daraufhin korrigierte Rechnung des Kammermitgliedes wollte der Bürger nun von der Berufskammer überprüfen lassen. In der Folge leitete die Berufskammer die korrigierte Rechnung an die bereits im Klageverfahren beteiligte Unfallkasse weiter, ohne dass der Bürger hierin eingewilligt hatte. Gegen diese Übermittlung von der Berufskammer an die Unfallkasse hat sich der Bürger schließlich mit einer Beschwerde an mich gewandt.

Berufskammer übermittelt Rechnung an Unfallkasse

Bereichsspezifische Übermittlungsbefugnis erforderlich

In meinem datenschutzrechtlichen Kontrollverfahren stützte sich die Berufskammer für die Übermittlung der Rechnung an die Unfallkasse auf Amtshilfe; sie habe die Rechtsauffassung der Unfallkasse zu der nun korrigierten Rechnung einholen wollen. Dieser Argumentation konnte ich nicht folgen, da die allgemeinen Regelungen zur Amtshilfe in den §§ 4 ff. Verwaltungsverfahrensgesetz keine Übermittlungsbefugnis für personenbezogene Daten darstellen. Vielmehr muss sich eine solche Übermittlungsbefugnis gemäß Art. 6 Abs. 2 und 3 DS-GVO bereichsspezifisch und hinreichend konkret aus dem jeweiligen Fachrecht ergeben.

Amtshilfe stellt keine Übermittlungsbefugnis dar

Ergebnis des Kontrollverfahrens

Eine solche bereichsspezifische Übermittlungsbefugnis für diese Datenübermittlung existierte nicht. Auch eine Einwilligung des Bürgers hatte nicht vorgelegen. Zudem können rechtliche Fragestellungen auch in anonymisierter Form zwischen öffentlichen Stellen erörtert werden. Es war somit in keinem Fall erforderlich, personenbezogene Daten an die Unfallkasse zu übermitteln. Der Beschwerde habe ich stattgegeben und gegenüber der Berufskammer eine Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b DS-GVO ausgesprochen.

Datenübermittlung ohne Rechtsgrundlage

J.4. Schule und Hochschule

4.1 Prüfung des Datenschutzniveaus an 50 niedersächsischen Schulen

Um einen Überblick über das bestehende Datenschutzniveau an den niedersächsischen Schulen zu gewinnen und daraus Handlungsempfehlungen abzuleiten, habe ich ein Kontrollverfahren an 50 niedersächsischen Schulen durchgeführt. Abgefragt wurden die Datenschutzkonzepte von weiterführenden allgemeinbildenden Schulen sowie Berufsbildenden Schulen (BBS).

Fragen zum digitalen und analogen Umgang mit personenbezogenen Daten von Schülern und Schülerinnen

Schwerpunkt: digitales Lernen

Die digitale Transformation des Unterrichts in Schulen hat sich durch die Covid-19-Pandemie beschleunigt. Das vom Bundesverfassungsgericht im Jahr 2021 entwickelte Grundrecht auf schulische Bildung von Schülerinnen und Schülern verpflichtet Schulen, auch Fernunterricht anzubieten, wenn Schulen einmal (z. B. pandemiebedingt) geschlossen sind. Daher betraf ein Drittel der Fragen der schriftlichen Prüfung auch die von den Schulen genutzten Lernplattformen, Videokonferenzsysteme und Messenger. Über die datenschutzkonforme Einbindung dieser Systeme in den digitalen Unterricht hatte ich bereits im Jahr 2021 in Form von FAQs und eines „Eckpunktepapiers zum Einsatz von Videokonferenzsystemen an Schulen“ aufgeklärt (Tätigkeitsbericht 2021, Seite 138 ff.). Nun wollte ich feststellen, ob diese Grundlagen auch in der Praxis beachtet werden.

Ergebnis: Durchschnittsnote 3

Licht und Schatten

Erfreulich ist, dass die Schulleiter und Schulleiterinnen aller geprüften Schulen mich über Unzulänglichkeiten, die im Rahmen der internen Prüfung des Datenschutzkonzepts erkannt wurden, selbstständig informierten. Zum Beispiel kam es vereinzelt vor, dass vorübergehend keine Datenschutzbeauftragte oder kein Datenschutzbeauftragter (DSB) bestellt war. Die Tätigkeit als DSB ist ein verantwortungsvolles Amt, das Lehrer und Lehrerinnen neben ihrer pädagogischen Arbeit wahrnehmen. Ich spreche mich dafür aus, dass Lehrkräf-

te, die dieses Amt wahrnehmen, in ihrer Unterrichtsverpflichtung entlastet werden, insbesondere, damit sie genug Zeit haben, sich fortzubilden.

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist das Herzstück einer jeden Datenverarbeitung. Es dokumentiert alle relevanten Verarbeitungstätigkeiten auf deren Basis dann – je nach Risiko eines Verarbeitungsvorgangs – weitere Pflichten, wie zum Beispiel eine Datenschutzfolgenabschätzung, anknüpfen. Ich konnte feststellen, dass Schulen oftmals nicht hinreichend die Löschfristen von personenbezogenen Daten von Schülerinnen und Schülern in einem VVT dokumentieren. Der pauschale Verweis auf den Runderlass des niedersächsischen Kultusministeriums vom 29.05.2020 (Nds. MBl. Nr. 32/2020 S. 696) ist nicht ausreichend, sondern es muss je nach Art der personenbezogenen Information die konkrete Löschfrist benannt werden. Darüber hinaus muss jede Schule ein Löschkonzept in Form von technischen und organisatorischen Maßnahmen vorhalten, in dem geregelt ist, wie die ordnungsgemäße Löschung der Daten sichergestellt wird.

Software als Unterrichtsgegenstand in BBS

Im Hinblick auf den Einsatz von digitalen Lernplattformen habe ich festgestellt, dass die allgemeinbildenden Schulen größtenteils auf bekannte Plattformen, wie IServ oder die Niedersächsische Bildungscloud (NBC) zurückgreifen, um das Recht der Schülerinnen und Schüler auf „digitales Lernen" zu erfüllen. Auffällig war, dass berufsbildende Schulen oftmals auf Softwareanbieter zurückgreifen, die in der beruflichen Praxis zur Anwendung kommen. Datenschutzrechtlichen Bedenken im Hinblick auf den Einsatz von US-Produkten wurde oftmals damit begegnet, dass diese Software nicht nur das digitale Lernen ermöglichen würde, sondern selbst Gegenstand des Unterrichts sei.

Ich spreche mich bereits seit längerem dafür aus, das Programmieren und die Informatik als Pflichtfach in den Schulen einzuführen. Man sollte aber auch die Gelegenheit ergreifen, den Datenschutz zu einem Unterrichtsthema insbesondere an Berufsbildenden Schulen zu machen. Allerdings gilt auch beim Einsatz von Software als Unterrichtsgegenstand, dass die Schulen als datenschutzrechtlich Verantwortliche stets ihrer Rechenschaftspflicht aus Artikel 5 Absatz 2 Datenschutz-Grundverordnung (DS-GVO) nachkommen müssen.

Künstliche Intelligenz (KI) als digitaler Lehrer

Die Schulprüfung hat zudem ergeben, dass sechs von 50 Schulen sogenannte intelligente Tutorensysteme einsetzen (sog. Online-Diagnose-Anwendungen). Intelligente Tutorensysteme sind Softwareanwendungen, die mit Methoden des maschinellen Lernens das Lernverhalten von Schülerinnen und Schülern aufzeichnen, bewerten und daraus automatisiert Schlussfolgerungen für zukünftige Lehrinhalte ziehen, die die Systeme selbstständig generieren. Die

Software passt die Aufgaben an den Wissenstand der jeweiligen Schülerin und des jeweiligen Schülers an, wodurch eine neue Form des individualisierten Lernens entstehen soll. Auf Basis der Testergebnisse kann die Software individuelle Elternbriefe erstellen, die vom Lehrer oder von der Lehrerin nur noch unterzeichnet werden müssen. In pädagogischer Hinsicht sprechen sich Studien schon seit einiger Zeit für die Nutzung solcher Systeme im Unterricht aus.[1]

Entsprechend offensiv bewirbt das Niedersächsische Kultusministerium den Einsatz des „digitalen Lehrers" an den Schulen. In datenschutzrechtlicher Hinsicht ist offenkundig, dass die Algorithmen der intelligenten Tutorensysteme eine große Menge an Metadaten von Schülerinnen und Schülern sammeln. Auf meine Nachfrage beim Niedersächsischen Kultusministerium, ob und, wenn ja, welche Stelle die Datenschutzkonformität der intelligenten Tutorensysteme geprüft hat, wurde auf das Vergabeverfahren verwiesen, in dessen Rahmen die Anbieter versichern müssten, die Vorgaben der DS-GVO einzuhalten. Eine konkrete Prüfung der Software habe nicht stattgefunden, verantwortlich für den konkreten Einsatz seien die Schulen und die jeweiligen Schulleiterinnen und Schulleiter.

Angesichts des Lehrkräftemangels, der nach Aussage der Expertenkommission der Kultusministerkonferenz noch „20 Jahre bestehen bleibt", liegt es auf der Hand, dass diese Systeme zukünftig verstärkt zum Einsatz kommen. Nach meiner Auffassung definieren diese Systeme das Verhältnis zwischen Schülerinnen und Schülern und Lehrkräften vollkommen neu, was in der Informationskampagne des Niedersächsischen Kultusministeriums nicht kommuniziert wird. Ich betone ausdrücklich, dass nach meiner Auffassung „der Datenschutz" dem Einsatz dieser Systeme nicht entgegensteht. Allerdings gibt es nach der DS-GVO einige grundlegende Spielregeln zu beachten.
Erforderlich ist:

- eine Rechtsgrundlage, die die Datenverarbeitung erlaubt,
- die Schülerinnen und Schüler sowie ggf. die Sorgeberechtigten im besonderen Maße zu informieren,
- ggf. auch eine gesonderte Datenschutzfolgenabschätzung.

Letztlich ist die verantwortliche Schule auch in der Rechenschaftspflicht, erklären zu müssen, dass die Software auf die hohe Zahl von Metadaten angewiesen ist, um zu funktionieren.

1 Hillmayr et al. Digitale Medien im mathematisch-naturwissenschaftlichen Unterricht der Sekundarstufe – Einsatzmöglichkeiten, Umsetzung und Wirksamkeit, 2017.

Die digitale Transformation des Lernens nur mit Datenschutzstrategie

Die geprüften niedersächsischen Schulen haben grundsätzlich ihre Hausaufgaben erfüllt. Insbesondere solche Schulen, die die Vorlagen der Regionalen Landesämter für Schule und Bildung (RLSB) verwenden, haben überdurchschnittlich gut abgeschnitten. Mit den RLSB stehe ich in einem regelmäßigen Austausch, den ich gerne auch in Zukunft fortsetzen werde. Ich stelle aber auch fest, dass das Niedersächsische Kultusministerium keine Datenschutzstrategie hat. Es gibt keine konsequente Auseinandersetzung mit Konzepten der datenschutzkonformen Integration von Software (auch in die NBC). Es ist in dieser Hinsicht keine Option, auf die Schulen zu verweisen, weil letztlich auch das Niedersächsische Kultusministerium als oberste Schulbehörde darauf hinzuwirken hat, dass das Schulwesen den geltenden (Datenschutz-)Vorschriften entspricht (§ 120 Abs. 2 Niedersächsisches Schulgesetz). Für die digitale Transformation des Lernens werden Leitlinien aus einer Hand benötigt, in denen die Medienkompetenz der Lehrerinnen und Lehrer, die Medientechnik, aber eben auch der Datenschutz strategisch mitgedacht werden.

Ausblick

Die Weiterentwicklung der Digitalisierung der Schulen und die sich anbahnende digitale Transformation des Lernens kann nur gelingen, wenn das individuelle Recht auf Bildung und das Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler in einen harmonischen Gleichklang gebracht werden.

Hierfür sind gemeinsame Anstrengungen von Schulen, der RLSB sowie strategische Impulse des Niedersächsischen Kultusministeriums erforderlich. Gerne begleite ich die beteiligten Institutionen bei der digitalen Transformation des Bildungssystems.

4.2 Eckpunkte für den Einsatz von Lernplattformen in den Schulen

Bei der Digitalisierung des Schulunterrichts gilt es, die Chancen digitalen Lernens zu nutzen und zugleich möglichen datenschutzrechtlichen Risiken zu begegnen. Hierzu geben meine Eckpunkte den Schulen die erforderliche Hilfestellung und Orientierung.

Digitales Lernen kann und muss datenschutzkonform erfolgen

In den niedersächsischen Schulen werden zunehmend digitale Lernplattformen im Unterricht eingesetzt. Dieser Trend wurde durch die Corona-Pandemie noch verstärkt. Die eingesetzten Lernumgebungen variieren im Hinblick auf die integrierten Anwendungen deutlich. Neben der Bereitstellung und Organisation digitaler Lerninhalte werden oftmals vielfältige elektronische Kommunikationsmöglichkeiten zwischen den Lernenden und Lehrenden eröffnet. Dabei wird eine Vielzahl von personenbezogenen Daten der Schülerinnen und Schüler verarbeitet. Dies birgt besondere datenschutzrechtliche Risiken. Beim Einsatz digitaler Lernplattformen gelten daher datenschutzrechtliche Anforderungen. Dies muss bei der Auswahl der Anwendungen beachtet werden.

Eckpunkte als Hilfestellung für die Schulen

Um sowohl den niedersächsischen Schulen als auch den Anbietern digitaler Lernplattformen eine Hilfestellung zu bieten, welche datenschutzrechtlichen Standards einzuhalten sind, habe ich im Sommer 2022 „Eckpunkte für den Einsatz von Lernplattformen in Schulen“ entwickelt und auf meiner Webseite veröffentlicht. Mit diesen Eckpunkten werden die gewonnenen Erkenntnisse aus der Begleitung der Niedersächsischen Bildungscloud sowie weiterer Digitalisierungsprojekte im Schulbereich (wie das Projekt DigLU – Digitales Lernen unterwegs) in rechtlicher und technischer Hinsicht zusammengeführt.

Eckpunkte zum Download (Kurzlink): https://t1p.de/EckpunkteLernplattformen

Die Eckpunkte habe ich auch an das Niedersächsische Kultusministerium sowie die Regionalen Landesämter für Schule und Bildung gesandt.

4.3 Hacking eines Schulservers und Veröffentlichung von personenbezogenen Daten im Internet

Im Berichtzeitraum hat mir eine Schule gemäß Artikel 33 Abs. 1 DS-GVO gemeldet, dass im Zuge eines Hacking-Angriffs sämtliche Daten auf dem Schulverwaltungsserver verschlüsselt wurden. Bei meinen Recherchen stieß ich darüber hinaus im Internet auf den erbeuteten Datensatz.

Veröffentlichung von personenbezogenen Daten und Erpressungsversuch

Im Zuge routinemäßiger Recherchen hat mein Fachreferat für den technischen und organisatorischen Datenschutz im Nachgang der Meldung herausgefunden, dass Daten der betroffenen Schule im Internet veröffentlicht wurden. Die Vorgehensweise, dass Angreifer Daten verschlüsseln und bei Nichtzahlung eines Lösegeldes die Daten im Internet veröffentlichen, ist bekannt und wurde augenscheinlich im vorliegenden Fall angewandt. Eine Sichtung der Daten hat ergeben, dass u. a. Fotos von Schülerinnen und Schülern, Lehrkräften sowie Erziehungsberechtigten, Jahrbücher, Namen und Adressdaten von Schülerinnen und Schülern in Verbindung mit Passwörtern für den Zugang zu einem Portal zur Schulanmeldung sowie korrigierte und benotete Klassenarbeiten aus den Jahren 2017 und 2018 in Form von Scans veröffentlicht wurden.

Weitere Analysen des Vorfalls erforderlich

Die Schule wurde umgehend auf die Veröffentlichung der Daten hingewiesen und gebeten, Strafanzeige zu erstatten sowie die Löschung der Daten zu erwirken. Zudem wurde die Schule um Mitteilung der getroffenen Maßnahmen zur Sicherung des Schulverwaltungsservers gebeten. Die vom Landeskriminalamt Niedersachsen federführend vorgenommene Analyse und Dokumentation des Vorfalls wurde durch mein technisches Fachreferat ausgewertet.

Ergebnis des Kontrollverfahrens

Ursache nicht feststellbar

Im Ergebnis konnte nicht festgestellt werden, wie der Angriff auf das Schulsystem erfolgt ist (Phishing oder „gewaltsames“ Eindringen) oder was für die Schutzverletzung tatsächlich ursächlich war. Es gab keine Hinweise, dass die technisch-organisatorischen Maßnahmen der Schule vor dem Vorfall unzureichend waren. Ebenso wenig waren andere Versäumnisse nachweisbar. Die Veröffentlichung der Daten im Internet war der Schule in diesem Fall somit nicht zuzurechnen. Ich habe daher von aufsichtsbehördlichen Maßnahmen abgesehen und Hinweise für zukünftige technische und organisatorische Schutzmaßnahmen gegeben.

4.4 Zertifizierung von schulischen Bildungssystemen – Das DIRECTIONS Forschungsprogramm

Die Datenschutz-Grundverordnung (DS-GVO) sieht als ein wichtiges Instrument zum Nachweis der Datenschutzkonformität von Verarbeitungsvorgängen die Möglichkeit einer Zertifizierung vor. Gerade in der komplexen Produktlandschaft schulischer Bildungssysteme können Zertifikate helfen, Schülern, Schulverantwortlichen, Eltern und der Aufsicht mehr Transparenz, Sicherheit und Vertrauen zu geben, damit diese Systeme dateschutzkonform zum Einsatz kommen. Das Projekt DIRECTIONS (Data Protection Certification for Educational Information Systems)[1] setzt an dieser Stelle an.

Die Forderung nach digitaler Unterstützung schulischer Lernprozesse und einer begleitenden Unterstützung durch Vermittlung von Medienkompetenz findet sich in Positionspapieren und schulpolitischen Programmen in Niedersachsen über viele Legislaturperioden hinweg. Förderprogramme, wie etwa der länderübergreifende „DigitalPakt Schule“ oder das Maßnahmenpaket Digitale Bildung im niedersächsischen „Masterplan Digitalisierung“ zeigen die Relevanz und das Nachholbedürfnis in diesem Bereich der Digitalisierung. Massiv verstärkt wurde der Druck auf ein schnelleres Vorankommen in diesem Bereich in Folge der Pandemie.

In Folge der Corona-Pandemie zeigte sich deutlich, wie notwendig der Einsatz digitaler Informations- und Kommunikationsformate war und ist. Gleichzeitig wurden die Lücken in der Infrastruktur und der brauchbaren Anwendungen noch deutlicher sichtbar. In dieser Ausgangslage kommt aus Sicht des Datenschutzes zum Tragen, dass gerade Schülerinnen und Schüler und ebenfalls deren Lehrerinnen und Lehrer zu den besonders schützenswerten Betroffenen zählen.

Das Projekt DIRECTIONS wird von einem Konsortium, bestehend aus dem Karlsruher Institut für Technologie (KIT), der Universität Kassel und der datenschutz cert GmbH getragen. Das Projekt hat eine Laufzeit von sechs Jahren. Die Projektziele sind Konzeption und Erprobung einer Datenschutzzertifizierung von schulischen Lernsystemen, wie insbesondere Content-Plattformen, virtuelle Klassenzimmer, Videokonferenzsysteme oder Systeme zur Unterstützung des Unterrichts. Dies schließt sowohl den Betrieb dieser Systeme im Rahmen einer Auftragsverarbeitung durch den System-Anbieter als auch in gemeinsamer Verantwortung durch System-Anbieter und System-Kunden ein. Unterstützt wird das Konsortium durch eine Vielzahl von assoziierten und beratenden Mitgliedern, unter anderem von Mitarbeiterinnen meiner Behörde im Rahmen der Beratung durch die Datenschutzkonferenz. Als erstes Projektergebnis wurde in dieser Berichtsperiode der Zertifizierungsgegenstand abgegrenzt, beschrieben und veröffentlicht. Das Konformitätsbewertungsprogramm, der Kriterienkatalog, Schutzklassen- sowie Modularitätskonzepte werden folgen. Ich werde weiter über Ergebnisse dieses Vorhabens berichten.

1 DIRECTIONS – Data Protection Certification for Educational Information Systems (directions-cert.de).

J.5. Wirtschaft

5.1 Warnungen genossenschaftlicher Banken vor Smart-Data-Verfahren

Im Berichtszeitraum habe ich 89 genossenschaftliche Banken in Niedersachsen vor der Durchführung von acht sogenannten Smart-Data-Verfahren gewarnt.

Bereits im 26. Tätigkeitsbericht habe ich von einem Verfahren gegen eine Bank wegen einer Klassifikation von Kunden berichtet. Die Rechtmäßigkeit der Verarbeitung von Kundendaten für Werbezwecke durch Kreditinstitute spielte auch in diesem Berichtsjahr eine erhebliche Rolle in meiner aufsichtsbehördlichen Tätigkeit. Dabei bin ich auf schwerwiegende Verstöße gegen die DS-GVO aufmerksam geworden.

Kundenprofiling

Meiner Warnung vorausgegangen war eine Vor-Ort-Kontrolle bei einem niedersächsischen Kreditinstitut. Durch die Kontrolle konnte ich mir ein umfassendes Bild von den durchgeführten Verfahren machen.

Bei Smart-Data-Verfahren handelt es sich in diesem Kontext um Algorithmen, die vor allem aus den bei der Bank vorhandenen personenbezogenen Daten eine Wahrscheinlichkeit dafür berechnen, dass Kunden bei werblicher Ansprache ein bestimmtes Produkt erwerben. So wird zum Beispiel berechnet, ob eine Kundin oder ein Kunde derzeit ein hohes Interesse an einem Immobilienkredit, einer Kreditkarte oder einem Wertpapiersparplan hat. Zur Bildung der entsprechenden Scorewerte werden unter anderem Zahlungsverkehrsdaten analysiert und bei einigen Verfahren auch Daten über das Wohnumfeld der Kundinnen und Kunden von externen Dienstleistern hinzugezogen.

So werden beispielsweise zur Berechnung, ob eine Kundin oder ein Kunde Interesse an einem Konsumentenkredit hat, 162 Datenfelder ausgewertet. Darunter auch folgende Informationen aus den Zahlungsverkehrsdaten:

- Bezug von sozialen Leistungen,
- Ausgaben für Haushalt und Lebensmittel,
- Höhe der Fahrzeugkosten,

- Höhe der „Grundkosten“, u. a. für Energieversorger,
- Höhe des Gehalts- oder Renteneingangs,
- Höhe der Auszahlungen an Geldautomaten,
- Umsätze in der Kategorie E-Payment, z. B. Paypal und Amazon.

Zudem werden von externen Dienstleistern Daten zum Wohnumfeld angekauft und fließen in die Berechnung ein, zum Beispiel:

- Anteil der Bevölkerung mit Realschulabschluss,
- durchschnittliche Anzahl der Kinder pro Haushalt,
- durchschnittliche Anzahl der Personen pro Haushalt,
- Nettoeinkommen der Haushalte,
- durchschnittliche private Kaufkraft für Hypothekendarlehen, Konsumentenkredite, Lebensversicherungen und private Krankenversicherungen,
- Anteil der Bevölkerung mit Familienstand „geschieden“.

Keine Rechtsgrundlage

Meine Prüfung hat ergeben, dass die Bank sowohl eine sogenannte Hinweislösung als auch eine Einwilligungslösung genutzt hat. Bei der Hinweislösung erhalten die betroffenen Kundinnen und Kunden ein Formularblatt mit der Überschrift „Besondere datenschutzrechtliche Hinweise zu individuellen Informationen, Empfehlungen und Angeboten“. Darin war unter anderem beschrieben, dass zehn verschiedene Kategorien personenbezogener Daten für die Bildung eines Kundenprofils verarbeitet werden. Zudem wurde den Kundinnen und Kunden mitgeteilt, dass sie der Verarbeitung widersprechen könnten.

Rechtsgrundlage sollte dann Art. 6 Abs. 1 lit. f DS-GVO sein. Danach können Verantwortliche personenbezogene Daten auf Grundlage einer Interessenabwägung durchführen. Bei der Abwägung dürfen die Rechte und Freiheiten der betroffenen Personen nicht die berechtigten Interessen des Verantwortlichen überwiegen.

Die Banken argumentierten unter anderem, dass die Verarbeitung im Interesse der Kundinnen und Kunden sei. Es sei in ihrem Sinne, wenn ihre Bank sie bestmöglich kenne und ihnen zum richtigen Zeitpunkt das richtige Produkt anbiete.

Dieser Auffassung habe ich widersprochen. Insbesondere die Verarbeitung von Zahlungsverkehrsdaten stellt einen sehr tiefgehenden Eingriff in das Recht auf Datenschutz aus Art. 8 Grundrechtecharta dar. Zahlungsverkehrsdaten weisen eine besondere Sensibilität auf. Sie geben Aufschluss über das Konsumverhalten, Beziehungen zu Mitmenschen, die wirtschaftliche Lage und persönliche Vorlieben der betroffenen Personen.

Solche Eingriffe können nicht mit dem Interesse an besonders zielgerichteter Werbung gerechtfertigt werden. Das Interesse der betroffenen Personen am Schutz ihrer personenbezogenen Daten überwiegt in diesen Fällen weit. Bei einer Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO sind unter anderem die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen. Diese müssen nicht erwarten, dass ihre Bank die bei ihr vorhandenen, sehr sensiblen Daten für die beschriebenen Analysen benutzt und erst recht nicht, dass noch weitere Daten aus externen Quellen für eine vermeintlich passgenaue Werbung verwendet werden. Die Datenschutzkonferenz (DSK) hat in ihrer Orientierungshilfe Direktwerbung deutlich gemacht, dass betroffene Personen kein Profiling für Werbezwecke auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO erdulden müssen, sondern hierfür eine wirksame Einwilligung in den jeweiligen Verarbeitungsvorgang notwendig ist.

OH Direktwerbung der DSK (Kurzlink): https://t1p.de/OHDirektwerbung

Während der Eingriff in die Rechte der betroffenen Personen hier schwerwiegend ist, gilt dies nicht für das Interesse der Banken an einer möglichst zielgerichteten Werbung. Es handelt sich zwar um ein berechtigtes Interesse, dieses hat aber kein besonderes Gewicht. Der Unionsgesetzgeber hat diese Wertung im Rahmen des Art. 21 Abs. 2 DS-GVO selbst vorgenommen, indem er betroffenen Personen bei jeder Verarbeitung für Zwecke der Direktwerbung ein voraussetzungsloses Widerspruchsrecht eingeräumt hat. Finden hingegen Verarbeitungen für andere Zwecke statt, muss die betroffene Person nach Art. 21 Abs. 1 DS-GVO bei einem Widerspruch Gründe vortragen, die sich aus ihrer besonderen Situation ergeben.

Auch Einwilligung verstößt gegen DS-GVO

Neben der Rechtfertigung über Art. 6 Abs. 1 lit. f DS-GVO kommt auch ein Einwilligungsformular zum Einsatz. Eine mit diesem Formular eingeholte Einwilligung verstößt jedoch ebenfalls gegen DS-GVO, weil die erforderliche Granularität bei der Einholung der Einwilligung nicht gewahrt wird. Das bedeutet, dass den betroffenen Personen in der Einwilligungserklärung keine ausrei-

chenden Möglichkeiten zur Verfügung standen, um den Umfang der Verarbeitung ihrer personenbezogenen Daten zu steuern. Sie konnten in das Profiling für Werbezwecke lediglich insgesamt einwilligen oder dieses ablehnen. Nach Erwägungsgrund 43 der DS-GVO müssen jedoch für unterschiedliche Verarbeitungsvorgänge auch gesonderte Einwilligungen eingeholt werden, sofern dies angebracht ist. Diese Vorgabe war in dem vorliegenden Formular nicht beachtet worden.

Anhörung zu Untersagung

Wegen dieser schwerwiegenden Verstöße habe ich die Bank, bei der ich die Vor-Ort-Kontrolle durchgeführt habe, zu einer Untersagung der Verfahren angehört. Diese hat daraufhin die Verfahren sofort beendet und zugesagt, diese zunächst nicht wieder aufzunehmen, sodass die Untersagung nicht mehr notwendig war.

Warnung

Eine Warnung kann die Aufsichtsbehörde nach Art. 58 Abs. 2 lit. a DS-GVO aussprechen, wenn beabsichtigte Verarbeitungsvorgängen voraussichtlich gegen die DS-GVO verstoßen. Bei den Smart-Data-Verfahren habe ich mich dazu entschieden eine solche Warnung auszusprechen. Das von mir kontrollierte Kreditinstitut war als Pilotbank tätig und erklärte, dass einige der Verfahren bereits allen genossenschaftlichen Banken zur Verfügung stehen. Unklar war, bei wie vielen Banken die Verfahren bereits eingesetzt werden. Um die Banken davon abzuhalten, die Verfahren einzuführen und die personenbezogenen Daten ihrer Kunden ohne Rechtsgrundlage für werbliche Zwecke zu analysieren und damit schwerwiegende Verstöße gegen die DS-GVO zu begehen, habe ich mich dazu entschieden, die genossenschaftlichen Banken vor dem Einsatz dieser Verfahren zu warnen.

Nach der Warnung habe ich weitere Kontrollverfahren gegen niedersächsische Genossenschaftsbanken eingeleitet, um die Einhaltung der Datenschutz-Grundverordnung in diesem besonders sensiblen Bereich zu überprüfen. Die Verfahren dauern noch an.

5.2 Prüfung der Auftragsverarbeitungsverträge von niedersächsischen Webhostern

Um externe Dienstleister (Webhoster) und verantwortliche Webseitenbetreiber beim Abschluss von rechtskonformen Auftragsverarbeitungsverträgen zu unterstützen, habe ich mich 2022 an einer länderübergreifenden Kontrolle beteiligt und die Musterverträge von sechs großen Webhostern aus Niedersachsen überprüft. Auch die Datenschutzaufsichtsbehörden aus Berlin, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt und Bayern (LDA) beteiligten sich an dieser koordinierten Prüfung.

Viele Unternehmen und Organisationen betreiben ihre Internetseite über einen Webhoster. Dabei werden personenbezogene Daten von Besucherinnen und Besuchern der Seite verarbeitet. Häufig findet diese Datenverarbeitung im Auftrag des Verantwortlichen, also des Seitenbetreibers, statt. Das heißt, der Webhoster ist ein Auftragsverarbeiter. Um einen konkreten Rahmen für diese weisungsgebundene Tätigkeit festzulegen, müssen der Verantwortliche und der Auftragsverarbeiter in der Regel einen Vertrag zur Auftragsverarbeitung (AVV) schließen. Die Datenschutz-Grundverordnung (DS-GVO) beschreibt im Detail in Art. 28 DS-GVO, welche Rechte, Pflichten und Maßnahmen im AVV geregelt werden müssen.

FAQ zur Auftragsverarbeitung (Kurzlink): https://t1p.de/FAQAVV

Auf der Grundlage einer von den Aufsichtsbehörden erarbeiteten Checkliste habe ich sechs niedersächsische Webhoster angeschrieben und um Auskunft zur Ausgestaltung ihrer AVV gebeten. Die Checkliste wurde den Webhostern zur Verfügung gestellt und ist auch auf meiner Webseite abrufbar.

Checkliste (Kurzlink): https://t1p.de/ChecklisteAVV

Die Auswertung der Rückmeldungen der Unternehmen hat erfreulicherweise ergeben, dass den Unternehmen grundsätzlich bekannt war, welche Anforderungen Art. 28 DS-GVO an die Ausgestaltung eines AVV stellt. Allerdings zeigte die Prüfung auch, dass in der Praxis im Detail in verschiedenen Regelungsbereichen noch erheblicher Verbesserungsbedarf bestand, um die Verträge in Einklang mit den Anforderungen aus Art. 28 DS-GVO zu bringen und letztlich die Rechte und Freiheiten der Betroffenen zu schützen.

Die Prüfung habe ich im Dezember 2022 abgeschlossen. Die identifizierten Defizite konnte ich im kooperativen Dialog mit den Unternehmen beseitigen und somit die Rechtmäßigkeit der AVV herstellen. Für 2023 plane ich, eine vergleichbare Prüfung in einem anderen Wirtschaftsbereich durchzuführen.

5.3 Zwangsweise Benutzung von Fitnesstrackern verboten

Ein Fitnessstudio hatte die Teilnahme an Kursen von der Verwendung eines bestimmten Fitnesstrackers abhängig gemacht. Da dies datenschutzrechtlich nicht gerechtfertigt ist, habe ich diese Vorgabe verboten.

Aufgrund von Beschwerden stellte ich fest, dass in manchen Fitnessstudios die Teilnahme an bestimmten Kursen, in denen Belastungssport getrieben wird, nur nach dem Erwerb sowie der Nutzung von Fitnesstrackern und einer Handy-App eines namhaften Herstellers von kabellosen Herzfrequenzmessgeräten ermöglicht wird.

Mit den Messutensilien sollen während des Trainings in Echtzeit Leistungsdaten von Clubmitgliedern in Form der Herzfrequenz, der Intensität und des Kalorienverbrauches erfasst werden, die dann automatisch über eine Cloudanwendung zum Hersteller hochgeladen und dort gespeichert werden. Die Teilnehmer haben die Möglichkeit, ihre Daten über die App einzusehen, um ihre Trainingsfortschritte zu verfolgen.

Bei den erhobenen und gespeicherten Angaben handelt es sich um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO. Eine Notwendigkeit zur verpflichtenden Nutzung dieser Datenerhebung und -nutzung ist nicht erkennbar.

Derartige Daten dürfen daher nach Art. 7 Abs. 1 DS-GVO nur mit informierter und freiwillig erteilter Einwilligung der Betroffenen und nur für festgelegte Zwecke verarbeitet werden. Die Wirksamkeit der eingeholten Einwilligungen steht in Zweifel, wenn der Erwerb der für die Datenerfassung und Wiedergabe benötigten Produkte für die Nutzung von Trainingsangeboten als verbindlich erklärt wird, ohne dass dies für die Erfüllung der Dienstleistungsverträge mit den Studios erforderlich wäre.

Verantwortung durch Hersteller delegiert

Bedeutsam in dem geprüften Fall ist auch, dass die Verantwortung für die Datenverarbeitung nach den mit dem Hersteller getroffenen Vereinbarungen nicht bei ihm, sondern bei den Studiobetreibern liegt. Denn der Hersteller gibt

Vertragsregelungen zur Nutzung seiner Produkte vor, die ihm die Position des Auftragsverarbeiters der Daten zuweisen, dessen Aufgabe darin besteht, Namen und Trainingsdaten der Nutzer zu sammeln, zu speichern und zu nutzen.

Den an der Nutzung der Messgeräte interessierten Studiobetreibern wird dagegen die Position der datenschutzrechtlich Verantwortlichen zugeschrieben. Diese können angeblich entscheiden, welche Daten im System gespeichert werden und wie diese behandelt werden. Ferner sind sie auch für die Richtigkeit der Daten und die datenbezogenen Anfragen der Benutzer zuständig.

Mit dieser Vertragsregelung ist der Hersteller nicht selbst in der Verantwortung für die Datenverarbeitung, solange er im Rahmen der erteilten Weisungen der Studiobetreiber handelt. Ob derartige Weisungen tatsächlich möglich sind oder Verarbeitungsmodalitäten tatsächlich vorgegeben werden können, bezweifele ich.

Ungeachtet dessen übernehmen die Studiobetreiber bei Abschluss des Vertrages mit dem Hersteller aus freiem Entschluss sämtliche Pflichten, die sich zur Herstellung und Wahrung der Rechtmäßigkeit der Datenverarbeitung aus der DS-GVO ergeben. Dazu gehört sowohl die Einholung wirksamer Einwilligungen als auch die Sicherstellung der umfassenden Information über sämtliche Verarbeitungen, die nicht alle unter der Regie der Studiobetreiber erfolgen.

Dem Studiobetreiber wurde die Verarbeitung der Daten untersagt, weil er die Rechtmäßigkeit der Verarbeitung nicht darstellen konnte und sie auch nicht ersichtlich ist. Dagegen wurde Klage erhoben, eine Entscheidung des Verwaltungsgerichts steht noch aus.

Aufsichtsbehörde schreitet gegen Hersteller ein

Hinzu kommt ein weiteres datenschutzrechtliches Problem: Der Hersteller mit Sitz in einem anderen EU-Staat wurde Ende 2022 von der zuständigen nationalen Aufsichtsbehörde verwarnt und mit einer Geldbuße belegt. Nach Feststellung der Aufsichtsbehörde sind die vom Hersteller eingeholten Einwilligungen für die Verarbeitung der Maximum-Sauerstoffaufnahme und des Body-Mass-Indexes datenschutzrechtswidrig. Der Hersteller wurde zudem angewiesen, die Einholung der Einwilligungen neu zu organisieren.

Studiobetreiber, die sich bislang auf die Zuschreibung der Rolle des primär Verantwortlichen für die Datenverarbeitung durch den Hersteller eingelassen haben, stehen somit vor einem weiteren Problem.

5.4 Gewinnspiele, Werbung und Adresshandel

Mich haben mehrere Beschwerden gegen zwei Gewinnspielveranstalter erreicht. In einem Fall war den Gewinnspielteilnehmern nicht transparent, dass ihre Daten über das Gewinnspiel hinaus zu Werbezwecken verarbeitet werden. Im anderen Fall konnte nicht nachgewiesen werden, dass neben der Gewinnspielteilnahme eine Einwilligung für Werbeanrufe Dritter erteilt worden ist.

Transparenz

Die Anmeldung zum Gewinnspiel erfolgte in einem Fall telefonisch, im anderen Fall über eine Webseite. In dem Fall, in dem die Anmeldung telefonisch erfolgte, wurden die Adressangaben der Interessenten, die an Verlosungen zu einer sogenannten Sofortrente teilnahmen, ohne ihr Wissen und Wollen durch den Veranstalter anderen Firmen zu Werbezwecken verfügbar gemacht.

Rechenschaftspflicht

In dem Fall, in dem die Anmeldung zum Gewinnspiel auf der Webseite des Gewinnspielveranstalters erfolgte, konnte nicht nachgewiesen werden, dass die Beschwerdeführer das Formular zur Gewinnspielteilnahme versandt und die Einwilligung für Werbeanrufe Dritter abgegeben haben. Der Nachweis hätte durch die Vorlage entsprechender Servereinträge erfolgen müssen. Die Servereinträge hat der Gewinnspielveranstalter im Vorfeld ohne nachvollziehbaren Grund gelöscht.

Adresshändler und Lettershop-Verfahren

Interessenprofile

Gewinnspiele sind eine weitverbreitete Bezugsquelle von Adresshändlern, die Daten von potenziellen Werbeadressaten aus unterschiedlichen Quellen sammeln, auswerten und zu granularen und damit aussagenkräftigen Interessenprofilen zusammenführen, um sie für zielgruppengerechte Werbekampagnen anderer Unternehmen zu vermarkten.

Akteure

Die Zusammenarbeit zwischen Adresshändlern und Unternehmen, deren Waren und Dienstleistungen beworben werden sollen, erfolgt häufig arbeitsteilig. Soweit es um Briefwerbung geht, ist das sogenannte Lettershop-Verfahren noch weit verbreitet. Beim Lettershop-Verfahren arbeiten grundsätzlich drei Unternehmen zusammen: Das werbende Unternehmen, dessen Leistungen im Werbebrief angepriesen werden, der Adresshändler und der Lettershop. Der Lettershop ist dasjenige Unternehmen, das die Werbebriefe personalisiert, druckt und dem Versanddienstleister zum Versand übergibt. Das Werbematerial erhält der Lettershop vom werbenden Unternehmen. Den Datensatz desjenigen, dessen Interessenprofil gut zur beworbenen Leistung passt, erhält der

Lettershop dagegen vom Adresshändler. Der Adresshändler übermittelt diejenigen Datensätze, die im Vorfeld nach den vom werbenden Unternehmen vorgegebenen Kriterien selektiert worden sind. Diese Art der Zusammenarbeit führt insgesamt dazu, dass das werbende Unternehmen von den beworbenen Personen keine Kenntnis erhält. Im Werbebrief wird als Kontakt- und Anlaufstelle häufig der Adresshändler genannt, demgegenüber die Werbeadressaten ihre Betroffenenrechte geltend machen können.

Die Betroffenen erhalten so unerwünschte Werbebriefe von verschiedensten Unternehmen. Die in der Regel unauffällig platzierten Hinweise auf die Möglichkeit, einen Werbewiderspruch nach Art. 21 DS-GVO beim Adresshändler zu erheben, werden von den Betroffenen häufig nicht bemerkt.

Datenschutzrechtliche Verantwortlichkeit und Rechtmäßigkeit

Zieht man zur Beurteilung der datenschutzrechtlichen Verantwortlichkeit die Kriterien des Europäischen Datenschutzausschusses heran und berücksichtigt die Rechtsprechung des Europäischen Gerichtshofs zur datenschutzrechtlichen Verantwortlichkeit, spricht vieles für die Annahme einer gemeinsamen

datenschutzrechtlichen Verantwortlichkeit zwischen Adresshändler und werbenden Unternehmen.

Joint Controllership

Das werbende Unternehmen und der Adresshändler sind an der Festlegung der Zwecke und Mittel gemeinsam beteiligt. Sie haben gleichermaßen entscheidenden Einfluss auf das „Ob" und „Wie" der Selektion und Bewerbung von potenziellen Neukunden. Die Selektion und Ansprache der Werbeadressaten erfolgen auf der Grundlage konvergierender Entscheidungen des werbenden Unternehmens sowie des Adresshändlers und dienen gemeinsamen wirtschaftlichen Zwecken: Gewinn von Neukunden für das werbende Unternehmen und Verbesserung der Qualität der Leistungen des Adresshändlers. Letzteres ergibt sich daraus, dass der Adresshändler als im Werbebrief genannter Ansprechpartner für die Werbeadressaten das „Ob" und „Wie" der Reaktionen der Werbeadressaten für seine Interessenprofile nutzen und deren Aussagekraft dadurch erhöhen kann, was sich wiederum positiv auf die Qualität der Datensätze und Leistungen des Adresshändlers auswirkt.

Berechtigtes Interesse

Ich sehe ohne die vorherige Einholung einer Einwilligung derzeit keine Rechtsgrundlage für diese Praxis, für die die Adresshändler und werbenden Unternehmen ein überwiegendes berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DS-GVO anführen. Gegen die Legitimation aufgrund eines überwiegenden berechtigten Interesses spricht, dass weder der Adresshändler noch das werbende Unternehmen in einer vertraglichen Beziehung zu den Betroffenen steht, und es sich mit Blick auf die Bildung von granularen Interessenprofilen um Datenverarbeitungen mit erheblicher Eingriffstiefe handelt. Die bisher geübte Praxis, die Werbeadressaten z. B. auf den Gewinnlosen lediglich zu informieren, erscheint mir deshalb unzureichend.

Neubewertung des Geschäftsmodells

Das Geschäftsmodell der Adresshändler muss umgehend und umfassend kritisch neu bewertet werden. Sowohl mit Blick auf die datenschutzrechtlichen Verantwortlichkeiten der beteiligten Akteure im Lettershop-Verfahren als auch und vor allem in Bezug auf die Rechtmäßigkeit der Datenverarbeitungen. Um Wettbewerbsnachteile einzelner Unternehmen zu vermeiden, die aus bundesweit unterschiedlich strengen Anforderungen der Aufsichtsbehörden resultieren könnten, bemühe ich mich darum, eine bundesweit einheitliche Rechtsauffassung herbeizuführen.

5.5 Stellvertretung beim Auskunftsrecht zulässig

Immer wieder wird von Verantwortlichen behauptet, das Auskunftsrecht nach Art. 15 DS-GVO könne nur in eigener Person geltend gemacht werden und eine Vertretung durch einen Rechtsanwalt sei nicht zulässig. Diese Auffassung ist falsch.

Auskunftsrecht ist kein höchstpersönliches Recht

Auch 2022 erreichten mich eine Vielzahl von Beschwerden zum Recht auf Auskunft nach Art. 15 DS-GVO. Vielfach richteten sich die Beschwerden gegen Verantwortliche, die die Auskunft nicht oder vermeintlich nicht vollständig erteilt haben. In einem erwähnenswerten Einzelfall trug ein Rechtsanwalt eine Beschwerde gegen ein in Niedersachsen ansässiges Versicherungsunternehmen vor. Der Rechtsanwalt wurde von seinem Mandanten beauftragt eine Auskunft nach Art. 15 DS-GVO von dem Versicherungsunternehmen einzuholen bei dem der Mandant Versicherungsnehmer war.

Der Rechtsanwalt hatte bei der Versicherung bereits zuvor eine von seinem Mandanten unterzeichnete Prozessvollmacht und Vollmacht zur außergerichtlichen Vertretung vorlegt, um in der Hauptsache Forderungen aus dem bestehenden Versicherungsvertrag durchzusetzen. Die Vollmacht beinhaltete u. a. aber auch die Abgabe und den Empfang von einseitigen Willenserklärungen und Vornahme einseitiger Rechtsgeschäfte und auch die Entgegennahme von Zustellungen. Das Versicherungsunternehmen antwortete dem Rechtsanwalt innerhalb der Monatsfrist des Art. 12 Abs. 3 DS-GVO, dass es sich einer Auskunft nach Art. 15 DS-GVO um ein höchstpersönliches Recht handelt und deswegen keinerlei Korrespondenz in dieser Sache mit dem Anwalt erfolgt.

Im Rahmen des daraufhin eingeleiteten Prüfverfahrens trug die Versicherung auch mir gegenüber vor, dass sie der Auffassung ist, es handele sich bei dem Recht auf Auskunft um ein höchstpersönliches Recht, dieses könne nur selbst geltend gemacht werden. Eine Vertretung sei deshalb ausgeschlossen und aufgrund dessen werde eine Auskunft nach Art. 15 DS-GVO auch nur an den Betroffenen selbst übermittelt. Eine Vertretung, auch durch einen Rechtsanwalt, sei nicht möglich, so die Versicherung. Die vorgelegte Vollmacht des Rechtsanwalts würde hieran nichts ändern, da diese keine Einwilligung in eine Datenweitergabe durch die Versicherung an bzw. die Datenentgegennahme durch den Rechtsanwalt einschließen würde und somit eine Übersendung der Auskunft an den Rechtsanwalt nicht datenschutzkonform wäre, da keine der Voraussetzungen des Art. 6 Abs. 1 DS-GVO erfüllt sei.

Verhaltensregeln ändern nicht die DS-GVO

Ferner beruft sich die Versicherung auf den Code of Conduct (CoC, Verhaltensregeln) der Versicherungswirtschaft, dem die Versicherung beigetreten wäre. In diesem hieße es u. a., dass nur die berechtigte Person Auskunft erhält und auch wenn ein Bevollmächtigter sie verlangt, die Auskunft nur der betroffenen Person oder ihrem gesetzlichen Vertreter erteilt wird. (vgl. Art. 23 Abs. 4 des CoC der Versicherungswirtschaft). Dementsprechend habe die Versicherung gehandelt und die Auskunft unmittelbar an ihren Versicherungsnehmer übersandt.

Die grundlegende Auffassung des Versicherungsunternehmens teile ich nicht. Gründe, die die vorgelegte Vollmacht ungenügend erscheinen lassen sind nicht gegeben, da es hinsichtlich der Ausgestaltung einer Vollmacht zur Einholung einer Auskunft in der DS-GVO keine Regelung gibt. Das Auskunftsrecht nach Art. 15 DS-GVO ist kein Recht, bei dem eine Stellvertretung ausgeschlossen ist. Eine Stellvertretung nach §§164 ff. BGB ist zulässig, so dass ein Verantwortlicher einen Bevollmächtigten nicht mit dem Hinweis abweisen darf, dass ausschließlich der Betroffene selbst seine Rechte geltend machen kann.

Auch der Hinweis des Versicherungsunternehmens auf den CoC der Versicherungswirtschaft kann hier nicht als rechtliche Grundlage dienen, da es sich hierbei lediglich um eine freiwillige Selbstverpflichtung der Versicherungswirtschaft handelt, die höherrangiges Recht, also die DS-GVO und auch das BDSG nicht zu ändern vermag. Für den CoC liegt zudem seitens der Aufsichtsbehörden (bisher) keine Genehmigung vor, sodass der CoC keine Wirksamkeit entfalten kann.

Im vorliegenden Fall wurde das aufsichtsbehördliche Verfahren allerdings eingestellt, da die Versicherung zwar die Vollmacht als nicht ausreichend verwarf, aber den durch den Rechtsanwalt gestellten Antrag auf Auskunft akzeptiert und die Auskunft dem Versicherungsnehmer innerhalb der verlängerten Frist des Art. 12 DS-GVO unmittelbar übersandt und den bevollmächtigten Rechtsanwalt darüber in Kenntnis gesetzt hat.

Dem Anliegen des Betroffenen, nämlich dem Erhalt einer Auskunft nach Art. 15 DS-GVO, wurde demnach fristgerecht nachgekommen, sodass ich nicht weiter tätig werden musste.

5.6 Datenübermittlung an Inkassobüros ist zulässig

Immer wieder erreichen mich Beschwerden, es seien unzulässigerweise personenbezogene Daten an ein Inkassobüro weitegeleitet worden. In nahezu allen Fällen liegt kein datenschutzrechtlicher Verstoß vor.

Die Einziehung von offenen Geldforderungen durch ein Inkassobüro ist ein in der Wirtschaft etabliertes Verfahren. Der Gläubiger wendet sich bei Ausbleiben der fälligen Zahlung durch den Schuldner an ein Inkassobüro und überlässt diesem die Geltendmachung bzw. Einziehung der Forderung.

Datenschutzrechtlich darf das Unternehmen dem Inkassobüro die personenbezogenen Daten des Schuldners übermitteln, wo diese weiterverarbeitet werden dürfen. Eine Einwilligung der betroffenen Person, also des Schuldners, ist dazu nicht notwendig. Die datenschutzrechtliche Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten des Schuldners ergibt sich aus Art. 6 Abs. 1 lit. b) und f) DS-GVO. Die Datenverarbeitung ist zu Erfüllung des Vertrages (Entrichtung des vereinbarten Preises) bzw. aufgrund des berechtigten Interesses des Gläubigerunternehmens erforderlich.

In den Beschwerden wird teilweise der Vorwurf erhoben, es liege eine Personenverwechselung vor. Da Namen oftmals nicht einmalig sind, ist eine Personenverwechselung für die betroffene Person ärgerlich, zumal in diesen Fällen die Geldforderung gegenüber der betroffenen Person, dem vorgeblichen Schuldner nicht existiert. Zur Klärung sollten sich Betroffene in jedem Fall mit dem Inkassounternehmen in Verbindung setzen, um mitzuteilen, dass man die Forderung nicht ausgelöst hat und diese unbekannt ist. Anderenfalls besteht die Gefahr, dass das Inkassobüro seine Arbeit fortsetzt, einen Negativeintrag bei einer Auskunftei veranlasst und sich zudem die Personenverwechselung manifestiert, also weitere Verwechselungen erfolgen.

Auch kommt es vor, dass trotz Einwendungen gegen die Geldforderung oder Begleichung der Geldforderung der Betrag (nochmals) von einem Inkassobüro geltend gemacht wird. Auch hier sollte der Kontakt mit dem Inkassounternehmen zur Klärung gesucht werden.

Schließlich mache ich darauf aufmerksam, dass das Bestehen oder Nichtbestehen einer Geldforderung zivilrechtlich zu beurteilen ist und sich meine Kompetenz allein auf die datenschutzrechtliche Beurteilung der Verarbeitung personenbezogener Daten erstreckt.

5.7 DS-GVO steht Rechtsstreit nicht entgegen

Immer wieder erreichen meine Behörde Beschwerden über die Verarbeitung von personenbezogenen Daten in einem Rechtsstreit, insbesondere vor den Zivilgerichten. Es wird behauptet, schon die Übermittlung von personenbezogenen Daten im Vorfeld eines gerichtlichen Rechtstreits vom Anspruchsteller an seinen Rechtsanwalt sei datenschutzrechtlich unzulässig und erst recht die Offenbarung der Daten durch den Rechtsanwalt bzw. den Kläger gegenüber dem Gericht.

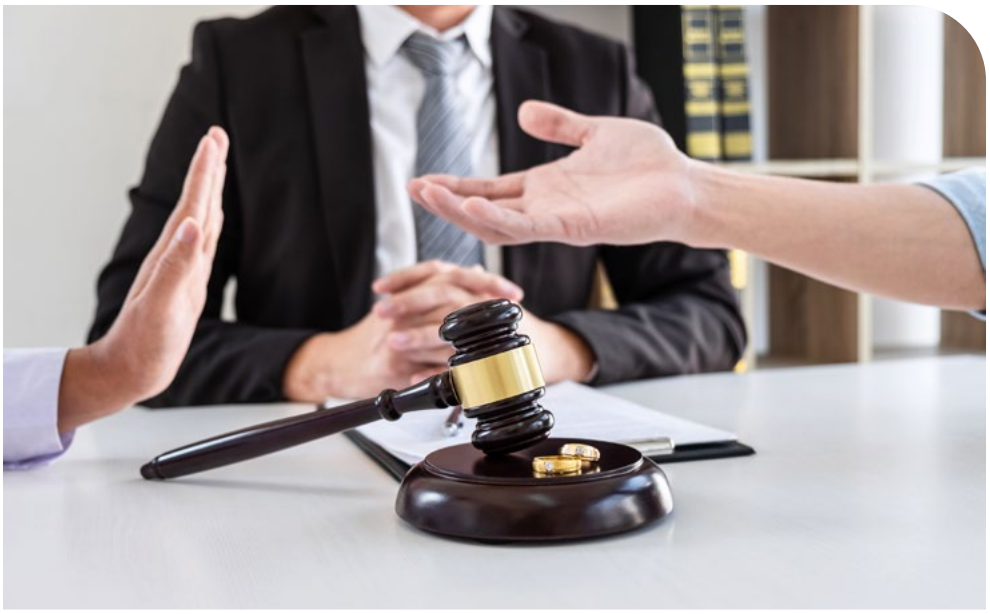
Gleiches wird eingewandt bei der Benennung von Zeugen oder Sachverständigen. Die betroffene Person ist häufig der Auffassung, dass die Zeugen oder Sachverständigen Kenntnis vom Rechtsstreit erhielten, was mit der DS-GVO unvereinbar sei.

In diesen Fällen unterliegen die Beschwerdeführer durchweg einem Irrtum. Abgesehen von ganz engen Ausnahmen ist die Verarbeitung und damit auch die Übermittlung von personenbezogenen Daten von den Prozessparteien an ihre Rechtsanwälte von Art. 6 Abs. 1 lit. f) DS-GVO gedeckt. Eine Ausnahme davon besteht nur dann, wenn die personenbezogenen Daten keinen Bezug zum Rechtsstreit haben.

Justizgewährleistungsanspruch überwiegt

Die Norm des Art. 6 Abs. 1 DS-GVO berücksichtigt nicht nur das Datenschutzinteresse der betroffenen Person, sondern auch die anerkennenswerten Interessen des Verantwortlichen an einer in engen Grenzen zulässigen Datenverarbeitung.[1] So ist nach Art. 6 Abs. 1 lit. f) DS-GVO die Verarbeitung und damit auch die Übermittlung personenbezogener Daten an Dritte, also an Rechtsanwälte und auch an die Gerichte, zulässig, soweit dies zur Wahrnehmung der berechtigten Interessen des Verantwortlichen, also des Anspruchstellers bzw. des Klägers erforderlich ist und nicht die Interessen oder Grundrechte der betroffenen Personen überwiegen. Dies ist bei der gerichtlichen, aber auch bei der außergerichtlichen Geltendmachung von Ansprüchen der Fall. Ein jeder hat das Recht seine Ansprüche unter Inanspruchnahme eines Rechtsanwalts oder mit gerichtlicher Hilfe durchzusetzen. Letzteres wird durch den Justizgewährleistungsanspruch nach Art. 47 EU-Grundrechte-Charta jeder Person eingeräumt. Das Recht erstreckt sich auch auf die Beibringung von Beweismitteln, die den Anspruch untermauern. Spiegelbildlich gilt dies ebenso für die Seite des Anspruchsgegners bzw. der Beklagtenseite. Es ist gerade die Funktion eines Rechtsstreits die unterschiedlichen Wahrnehmungen und Auffassun-

1 Vgl. VG Hannover, 08.12.2020, 10 A 1321/19



gen dem Gericht vorzutragen und einer Lösung zuzuführen. Dabei müssen die Prozessparteien und ihre Anwälte darauf achten, dass die übermittelten Daten nicht an Dritte außerhalb des gerichtlichen Verfahrens gelangen.

In den genannten Fällen sind auch die Voraussetzungen von Art. 6 Abs. 4 DS-GVO im Regelfall gegeben. Zumeist sind die personenbezogenen Daten aufgrund eines anderen Zweckes erhoben worden und werden nunmehr zum Zweck der gerichtlichen Geltendmachung eines Anspruchs verwendet. Dies ist nach den Art. 6 Abs. 4, 23 Abs. 1 lit. j) DS-GVO i.V.m. § 24 Abs. 1 Nr. 2 BDSG zulässig. Die Durchsetzung zivilrechtlicher Ansprüche ist explizit erwähnt.

Selbst besondere Kategorien personenbezogener Daten dürfen in einem Rechtsstreit verwendet werden. Grundlage hierfür ist Art. 9 Abs. 2 lit. f) DS-GVO, der die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen zulässt.

5.7 Praxistag Beschäftigtendatenschutz

Gelegentlich wird den Aufsichtsbehörden vorgeworfen, im datenschutzrechtlichen „Elfenbeinturm" zu sitzen. Um dieser Falscheinschätzung entgegenzuwirken, habe ich mich im Berichtszeitraum als Vorsitzende des AK Beschäftigtendatenschutz für einen Austausch der Aufsichtsbehörden mit Vertreterinnen und Vertretern der Wirtschaft im Bereich des Beschäftigtendatenschutzes (mit-) eingesetzt.

Siehe zum AK Beschäftigtendatenschutz auch E.1

Themenschwerpunkte

Am 19. Mai 2022 fand der vom Bayrischen Landesamt für Datenschutz und der Landesbeauftragten für den Datenschutz Niedersachsen ausgerichtete Praxistag im Hannover Congress Centrum (HCC) statt.

Die Veranstaltung richtete sich sowohl an Vertreterinnen und Vertreter aus der Wirtschaft (Bereich „HR") als auch an die datenschutzrechtlichen Aufsichtsbehörden. Ziel des Praxistages war es, sich in einem vertraulichen Rahmen ergebnisoffen über Thematiken, Entwicklungen und Fragestellungen rund um das Beschäftigungsverhältnis auszutauschen. Diese sollten aus verschiedenen Blickwinkeln beleuchtet werden, um ein gegenseitiges Verständnis hierfür entwickeln zu können.

Weitere Informationen unter: https://t1p.de/Beschaeftigtendatenschutz

Die Vorträge befassten sich mit Themen wie

- „Eignungsdiagnostische Grundlagen",
- „Folgen der Nichtbeachtung von wissenschaftlichen Erkenntnissen und Praxisgrundlagen für rechtliche Beurteilungen im Beschäftigtendatenschutz",
- „Negative Bewerbervorauswahl in der Praxis am Beispiel Online-Assessments",
- „Social Recruting & Active Sourcing",
- „KI im Recruiting & Personalmanagement",
- „Beschäftigtendatenschutz und Betriebsrat" sowie
- „Praxisrelevante Fragen in der aufsichtsbehördlichen Arbeit".

Zwischen den einzelnen Vorträgen sowie im Anschluss an alle Vorträge fand ein Austausch zwischen den insgesamt 32 Teilnehmerinnen und Teilnehmern aus der Wirtschaft sowie den datenschutzrechtlichen Aufsichtsbehörden statt.

Erkenntnisgewinn

Die aus dieser Veranstaltung gewonnenen Erkenntnisse wurden beziehungsweise werden genutzt, um neuere Entwicklungen im Bereich Beschäftigtendatenschutz rechtzeitig zu erkennen und diese bei Veröffentlichungen oder in der konkreten Fallbearbeitung berücksichtigen zu können.

J.6. Gesundheit und Soziales

6.1 Abschluss der mehrteiligen Krankenhausprüfung in Niedersachsen – Schwerpunktprüfung zum Verzeichnis der Verarbeitungstätigkeiten

In meinem vorhergehenden Tätigkeitsbericht habe ich bereits angekündigt, aufgrund des Ergebnisses der allgemeinen Krankenhausprüfung, eine Schwerpunktprüfung zum Verzeichnis der Verarbeitungstätigkeiten (VVT) durchzuführen. Die Auswertung der Prüfung von 30 Krankenhäusern im vergangenen Jahr hatte Unstimmigkeiten bezüglich der gesamten Anzahl von einzelnen Verarbeitungstätigkeiten sowie dem Inhalt der Dokumentation zu den einzelnen Verarbeitungstätigkeiten ergeben.

Datenschutzrechtliche Wichtigkeit des VVT

Gerade in Zeiten, in denen Krankenhäuser aus verschiedenen Gründen stark belastet sind, ist es nicht meine Absicht, diese zusätzlich zu belasten. Aus diesem Grund habe ich bei allen Prüfungen ausreichend lange Antwortfristen gewährt und Fristversäumnisse nicht geahndet. Gleichwohl war es mir ein Anliegen, die Verantwortlichen auf die Wichtigkeit der Führung eines VVT hinzuweisen und die Umsetzung zum Wohle der Patientinnen und Patienten zu kontrollieren.

Die gesetzliche Verpflichtung zur Führung eines VVT dient dazu, dass sich die Verantwortlichen zu jeder einzelnen Verarbeitungstätigkeit Gedanken zum Schutz der personenbezogenen Daten machen. Unter Bezug auf die eingesetzten Mittel der Verarbeitung muss eine Risikoanalyse durchführen werden. Zudem müssen geeignete Maßnahmen ergriffen werden, um ein potentielles Risiko zu minimieren oder bestenfalls auszuschließen. Ein sorgfältig und gewissenhaft geführtes VVT ist der beste Schutz vor einer Datenschutzverletzung.

Je nach Art des Verarbeitungsvorgangs müssen im VVT Angaben zu einer durchgeführten Datenschutz-Folgenabschätzung sowie in Bezug auf den Verarbeitungsvorgang getroffene technisch-organisatorische Sicherheitsmaßnahmen enthalten sein. Durch die technische Entwicklung sowohl auf der Seite der Schutzmaßnahmen, als auch auf der Seite der Bedrohungen, sind diese von der verantwortlichen Stelle regelmäßig dahingehend zu prüfen, ob die getroffenen Maßnahmen noch dem Stand der Technik im Sinne der Art. 25 und Art. 32 DS-GVO entsprechen.

Auslegung des Begriffs der Verarbeitungstätigkeit

Wie in meinem vorherigen Tätigkeitsbericht bereits dargestellt, hatte ich in der Prüfung 2020/2021 große Abweichungen bezüglich der gesamten Anzahl der Einträge im VVT festgestellt. Die Spanne reichte von ca. 20 Verarbeitungstätigkeiten bis hin zu über 800 Verarbeitungstätigkeiten. Im Rahmen dieser Prüfung wurde jedoch nur die Anzahl und nicht der Inhalt geprüft. Auch wenn berücksichtigt wurde, dass bei der Prüfung unterschiedlich große Krankenhäuser und Krankenhäuser einer oder mehrerer Fachrichtungen angeschrieben wurden, erschienen 20 Einträge deutlich zu gering bemessen. Der Durchschnitt lag bei 90 Einträgen bei kleinen Krankenhäusern und bei 207 Einträgen bei größeren Einrichtungen.

Im Rahmen der Schwerpunktprüfung wurden die vollständigen Inhaltsverzeichnisse der VVT von acht kleinen und großen Krankenhäusern ausgewertet und auf Vollständigkeit geprüft.

Die Überprüfung ergab, dass alle Einrichtungen die wesentlichen Verarbeitungstätigkeiten in das VVT aufgenommen haben. Die für die Prüfung ausschlaggebenden Kliniken, welche im Rahmen der vorhergehenden Prüfung nur sehr wenige Einträge im VVT angegeben hatten, haben das VVT aufgrund meiner, zusammen mit dem letzten Prüfbericht zur Verfügung gestellten Informationsmaterialien gründlich überarbeitet und verbessert.

Die Anzahl an Verarbeitungstätigkeiten ist weiterhin sehr unterschiedlich. Ich konnte jedoch ermitteln, dass dies nicht auf einer fehlerhaften Auslegung des Begriffs der Verarbeitungstätigkeit beruht, sondern zum einen an der Anzahl der Fachabteilungen der jeweiligen Klinik zum anderen mit der datenschutzrechtlich zulässigen Clusterung begründet ist. Insbesondere der Bereich „Personal“ wird teilweise sehr feingranular dargestellt. Ein Klinikum mit insgesamt sehr vielen Einträgen im VVT hat alleine in diesem Bereich 213 Einträge verzeichnet. Datenschutzrechtlich ist dies nicht zu beanstanden. Es obliegt den Verantwortlichen selbst zu entscheiden, wie feingranular das VVT geführt wird, solange alle wesentlichen Verarbeitungstätigkeiten mit der jeweils erforderlichen Risikobewertung erfasst sind.

Das Ergebnis dieses Teils der Prüfung fällt durchweg positiv aus. Es wird deutlich, dass die vorhergehende Prüfung ihre Wirkung entfaltet und die Verantwortlichen sensibilisiert hat.

Vollständige Prüfung von 16 Einträgen im VVT

Im zweiten Teil der Schwerpunktprüfung habe ich insgesamt 16 VVT-Einträge von sieben verschiedenen Krankenhäusern inhaltlich geprüft. Die Prüfung erstreckte sich auf die Darstellung

der Gefährdungsbeurteilung, die Einhaltung der Gewährleistungsziele der DS-GVO, die Bewertung der Risiken der Datenverarbeitung und die auf den konkreten Verarbeitungsvorgang bezogenen Dokumentationen der getroffenen technisch-organisatorischen Schutzmaßnahmen.

Der überwiegende Teil der Krankenhäuser hat gute bis sehr gute VVT-Einträge mit den entsprechenden Risikobetrachtungen vorgelegt. Bei zwei Einrichtungen haben sich Rückfragen ergeben, welche im Rahmen einer Vor-Ort-Kontrolle besprochen wurden.

Vor-Ort-Kontrollen

Während der Vor-Ort-Kontrollen wurde zunächst ein Gespräch über das Ergebnis der schriftlichen Prüfung geführt. Zudem wurde allgemein der Umsetzungsstand der DS-GVO und die Herangehensweise bei der Umsetzung datenschutzrechtlicher Vorgaben in Form einer Selbsteinschätzung abgefragt.

Im Anschluss wurden am Beispiel der Patientenaufnahme ins Krankenhausinformationssystem (KIS) die technischen und organisatorischen Maßnahmen, welche den direkten Patientenkontakt bei der Aufnahme betreffen, geprüft. Dies sind der Wartebereich vor der Aufnahme, die Diskretionszone bei der Aufnahme und erster Anamnese inklusive der Information über die Betroffenenrechte gem. Art. 13 DS-GVO. In technischer Hinsicht wurden die Zugriffsberechtigung der Aufnahmekräfte im KIS und die Umsetzung des Rollen-Rechte-Konzepts hinsichtlich der administrativen Aufnahme geprüft.

Fazit

Das Ergebnis der Prüfung Schwerpunktprüfung fällt positiv aus. Es wird deutlich, dass die vorhergehende Prüfung ihre Wirkung entfaltet und die Verantwortlichen sensibilisiert hat. Insbesondere die Vor-Ort-Prüfung hat zu einer erheblichen Verbesserung des Datenschutzes in den Krankenhäusern und zu einem besseren Verständnis der Gegebenheiten in einem Krankenhaus auf Seiten meiner Behörde beigetragen.

6.2 FAQ 2.0 und Runder Tisch im Gesundheitswesen

FAQ zum Gesundheitsbereich (Kurzlink): https://t1p.de/FAQGesundheitsbereich

Das in der Praxis von Bürgerinnen und Bürgern sowie Verantwortlichen der verschiedenen Heilberufe gerne genutzte FAQ zur DS-GVO im Gesundheitsbereich wurde um 13 Punkte ergänzt, sodass sie nunmehr Antworten auf 40 oft gestellte Fragen im Gesundheitswesen geben. Der Runde Tisch im Gesundheitswesen fand erstmals wieder in Präsenz statt.

Die FAQ im Gesundheitsbereich zeigen Wirkung

Mit Anwendbarkeit der Datenschutz-Grundverordnung (DS-GVO) im Jahr 2018 erreichten meine Behörde eine Vielzahl an Fragen und Beratungsersuchen. Dies führte nicht nur zu langen Bearbeitungszeiten – anlassunabhängige Prüfungen konnten nahezu gar nicht durchgeführt werden. Um Bürgerinnen und Bürgern sowie den Verantwortlichen der verschiedenen Heilberufe zeitnah eine Hilfestellung zu geben, habe ich die Antworten zu den häufigsten Fragen im Gesundheitswesen zu einem FAQ zusammengestellt. Dieses wurde sehr gut angenommen. Die Zahl der Beratungsanfragen ist spürbar zurückgegangen, wodurch mir wieder die Möglichkeit eröffnet wurde, umfangreiche Schwerpunktprüfungen, wie die Krankenhausprüfung durchzuführen.

Nach nunmehr vier Jahren DS-GVO erreichen mich weiterhin lobende Worte für diese übersichtliche Zusammenstellung. Im Berichtsjahr habe ich das FAQ überarbeitet und um viele weitere Punkte ergänzt. In die Überarbeitung sind neben weiteren häufig gestellten Fragen auch die Ergebnisse aus den im Verlauf der Jahre durchgeführten Prüfungen eingeflossen. Wie bereits bei der Erstellung der ersten Version habe ich die Mitglieder des Runden Tisches Gesundheit, welche die großen Interessenvertretungen, Vereinigungen und Kammern der verschiedenen Heilberufe sind, gebeten, das FAQ 2.0 ihren Mitgliedern bekannt zu machen.

Runder Tisch im Gesundheitswesen

Pandemiebedingt konnte der Runde Tisch im Gesundheitswesen, ein fachlicher Austausch mit Datenschutzbeauftragten und Justiziaren der Kammern und Kassen(zahn)ärztlichen Vereinigungen der verschiedenen Fachrichtungen der Verantwortlichen im Gesundheitswesen, erstmals seit 2019 in diesem Jahr wieder in Präsenz stattfinden. Der persönliche fachliche Austausch war für beide Seiten eine Bereicherung. Neben verschiedenen datenschutzrechtlichen Themen auf Seiten der Aufsichtsbehörde wurden unter anderem auch das erweiterte FAQ im Gesundheitswesen diskutiert und von allen Teilnehmenden ausdrücklich begrüßt. Das Format wird von den Beteiligten als sehr gewinnbringend erachtet und soll fortgesetzt werden.

6.3 Einführung des E-Rezepts verzögert sich. In der Übergangszeit sind datenschutzrechtliche Grundsätze zu beachten.

Ursprünglich war die flächendeckende Einführung elektronisch erstellter Rezepte (E-Rezept) ab dem 1. Januar 2022 für verschreibungspflichtige Arzneimittel vorgesehen. Aufgrund von verschiedenen Komplikationen wurde die Einführung auf unbestimmte Zeit verschoben.

Niedersachsen zunächst keine Fokusregion

Das E-Rezept wurde seit dem Sommer 2021, zunächst in der Fokusregion Berlin/Brandenburg und seit dem 1. Dezember 2021 von freiwillig teilnehmenden Arztpraxen und Apotheken bundesweit, getestet.

Die Umstellung auf die Nutzung des E-Rezepts in den (Zahn-)Arztpraxen und Krankenhäusern erfolgt nach einem regional und zeitlich gestuften Verfahren („E-Rezept-Rollout"): Seit dem 1. September 2022 ist die 1. Stufe des E-Rezept-Rollouts in Westfalen-Lippe und Schleswig-Holstein gestartet. Die nächsten Schritte der stufenweisen Einführung werden von den Gesellschaftern der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (Gematik) zeitnah festgelegt. Die Gematik wird den Rollout-Prozess eng begleiten.

Auch außerhalb des regional begleiteten E-Rezept-Rollouts kann das E-Rezept bundesweit in den (Zahn-)Arztpraxen und Krankenhäusern für die Verordnung von Arzneimitteln genutzt werden. Denn seit dem 1. September 2022 sollten die Apotheken flächendeckend in ganz Deutschland in der Lage sein, E-Rezepte einzulösen und mit den Krankenkassen abzurechnen.

Datenverarbeitung und Funktionsweise des E-Rezepts

Für die Übermittlung des E-Rezepts wird die Telematikinfrastruktur (TI) im Gesundheitswesen verwendet. Die TI ist das sichere Informations- und Kommunikationsnetz im Gesundheitswesen, das Praxen, Krankenhäuser, Apotheken und weitere Leistungserbringereinrichtungen im Gesundheitswesen sicher miteinander verbindet, so dass die an der Versorgung Beteiligten besser und schneller miteinander kommunizieren können.

Das E-Rezept kann von den Patientinnen und Patienten über zwei verschiedene Wege genutzt werden. So können diese entscheiden, ob sie ihr E-Rezept per Smartphone über eine E-Rezept-App verwalten und digital über gesicherte Verbindungen an die gewünschte Apotheke ihrer Wahl senden wollen oder ob ihnen die für die Einlösung ihres E-Rezepts erforderlichen Zugangsdaten (ähnlich einem QR-Code) als Papierausdruck in der Arztpraxis ausgehändigt werden sollen.

Datenschutzrechtliche Probleme beim Umgang mit ausgedruckten E-Rezepten

Die Einführung des E-Rezepts hat in Schleswig-Holstein zu datenschutzrechtlichen Problemen geführt, da Ärztinnen und Ärzte den Patienten, die keine E-Rezept-App nutzen, den QR-Code statt als Ausdruck per unverschlüsselter E-Mail übermittelt hatten. Ein derartiges Verfahren hat der Gesetzgeber aus gutem Grund nicht vorgesehen. Da der QR-Code auslesbare personenbezogene Daten der Patienten enthält, verstieß die Übermittlung von Gesundheitsdaten per unverschlüsselter E-Mail gegen den Datenschutz.

Ausführlicher Bericht zur elektronischen Patientenakte: 27. Tätigkeitsbericht ab Seite 156.

Auch wenn in Niedersachsen keine derartigen Vorfälle bekannt sind, ist die Einführung des E-Rezepts ohne flächendeckende Bereitstellung der erforderlichen technischen Infrastruktur und ohne detaillierte Aufklärung der Verantwortlichen und der Betroffenen hinsichtlich der Nutzung und datenschutzrechtlichen Risiken nach der zunächst nicht datenschutzkonformen Einführung der elektronischen Patientenakte erneut ein Negativbeispiel.

6.4 Beratung des Sozialministeriums für die Online-Leistung „Schwerbehindertenausweis“

Die Verwaltungsdigitalisierung bringt viele datenschutzrechtliche Herausforderungen mit sich. Vor diesen steht auch das Niedersächsische Sozialministerium bei der Digitalisierung von Gesundheitsleistungen.

Im Berichtszeitraum habe ich das Sozialministerium im Hinblick auf die mir vorgelegte Datenschutzfolgen-Abschätzung (DSFA) für die Online-Leistung „Schwerbehindertenausweis“ beraten. Eine DSFA muss für eine Verarbeitung personenbezogener Daten durchgeführt werden, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte. Da bei Beantragung von Gesundheitsleistungen in der Regel besonders schutzwürdige Daten verarbeitet werden, ist bei den meisten Gesundheitsleistungen eine DSFA erforderlich.

Im Rahmen einer DSFA werden geplante Verarbeitungsvorgänge systematisch beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit beurteilt und die Risiken für die Rechte und Freiheiten der betroffenen Personen bewertet. Für die identifizierten Risiken werden vorab Abhilfemaßnahmen festgelegt. Vor der Prüfung der gewählten technischen und organisatorischen Maßnahmen muss zudem eine Prüfung der Rechtsgrundlagen der Verarbeitung vorgenommen werden.

Angesichts der Komplexität des Vorhabens, eingebettet in die Gesamtdigitalisierungsstrategie des Bundes und der Länder, verwundert der hohe Beratungsbedarf des Sozialministeriums nicht. Den von mir erteilten Hinweisen folgte ein vom Ministerium organisierter Workshop mit den Landesverbänden und dem zuständigen IT-Dienstleister, in dem ich auf wichtige Aspekte bei der Durchführung und Erstellung einer DSFA vertieft eingehen konnte.

Ich freue mich über die konstruktive und wertschätzende Atmosphäre, von der die Beratung geprägt war, und hoffe, mit den erteilten Hinweisen eine datenschutzkonforme Umsetzung der niedersächsischen Digitalisierungsprojekte nachhaltig fördern zu können.

J.7. Telemedien

7.1 Pur-Abos auf Webseiten – Erkaufter Datenschutz?

Neben den zahlreichen Beschwerden gegen gängige Einwilligungsbanner auf Webseiten erreichen mich immer mehr Eingaben gegen sogenannte Pur-Abo-Modelle. Nutzern werden im Einwilligungsbanner zwei Möglichkeiten gegeben, die Inhalte der Webseite zu konsumieren. Entweder schließen sie das Pur-Abo ab und zahlen einen Monatsbeitrag, um ohne Werbung und ohne Werbetracking die Webseite besuchen zu können oder sie willigen insbesondere in personalisierte Werbung, Werbetracking, individuelle Profilbildung und individuelle Nutzungsanalyse ein. Zunächst waren diese Pur-Abo-Modelle vor allem auf Webseiten von Zeitungsverlagen und sonstigen Medien zu finden. Mittlerweile breiten sie sich allerdings immer weiter aus. Umso drängender wird es, dass Aufsichtsbehörden diese Geschäftsmodell datenschutzrechtlich bewerten.

Orientierungshilfe abrufbar unter (Kurzlink): https://t1p.de/OH-Telemedien-1-1

Bereits 2021 habe ich die Webseiten von Medienhäusern in den Fokus genommen und eine länderübergreifende koordinierte Prüfung durch zahlreiche Aufsichtsbehörden initiiert. Zu Beginn der Prüfung, hatte nicht eine der fünf geprüften Medienseiten ein Pur-Abo-Modell auf seiner Webseite; mittlerweile sind es fast alle.

Bemerkenswerterweise wurden diese Webseiten nach ihrer Umstellung sehr schnell wieder zum Gegenstand von Beschwerden, die uns erreichten. Häufig bringen die Beschwerdeführer zum Ausdruck, dass es nicht korrekt sein könne, wenn man sich den Datenschutz „erkaufen“ müsse und sie beanspruchen einen sowohl kostenlosen als auch werbe- und trackingfreien Zugang zu den Medieninhalten. Ganz so einfach ist die datenschutzrechtliche Bewertung allerdings nicht.

Aus dem Datenschutzrecht lässt sich kein Anspruch des Nutzers auf einen kostenlosen Zugang zu Onlinemedien ableiten. Der Medienanbieter kann grundsätzlich entscheiden, an welche Voraussetzungen er das Lesen der Webseite knüpft und wie er diese finanziert. Allerdings muss jedes gewählte Geschäftsmodell und dessen Umsetzung auf der Webseite den rechtlichen Anforderungen des

Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) und der DS-GVO entsprechen. Aus der Perspektive des Nutzers der Webseite dienen Vorschriften der DS-GVO dazu, sein Recht auf informationelle Selbstbestimmung zu schützen, und nicht, eine kostenlose Nutzung von Onlinemedien zu ermöglichen. Marktwirtschaftlich gesehen entsprechen kostenpflichtige Medieninhalte dem bisher üblichen Geschäftsmodell im Offline-Bereich, wo Zeitungen und Zeitschriften regelmäßig nur gegen Zahlung von Geld zur Verfügung gestellt werden.

Grundsätzlich kann die Nachverfolgung von Nutzerverhalten (Tracking) auf eine Einwilligung gestützt werden, wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dies bezahlpflichtig ist. Die Leistung, die Nutzerinnen und Nutzer bei einem Bezahlmodell erhalten, muss jedoch erstens eine gleichwertige Alternative zu der Leistung darstellen, die Nutzerinnen und Nutzer durch eine Einwilligung erhalten. Zweitens muss die Einwilligung alle Wirksamkeitsvoraussetzungen gemäß Art. 4 Nr. 11 DS-GVO erfüllen.

Vor allem die 1. Generation der Pur-Abo-Modelle erfüllt die zweite Voraussetzung nicht und weist erhebliche datenschutzrechtliche Defizite auf. Nutzer, die kein Pur-Abo abschließen, müssen ausnahmslos in alle auf der Webseite eingebundenen Dienste einschließlich einer oft sehr hohen Anzahl von Diensten des digitalen Marketings einwilligen. Plakativ wird dies auch als „Pay or Okay" bezeichnet. Hierbei wird eine gebündelte Einwilligung in mehrere unterschiedliche Zwecke und bezogen auf mehrere verantwortliche Drittdienstleister mit dem Klick auf eine Schaltfläche eingeholt. Dies ist nur zulässig, wenn die Zwecke in einem sehr engen Zusammenhang stehen. Eine pauschale Gesamteinwilligung in verschiedene Zwecke ist nicht wirksam, weil die Anforderung der Granularität der Einwilligung nicht erfüllt wird. Dies bedeutet, dass Nutzerinnen und Nutzer grundsätzlich die Möglichkeit haben müssen, die einzelnen Zwecke, zu denen eine Einwilligung eingeholt werden soll, selbst und aktiv auswählen zu können (Opt-In).

Ich bin sicher, dass mich die Pur-Abo-Modelle auf Webseiten auch 2023 noch intensiv beschäftigen werden. Noch ist es möglich, auf diese Entwicklung einzuwirken und auf die Datenschutzkonformität dieser Geschäftsmodelle zu drängen. Verantwortlichen können hierzu klare Bewertungsmaßstäbe an die Hand gegeben werden. Ich werde mich dafür einsetzen, dass sich auch die Datenschutzkonferenz zum Pur-Abo-Modell positioniert.[1]

1 Die DSK hat in einer Pressemeldung vom 30.3.2023 (https://t1p.de/DSK_PM_Pur-Abo-Modell) über ihren Beschluss vom 22.3.2023 zur Bewertung von Pur-Abo-Modellen auf Websites informiert (https://t1p.de/DSK_Beschluss_Pur-Abo-Modell).

7.2 Proaktive Prüfung von Microsoft-Exchange-Servern

Aufgrund der seit 2021 bekannt gewordenen schwerwiegenden Schwachstellen (auch bekannt u. a. als Proxy-Logon) in dem weit verbreiteten Produkt Microsoft Exchange habe ich zur nachhaltigen Überwachung der DS-GVO eine proaktive Prüfung durchgeführt. Hierbei habe ich Verantwortliche ermittelt, bei denen das Produkt zum Einsatz kommt und deren Server diese Schwachstellen aufweisen. In diesen Fällen habe ich die Verantwortlichen zur Schließung der Schwachstellen aufgefordert und die Umsetzung anschließend kontrolliert.

Eingehende Artikel 33 Meldungen

Anfang März 2021 wurden vier sicherheitsrelevante Schwachstellen in der Group- und E-Mail Software Microsoft Exchange Server mit sogenannten CVE-Meldungen[1] bekannt gemacht[2] und Patches bzw. Updates zur Schließung der Lücken des Herstellers veröffentlicht. Unmittelbar nach der Bekanntgabe durch Microsoft begannen im Internet automatisierte Suchläufe nach anfälligen Servern. Darunter haben – wie üblich – auch Angreifer anfällige Server aufgespürt und angegriffen.

In der Folgezeit erreichten mich wegen dieses Sachverhalts zahlreiche Meldungen zu jeweiligen Verletzungen des Schutzes der personenbezogenen Daten gemäß Art. 33 DS-GVO. Auf meiner Webseite veröffentlichte ich Informationen zu den Anforderungen im Umgang mit den Sicherheitslücken durch Verantwortliche.

Da auch mit deutlichem zeitlichem Abstand noch Meldungen nach Art. 33 DS-GVO bei mir eingingen, die auf die genannten Sicherheitslücken zurückzuführen waren, entschloss ich mich, proaktiv tätig zu werden.

Prüfung im IT-Labor

In einem gemeinsamen Projekt mit Juristen und Informatikern meines Hauses habe ich, unabhängig von individuellen Beschwerden oder Art. 33-Meldungen, Verantwortliche identifiziert, die weiterhin ein mit Schwachstellen

1 CVE ist ein Industriestandard für eine einheitliche Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen. Es ist die Kurzform von „Common Vulnerabilities and Exposures“ (deutsch häufige Schwachstellen und Anfälligkeiten).

2 vgl. Bundesamt für Sicherheit in der Informationstechnik: Microsoft Exchange Schwachstellen CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 Detektion und Reaktion Version 2.4, Stand 19.03.2021

behaftetes E-Mail-System betreiben. Die Ausnutzung dieser Schwachstellen führt mit großer Wahrscheinlichkeit zur Verletzung des Schutzes personenbezogener Daten.

Um einen Überblick über die in Niedersachsen betroffenen Mailserver zu bekommen, entschied ich mich, auf die Informationen von Internet-Wide Scanning Datenbanken zurückzugreifen. Anbieter solcher Datenbanken durchsuchen das Internet nach vorhandenen Systemen und speichern die bei der Suche erlangten Informationen in einer Datenbank ab. Diese Informationen enthalten u. a. auch Dienste, welche von den gefundenen Systemen angeboten werden. Zu diesen angebotenen Diensten zählen auch die von den vorgenannten Sicherheitslücken betroffenen Microsoft Exchange Server. In meinem IT-Labor habe ich unter Nutzung dieser Internet-Wide Scanning Datenbanken in einem teilautomatisierten Prozess Verantwortliche aus Niedersachsen identifiziert, deren Server die MS Exchange-Sicherheitslücken aufweisen.

Da die von den Anbietern der Datenbanken bereitgestellten Informationen veraltete oder falsch positive Einträge beinhalten können, habe ich jedes ermittelte System einer zusätzlichen Verifikation in meinem IT-Labor unterzogen. Mit Hilfe eines Schwachstellenscanners habe ich bei den zuvor ermittelten Verantwortlichen eine Prüfung ihrer E-Mailserver in Echtzeit durchgeführt.

Die Ergebnisse beweisen, dass die von den Verantwortlichen zum Zeitpunkt meiner Prüfung betriebenen Microsoft Exchange Server diese Sicherheitslücken aufgewiesen haben.

Kooperative Verantwortliche

Gegen die ermittelten Stellen wurden Prüfverfahren eingeleitet, welche in Abhängigkeit von den weiteren tatsächlichen Feststellungen mit Verwarnungen, Einstellungen oder auch einer Anweisung beendet wurden.

Erfreulich war, dass alle Verantwortlichen kooperativ waren und nach Einleitung des Prüfverfahrens die festgestellten Sicherheitslücken zeitnah schließen wollten.

Im Nachgang der Prüfung habe ich in meinem IT-Labor abschließend überprüft, ob die Lücken tatsächlich geschlossen und die Schwachstellen in den Exchange Servern damit behoben worden sind. Ferner wurde das Prüfverfahren bei den Verantwortlichen zum Anlass genommen, die internen Prozesse in Bezug auf die Pflege der genutzten Softwareprodukte zu verbessern.

Für die Zukunft sind weitere proaktive Prüfungen in verschiedenen Bereichen der Wirtschaft und zu unterschiedlichen Softwareanwendungen geplant.

Allgemeine Erkenntnisse zu zentralen Kommunikationslösungen

Das Fallbeispiel ProxyLogon und ProxyShell zeigte in besonderem Maße, welch brisante Auswirkung Schwachstellen und Sicherheitslücken in Produkten mit hohem Verbreitungsgrad nach sich ziehen. Das Niveau der Informationssicherheit wird dadurch für viele Systeme und Daten gefährdet und damit steigen die Risiken für Rechte und Freiheiten Betroffener in potentiell großem Ausmaß.

Monatelang war die Gefahr durch die genannten Sicherheitslücken nicht gebannt; im August 2021 berichteten Medien, dass noch immer eine „massive Angriffswelle auf ungepatchte Exchange-Server" rollt. Obwohl die Lücken bekannt und Patches vorhanden waren, waren tausende Exchange-Server weiter angreifbar und die Schwachstellen wurden ausgenutzt.[3]

Im Fall Microsoft Exchange Server traten zudem im Berichtszeitraum seit September 2022 zwei weitere Sicherheitslücken mit dem Schweregrad „hoch" und „mittel" mit dem Namen „ProxyNotShell" (zuerst veröffentlicht bei der IT-Sicherheitsfirma GTSC) auf. Eine weitere neue Attacke-Form namens „OWASSRF" trat im Dezember auf. Zuletzt veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) daher am 21.12.2022 die Cyber-Sicherheitswarnung[4] zum neuen Zero-Day Exploit in Microsoft Exchange Server mit weiteren empfohlenen Patches und Maßnahmen.

Die Sicherheitslücken sind allerdings kein Phänomen, welches ausschließlich bestimmte Produkte trifft. Vielmehr lassen sich bei jedem komplexen System- und Anwendungs-Software-Produkt Codierungs- und Implementierungsfehler finden. Bei weit verbreiteten Produkten ist allerdings auch das Angriffsinteresse durch Cyberattacken höher, da die Erfolgsaussichten des Angriffs mit zunehmender Betroffenenzahl steigt. Daher ist es von großer Bedeutung, dass Verantwortliche auf ausgereifte Architekturkonzepte und zeitnahes und fachkundiges Update- und Patchmanagement achten sowie Sicherheitsaudits und Penetrationstest durchführen. Informationssicherheit und technisch-organisatorischer Datenschutz erfordern eine prozesshafte und zyklische Daueranalyse und -betreuung aller IT-Komponenten und eines ständigen Anpassens der angemessenen und wirksamen technisch-organisatorischen Maßnahmen.

3 Vgl. Heise online vom 22.08.2021, https://t1p.de/Heise_Exchange-Server
4 Cyber-Sicherheitswarnung (CSW)-Nr. 2022-258168-1332, Version 1.3, 21.12.2022 unter https://t1p.de/BSI_Exchange-Server

7.3 „Neue“ Cookie-Regelung im TTDSG – Ausnahmen von der Einwilligung

Die Einführung des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) sorgte zum Ende des Jahres 2021 für einige Aufregung bei Betreibern von Webseiten und Apps. Insbesondere die nun nach über zehn Jahren vorgenommene europarechtskonforme Umsetzung der sogenannten Cookie-Regelung der ePrivacy-Richtlinie durch § 25 TTDSG hat in der Praxis für viel Wirbel und Diskussionen gesorgt. Entsprechend häufig wurden meiner Behörde zu dieser Vorschrift Fragen gestellt und es waren einige Verfahren zu der neuen Regelung zu bearbeiten.

In der praktischen Anwendung wirft der § 25 TTDSG, zu Cookies und Tracking-Methoden auf Webseiten und in Apps, zahlreiche Detailfragen auf. Die grundsätzlichen Probleme und Prüfungsschritte werden sehr detailliert in der 2022 aktualisierten Orientierungshilfe der Datenschutzkonferenz (DSK) für Anbieter von Telemedien dargestellt. Diese ist als Ergebnis des Konsultationsverfahrens um ein Kapitel zur Gestaltung von Einwilligungsbannern ergänzt worden, in dem konkrete Hinweise für die Abfrage von Einwilligungen auf Webseiten gegeben werden.

Orientierungshilfe Telemedien als PDF-Download (Kurzlink): https://t1p.de/OHTelemedien

Vorgelagert ist die rechtliche Prüfung, ob eine Einwilligung für den Einsatz von Cookies und anderen Tracking-Techniken sowie die Einbindung von Drittdiensten auf Webseiten notwendig ist oder nicht. § 25 Abs. 1 TTDSG normiert den Grundsatz, dass eine Einwilligung erforderlich ist. Von diesem Grundsatz regelt § 25 Abs. 2 Nr. 2 TTDSG eine Ausnahme für Webseiten (= Telemedien). Danach bedarf es keiner Einwilligung, wenn der Einsatz von Cookies und anderen Trackingtechnologien sowie die Einbindung von Drittdiensten unbedingt erforderlich ist, damit der Betreiber der Webseite oder App einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Die Ausnahme wird somit im Kern an zwei Voraussetzungen geknüpft – erstens einen ausdrücklich vom Nutzer gewünschten Telemediendienst und zweitens, dass die Cookies oder anderen Trackingtechnologien für die Erbringung des Dienstes „unbedingt erforderlich“ sind. Obwohl diese Voraussetzungen meines Erachtens klar und stringent formuliert sind – und zudem der umzusetzenden europäischen Vorschrift entsprechen – gibt es hier sehr weitreichende Auslegungsansätze.

Es wird z. B. argumentiert, dass ein Nutzer einer Webseite allein indem er sie im Browser öffnet, zum Ausdruck bringt, dass er diese Webseite in genau der vorliegenden Ausgestaltung wünscht. Bezogen auf eine Suchmaschine würde dies z. B. bedeuten, dass der Nutzer nicht nur eine Auflistung relevanter Inhalte im Web nach Eingabe eines Suchwortes anstrebt, sondern auch eine personifizierte Anzeige und Sortierung von Suchergebnissen, gesponserte Links, Werbeanzeigen und die Erstellung individueller Persönlichkeitsprofile auf der Grundlage aller Suchanfragen und der hierfür eingesetzten verschiedenen Geräte. Auch eingebundene Chatdienste, Kontaktformulare, Kartendienste, Videos etc. seien immer und ausnahmslos vom Nutzer „ausdrücklich gewünscht", auch wenn er sie auf der Webseite vielleicht nie wahrgenommen oder genutzt hat.

Die Aufsichtsbehörden stellen höhere Anforderungen, um den Wunsch des Nutzers objektiv annehmen zu können. Üblicherweise bieten Webseiten eine Vielzahl von Funktionen und Diensten. Daher fordern die Aufsichtsbehörden eine funktionale Betrachtung des Telemediendienstes. Bezogen auf das Beispiel der Webseite werden einzelne Funktionen auf Webseiten, die den Einsatz von Cookies und anderen Trackingtechnologien oder Drittdienstleistern fordern, erst dann als vom Nutzer gewünscht angesehen, wenn der Nutzer sie explizit nutzt – also bei einem Onlineshop ein Produkt in den Warenkorb legt, einen konkreten Bezahldienstleister auswählt, ein integriertes Video anklickt oder ein Kontaktformular ausfüllt. Nach Auffassung der Aufsichtsbehörden dürfen Cookies und Drittdienste jeweils erst bei bestimmten Nutzungsvorgängen auf der Webseite aktiv werden, aber nicht unterschiedslos bereits beim Aufruf der Startseite.

Insbesondere Interessenverbände der Wirtschaft vertreten ebenfalls bezogen auf das Merkmal „unbedingt erforderlich" ein recht weites Verständnis. So sei „unbedingt erforderlich" auch dann erfüllt, wenn rechtliche, vertragliche, wirtschaftliche oder betriebliche Aspekte notwendigerweise zu berücksichtigen sind, um den ausdrücklich gewünschten Dienst zu erbringen.[1] Die DSK geht dagegen davon aus, dass diese Tatbestandsvoraussetzung restriktiv zu verstehen ist, im Sinne von „technisch unbedingt erforderlich", um die ausdrücklich gewünschte Funktion des genutzten Telemediendienste bereitzustellen.[2] Eine Ausnahme von der Einwilligungsbedürftigkeit kann daher nicht damit begründet werden, dass das Speichern von oder der Zugriff auf Informationen im Endgerät wirtschaftlich für das Geschäftsmodell erforderlich ist.

Es freut mich sehr, dass es der DSK zeitnah mit dem Inkrafttreten des TTDSG gelungen ist, eine einheitliche Rechtsauffassung zu der Ausnahmeregelung in § 25 Abs. 2 Nr. 2 TTDSG zu finden und diese auch in der Orientierungshilfe für Anbieter von Telemedien 2021 zu veröffentlichen. Das durchgeführte Konsultationsverfahren hat die dargestellte Position noch einmal bestätigt. Für die Bearbeitung von Beschwerden und Beratungsanfragen ist es eine große Arbeitserleichterung, wenn auf Dokumente der DSK verwiesen werden kann. Nichtsdestotrotz ist bereits abzusehen, dass es auch zukünftig Beschwerden gegen Webseiten geben wird, die die Vorgaben von § 25 TTDSG nicht einhalten und in Einzelfällen eine Durchsetzung der Norm erfordern werden.

1 Zu den entsprechenden Äußerungen s. u. a. den Bericht des AK Medien zum Konsultationsverfahren zur OH Telemedien 2021, „Auswertungsbericht des AK Medien Konsultation zur Orientierungshilfe für Anbieter von Telemedien", Stand: 19.10.2022, S. 25 ff.

2 S. ausführlich OH Telemedien 2021, Version 1.1, Rn. 76 ff.

J.8. Videoüberwachung

8.1 Daueraufgabe Rechtmäßigkeitsprüfung

Videoüberwachungen richten sich häufig auf einzelne Erfassungsbereiche, die von mir kritisch gesehen, jedoch von Verantwortlichen als unerlässlich dargestellt werden. Gelegentlich gebe ich deshalb den Verantwortlichen auf, die Rechtmäßigkeit dieser Überwachung in der „Grauzone" dauerhaft zu prüfen. Zeitversetzte Nachfragen meinerseits ergaben unbefriedigende Ergebnisse.

Eine Videoüberwachung ist nach Artikel 6 Absatz 1 Buchstabe f DS-GVO nur dann rechtmäßig, wenn die Verarbeitung personenbezogener Daten zur Wahrung der berechtigten Interessen der Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Berechtigt ist ein Interesse, wenn es rechtmäßig, hinreichend klar formuliert und nicht rein spekulativ ist.

Gefordert sind konkrete Tatsachen, aus denen sich beispielsweise eine Gefahrenlage ergibt, die über das allgemeine Lebensrisiko hinausgeht. Eine Gefährdung kann sich nur aus tatsächlichen Erkenntnissen ergeben – subjektive Befürchtungen oder ein Gefühl der Unsicherheit reichen nicht aus. Das bedeutet, dass Beschädigungen, Vorfälle in der Vergangenheit oder andere Er-

Orientierungshilfe der DSK Videoüberwachung durch nicht-öffentliche Stellen (Kurzlink): https://t1p.de/OH_Videoueberwachung

eignisse, die eine Gefahrenlage objektiv begründen können, gegenüber der Aufsichtsbehörde nachgewiesen werden müssen. Solche Vorfälle sollten daher entsprechend dokumentiert sein. Konkrete Vorfälle müssen dabei nicht in jedem Fall beim Überwachenden selbst stattgefunden haben. Allgemeine Statistiken reichen jedoch nicht als konkreter Nachweis aus.

Verarbeitung personenbezogener Daten muss datenschutzkonform erfolgen

Die Rechtmäßigkeit einer Videoüberwachung muss regelmäßig durch die verantwortliche Stelle überprüft werden. Dabei ist darauf zu achten, dass die Rechtsgrundlage weiterhin anwendbar ist:

- Ein berechtigtes Interesse kann durch Änderung der Gegebenheiten wegfallen,
- die Überwachung kann durch Veränderung in den überwachten Räumlichkeiten zum Erreichen des Zwecks nicht mehr geeignet oder erforderlich sein,
- Personen, deren Interessen einer Überwachung entgegenstehen, können sich nach einer räumlichen Umgestaltung plötzlich im Erfassungsbereich der Kameras befinden.

Kann bei einer Prüfung das berechtigte Interesse an einer Videoüberwachung nicht nachgewiesen werden oder habe ich bei der Prüfung Zweifel an der Erforderlichkeit, habe ich die Möglichkeit, die Verarbeitung zu untersagen oder einzuschränken (Artikel 58 Absatz 2 Buchstabe f DS-GVO). Erweist sich der Vortrag der verantwortlichen Stelle jedoch zunächst als nachvollziehbar, habe ich dieser in der Vergangenheit in mehreren Fällen aufgegeben, die Rechtmäßigkeit der Videoüberwachung, insbesondere in den von mir kritisch gesehenen Bereichen für einen bestimmten Zeitraum zu evaluieren und mir das Ergebnis anschließend vorzulegen.

Ergebnis meiner Nachprüfungen

Alle von mir nachgeprüften Verfahren erwiesen sich als datenschutzrechtlich unzulässig. Die Verantwortlichen haben ihre Pflicht aus Artikel 5 Absatz 2 DS-GVO, wonach sie für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich sind und dessen Einhaltung nachweisen können müssen, nicht erfüllt.

Vertreter fremder Interessen

Ein Fastfood-Restaurant hat mir gegenüber angegeben, dass die Überwachung von Sitzbereichen unerlässlich sei. Das Restaurant sei aufgrund seiner Lage in einem Kriminalitätsschwerpunkt so häufig Delikten wie Sachbeschädigungen, Diebstahl und Körperverletzung ausgesetzt, dass die Sicherheit der

Beschäftigten, der Kundinnen und Kunden sowie des Eigentums andernfalls nicht gewährleistet werden könne. Kopien von Strafanzeigen konnten allerdings nicht vorgelegt werden.

Die Überwachung von Sitz- und Verzehrbereichen ist in der Regel nicht zulässig. Die Schutzbedürftigkeit der Interessen der von der Videoüberwachung betroffenen Personen ist in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, besonders hoch einzustufen. Dies trifft auf die für Kunden eingerichteten Sitz- und Verzehrbereiche, durch die ein längerer Aufenthalt ermöglicht und dazu eingeladen werden soll, im besonderen Maße zu. Daher werden die Persönlichkeitsrechte der sich in den Sitz- und Verzehrbereichen länger aufhaltenden Kunden durch eine ständige Videoüberwachung erheblich beeinträchtigt.

Da sich das Restaurant jedoch tatsächlich in einem Kriminalitätsschwerpunkt befindet und eine dauerhafte Sichtkontrolle durch anwesendes Personal nicht möglich war, gab ich dem Unternehmen Gelegenheit, mir nach einem Jahr nachzuweisen, welche der gegen das Unternehmen oder dessen Beschäftigte gerichtete Straftaten in dieser Niederlassung angezeigt wurden. Auch war darzulegen, dass für deren Aufklärung die Bilddaten der jeweiligen Kamera in den Sitzbereichen tatsächlich erforderlich waren.

Auf Nachfrage wurde mir eine Aufstellung von 532 Vorgangsnummern der zuständigen Polizeidienststelle vorgelegt, darunter Straftaten wie Computerbetrug, Verstoß gegen das Aufenthaltsrecht und Beförderungserschleichung. Das führte zu meiner Nachfrage, welche der Anzeigen denn nun tatsächlich von dem Unternehmen erstattet wurden. Antwort: Keine. Der Aufwand dafür sei zu hoch. Wenn die Polizei aufgrund der Anzeigenerstattung der Kunden die Aufnahmen anfordere, gebe man diese heraus.

Da somit nicht einmal ein berechtigtes Interesse des Unternehmens vorlag, musste die Videoüberwachung wegen Unzulässigkeit beendet werden.

Verhaltens- und Leistungskontrolle bei Beschäftigten?

In einem weiteren Fall hat ein Supermarkt den Personaleingang überwacht, um Überfälle auf das Personal zu verhindern. Dort befand sich auch ein Raucherbereich. Die Kamera wurde von mir beanstandet, weil mit der Überwachung dieses Bereiches eine unzulässige Verhaltens- und Leistungskontrolle ermöglicht wurde. Vorgetragen wurde, dass der Aschenbecher dort ausschließlich für die Kunden stehe. Für das Personal gäbe es einen Raucherraum. Die Überwachung könne auch nicht auf die Zeiten des Arbeitsbeginns und des Arbeitsendes beschränkt werden, da die Taten dort während der Öffnungszeiten vorbereitet würden. Der Betriebsrat hat die Überwachung als „dringend erforderlich für die Sicherheit der Mitarbeiter“ bestätigt.

Ich forderte die verantwortliche Stelle auf, spätestens im Rahmen der Evaluation zu prüfen, ob die Überwachung des Personaleingangs wirklich erforderlich ist oder zumindest auf die Abend- und Nachtstunden begrenzt werden kann, auch weil der Eingang tagsüber vom Parkplatz gut einsehbar ist. Eine erneute Prüfung habe ich mir vorbehalten.

Eineinhalb Jahre später forderte ich das Ergebnis der regelmäßigen Überprüfung an. Auch hier gab es nur eine Fehlanzeige. Es wurde ausschließlich auf den alten Vortrag verwiesen und zudem neue Zwecke geltend gemacht. Demnach würden Diebinnen und Diebe das Gebäude durch den Personaleingang verlassen, die man so erfassen wolle. Auch für diesen neuen Zweck konnte keine Dokumentation darüber vorgelegt werden, wie oft Täter den Ausgang nutzten oder wie oft die Auswertung der Bilddaten zur Aufklärung von Diebstählen herangezogen wurde und beitragen konnte. Mildere Mittel wie beispielsweise die Anbringung eines elektronischen Türwächters wurden von dem Unternehmen nicht geprüft.

Die Kamera wurde aufgrund meiner Beanstandung außer Funktion genommen.

Dann halt zur Erfüllung vertraglicher Pflichten …

Auch bei einem Elektronikmarkt konnte ich die Erforderlichkeit für eine Überwachung im Kassenbereich nicht ohne Weiteres nachvollziehen. Im Zuge meiner Nachprüfung wurde neu vorgetragen, dass die Überwachung auch auf Grundlage des Artikels 6 Absatz 1 Satz 1 Buchstabe b DS-GVO dazu diene, die vertragsgemäße Erfüllung nachweisen zu können. Dieses sollte für den Fall in Betracht kommen, falls sich Kunden nachträglich über eine nicht ausreichende Leistung beschweren sollten. Ein Quittieren des Empfangs der Ware durch die Kunden als milderes Mittel wurde von dem Unternehmen abgelehnt, da dies nicht „marktüblich“ sei.

Dem vorgetragenen Versuch einer Rechtfertigung konnte ich nicht folgen. Artikel 6 Absatz 1 Satz 1 Buchstabe b DS-GVO zählt zu den Erlaubnistatbeständen, die eine Datenverarbeitung ganz wesentlich auf Grundlage einer willentlichen Entscheidung der betroffenen Person für zulässig erachten (siehe Schulz in Gola/Heckmann, DS-GVO – BDSG, Art. 6, Rn. 27). Der Erlaubnistatbestand verlängert gewissermaßen den der Einwilligung. Zwar wird bei einer Verarbeitung auf Grundlage von Artikel 6 Absatz 1 Satz 1 Buchstabe b DS-GVO nicht ausdrücklich der Verarbeitung zugestimmt, doch wird diese als notwendiges Zwischenziel gewissermaßen von der Freiwilligkeit des Vertragsschlusses mitumfasst (siehe Philipp Reimer in Sydow, Europäische DS-GVO, Art. 6, Rn. 21).

Im Ergebnis kann nicht davon ausgegangen werden, dass die Erklärung eines Kunden zum Vertragsabschluss eine Verarbeitung seiner personenbezogenen Daten mittels Videoüberwachung umfasst. Insofern musste ich die Videoüberwachung zu diesem Zweck ablehnen.

8.2 Wächtermodus von Tesla-Fahrzeugen

Im Jahr 2022 haben mich viele Beratungsanfragen und Beschwerden zum sogenannten Wächtermodus (engl.: Sentry Mode) bei Fahrzeugen der Marke Tesla erreicht. In erster Linie sahen sich Bürgerinnen und Bürger dabei einer mutmaßlich unzulässigen Videoüberwachung ausgesetzt. Ich habe mich daher mit der Sach- und der Rechtslage um den Wächtermodus intensiv befasst.

Big Brother schaut aus einem parkenden Fahrzeug zu.

Im Unterschied zu der bereits länger verbreiteten Funktion „Dashcam" zeichnet der Wächtermodus die Umgebung nicht während der Fahrt, sondern aus dem geparkten Fahrzeug auf.

Bereits im Rahmen des Standby-Modus findet eine Videoaufzeichnung der Umgebung mit einer Reichweite von mindestens 50 Metern im Umkreis des Fahrzeugs statt. Diese Aufnahmen werden vorläufig in 60-Minuten-Sequenzen gespeichert und in einem Ringspeicherverfahren immer wieder mit neuen Sequenzen überschrieben.

Im Warnung- und Alarmmodus werden die letzten 10 Minuten vor dem auslösenden Ereignis dauerhaft auf einem USB-Stick im Fahrzeuginneren gespeichert. Ein solches auslösendes Ereignis kann dabei nicht nur eine physische Einwirkung auf das Fahrzeug sein, sondern z. B. auch ein nahes Herantreten einer Person an das Fahrzeug.

Sowohl die beschriebene Aufzeichnung der Fahrzeugumgebung im öffentlichen Raum als auch eine vorläufige oder dauerhafte Speicherung dieser Aufnahmen sind datenschutzrechtlich unzulässig. Ähnlich wie im Falle der Nutzung einer Dashcam eines fahrenden Autos muss sich sowohl die Aufzeichnung als auch die weitere Speicherung an den Anforderungen des Art. 6 Abs. 1 S. 1 Buchstabe f) DS-GVO (berechtigtes Interesse des Verantwortlichen) messen lassen.

Beweisführungsinteresse des Halters ist nachvollziehbar, jedoch nicht um jeden Preis!

Dabei muss das berechtigte Interesse des Verantwortlichen abgewogen werden gegenüber dem Recht der betroffenen Person, sich in der Öffentlichkeit frei zu bewegen und nicht befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Selbst wenn man ein berechtigtes Interesse des Tesla-Halters an der Beweisführung in möglichen Schadensfällen bejaht, ist die beschriebene Verarbeitung personenbezogener Daten von Passantinnen und Passanten und anderen Verkehrsteilnehmenden zur Wahrung dieses Interesses nicht erforderlich. Insbesondere ist es nicht erforderlich, die Fahrzeugumgebung im Umkreis von mindestens 50 Metern dauerhaft und anlasslos zu erfassen, um in einem potentiell eintre-

tenden Schadensfall Beweis führen zu können; selbst in den Fällen starker Beschädigung des Fahrzeugs ist jedenfalls eine Aufnahme und Speicherung von Filmsequenzen von 10 Minuten vor dem auslösenden Ereignis für eine Beweisführung nicht erforderlich. Ferner erfüllen die Verantwortlichen beim Betrieb des Wächtermodus ihre Informationspflichten aus Art. 13 DS-GVO nicht. Sowohl die Videoaufzeichnung ohne eine Rechtsgrundlage als auch der Verstoß gegen die Informationspflicht sind gemäß Art. 83 Abs. 5 Buchstabe a) und b) DS-GVO bußgeldbewährt.

Den bei mir eingegangenen Beschwerden gehe ich nach und werde auch die Öffentlichkeit weiter für das Thema sensibilisieren.

Darüber hinaus arbeitet meine Behörde in einer Unterarbeitsgruppe der Datenschutzkonferenz an einem Positionspapier zu solchen Fahrzeugfunktionen.

Zum Ende des Jahres 2022 erreichten mich Hinweise auf eine Veränderung der Wächtermodus-Funktionen. So soll z. B. nach Einspielen eines Updates die Speicherdauer individuell einstellbar sein (mindestens jedoch 1 Minute betragen); ferner soll es mehr Optionen für den Einsatz der Kamerafunktion geben. Selbstverständlich werde ich auch diesen Hinweisen, die die Verantwortlichen möglicherweise begünstigen, nachgehen. Keine Auswirkung haben diese eventuellen Änderungen jedoch auf die Fälle, in den nachweislich eine anlasslose Videoaufzeichnung stattgefunden hat.

8.3 Rechtswidriger Livestream von Fahrstunden

Im Berichtszeitraum erreichten mich Beschwerden über zwei Fahrschulen, die Fahrstunden live in Bild und Ton im Internet streamten. Dabei wurden auch Bilder von anderen Verkehrsteilnehmerinnen und Verkehrsteilnehmern, die sich im Erfassungsbereich der Kamera aufhielten sowie Bilder von und die Gespräche mit den Fahrschülerinnen und Fahrschülern übertragen. Diese Datenverarbeitungen waren rechtswidrig.

Für die Erhebung und Veröffentlichung personenbezogener Daten von Personen, die sich im öffentlichen Verkehrsraum befinden, gab es keine Rechtsgrundlage.

Auch wenn der Gedanke, Fahrschülerinnen und Fahrschülern die Gelegenheit zu geben, online von den Erfahrungen anderer zu profitieren, zunächst nachvollziehbar ist, kann die Verarbeitung nicht auf das berechtigte Interesse nach Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden. Die Rechte der betroffenen anderen Verkehrsteilnehmerinnen und Verkehrsteilnehmer stehen diesem Wunsch entgegen.

Das verfassungsmäßige Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Dazu gehört auch die Möglichkeit, eine Straße und andere öffentlich zugängliche Flächen zu durchqueren, ohne videoüberwacht zu werden.

Aufnahmen im Internet sind zudem einer unbestimmten Zahl von Personen weltweit zugänglich. Problematisch ist dabei, dass einmal veröffentlichte personenbezogene Daten nicht mehr vollständig zurückgeholt werden können. Für zufällig von der Kamera erfasste Personen und gegebenenfalls aus den Aufnahmen zu erkennenden Lebensumständen besteht daher ein großes Risiko. Dieses wird durch die steigende Qualität der Aufnahmen sowie die einfache Möglichkeit der technischen Vervielfältigung und Bearbeitung der Aufnahmen noch erhöht.

Datenschutzkonforme Ausgestaltung kaum möglich

Im Zuge des Verfahrens hatte sich eine der beiden Fahrschulen noch bemüht, das von ihr betriebene Livestreaming der Fahrstunden datenschutzkonform auszugestalten. Das erwies sich allerdings als kaum machbar.

Zwar wurde die Kamera zunächst ins Fahrzeuginnere gedreht, um keine anderen Verkehrsteilnehmerinnen und Verkehrsteilnehmer aufzunehmen. Jedoch konnten diese durch die Seitenfenster weiterhin erkennbar wahrgenommen werden.

Keine wirksame Einwilligung bei Minderjährigen

Aber auch für die Erfassung der Fahrschülerinnen und Fahrschüler braucht es eine Rechtsgrundlage. Die Verarbeitung sollte sich auf Einwilligungen der Fahrschülerinnen und Fahrschüler stützen.

Es ist davon auszugehen, dass viele Fahrschülerinnen und Fahrschüler das 18. Lebensjahr noch nicht vollendet haben. Durch den „Führerschein ab 17" besteht auch bei Sechzehnjährigen schon ein Interesse an Fahrstunden.

In Erwägungsgrund 38 zur DS-GVO heißt es „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind."

Ab welchem Alter Minderjährige selbst wirksam die Einwilligung in die Verarbeitung der sie betreffenden Daten erteilen können, hat die DS-GVO nicht eindeutig geregelt. Aus der Definition in Artikel 4 Nummer 11 DS-GVO lässt sich ableiten, dass die betroffene Person fähig sein muss, Bedeutung und Tragweite ihrer Erklärung zu erfassen. Zu der Frage, ab welchem Alter davon auszugehen ist, enthält die DS-GVO nur vereinzelte Aussagen. So regelt etwa Artikel 8 DS-GVO, dass bei einem direkt an ein Kind gerichteten Angebot von Diensten der Informationsgesellschaft das Kind selbst wirksam in die Datenverarbeitung einwilligen kann, wenn es 16 Jahre alt ist. Ist es jünger, bedarf es (auch oder stattdessen) der Zustimmung der Erziehungsberechtigten. Inwieweit diese Regelung der DS-GVO auf andere Einwilligungserklärungen durch Minderjährige verallgemeinerungsfähig ist, ist allerdings umstritten.

Der Maßstab für die Bewertung, bis zu welchem Alter Eltern anstatt des Kindes oder zusätzlich die Einwilligung erteilen müssen, ist nicht das Alter selbst, sondern ob eine minderjährige Person fähig ist, die Tragweite der Entscheidung zu erfassen.

16 Jahre scheint grundsätzlich eine plausible Altersgrenze zu sein, da man Minderjährigen mit 16 durchaus eine Entscheidungsfähigkeit zusprechen kann. Das Einvernehmen mit der oder dem Minderjährigen ist in jedem Fall herzustellen.

Allerdings sind die Fahrschülerinnen und Fahrschüler in der Fahrstunde durch die ungewohnte für sie neue Tätigkeit des Fahrens abgelenkt und mit der zeitgleichen Reflektion, dass ihre Äußerungen über sich und andere weltweit übertragen werden, überfordert. Die latent bestehenden besonderen Gefahren durch die weltweite Live-Veröffentlichung von Äußerungen über das Internet sind der betroffenen Person – insbesondere der sehr jungen Person – in der besonderen Situation vermutlich nicht bewusst.

Auch im BGB wird bei der Abgabe von Willenserklärungen in Rechtsgeschäften vielfach auf die Verständigkeit von Minderjährigen abgestellt. Gemäß § 107 BGB benötigt der Minderjährige zu einer Willenserklärung, durch die er nicht lediglich einen rechtlichen Vorteil erlangt, der Einwilligung seines gesetzlichen Vertreters. Im dargestellten Zusammenhang ergibt sich für die Fahrschülerinnen und Fahrschüler kein Vorteil durch die Verarbeitung ihrer personenbezogenen Daten.

In einem Gespräch können auch politische Meinungen, religiöse oder weltanschauliche Überzeugungen geäußert werden. Es ist zu berücksichtigen, dass die Veröffentlichung dieser durch Artikel 9 DS-GVO besonders geschützten personenbezogenen Daten für die Betroffenen besonders folgenschwer sein kann.

Aus dem Zusammentreffen dieser Besonderheiten ergab sich die Erforderlichkeit der Einwilligung der gesetzlichen Vertreter bei den minderjährigen Fahrschülerinnen und Fahrschülern.

Keine geeigneten Garantien bei Drittstaatentransfer

Die zur Veröffentlichung genutzten Plattformen wurden unter anderem von US-amerikanischen Unternehmen bereitgestellt. Damit wurden die personenbezogenen Daten der Nutzer potenziell in die USA übermittelt. In den USA besteht derzeit kein angemessenes Datenschutzniveau. Transfers von personenbezogenen Daten an Diensteanbieter aus den USA dürfen daher nur vorbehaltlich geeigneter Garantien, wie zum Beispiel Standarddatenschutzklauseln, oder bei Vorliegen eines Ausnahmetatbestandes für bestimmte Fälle gemäß Artikel 49 DS-GVO erfolgen. Zu beachten ist, dass der reine Abschluss von Standarddatenschutzklauseln wie den von der EU-Kommission beschlossenen Standardvertragsklauseln nicht ausreicht. Im Einzelfall muss darüber hinaus geprüft werden, ob das Recht oder die Praxis des Drittlandes den durch die Standardvertragsklauseln garantieren Schutz beeinträchtigen und ob gegebenenfalls ergänzende Maßnahmen zur Sicherstellung der Wirksamkeit der Standardvertragsklauseln zu treffen sind. Für die USA ist der EuGH im Anwendungsbereich der US-Auslandsaufklärungsprogramme der Auffassung,

dass das Schutzniveau nicht dem in der EU entspricht, unter anderem weil nationale Regelungen der USA unverhältnismäßige Zugriffsrechte für US-Geheimdienste vorsehen und weil EU-Bürgerinnen und -Bürger keine wirksamen Rechtsbehelfe gegen die weitreichenden Zugriffsbefugnisse von US-Behörden auf personenbezogene Daten haben. Um die vom EuGH identifizierten Unzulänglichkeiten der nationalen Regelungen der USA auszugleichen, wäre es erforderlich, Maßnahmen zu ergreifen, die den Zugriff der US-Behörden – und damit der Diensteanbieter – auf personenbezogene Daten verhindern oder ineffektiv machen. In den beiden durchgeführten Verfahren haben die Inhaber der Fahrschulen nicht nachgewiesen, dass der Zugriff der US-Behörden auf personenbezogene Daten durch zusätzliche Maßnahmen verhindert oder ineffektiv gemacht wurde.

Verarbeitung beendet

Beide Fahrschulen haben aufgrund der geführten Verwaltungsverfahren das Streamen der Fahrstunden eingestellt.

Zudem sind in beiden Fällen Ordnungswidrigkeitenverfahren eingeleitet worden.