Schleswig-Holsteinischer Landtag
Umdruck 20/4694

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Kiel, 9. Oktober 2024

Sitzung des Innen- und Rechtsausschusses am 09.10.2024 – TOP 2

Sehr geehrte Damen und Herren Abgeordnete,

vielen Dank für die Einladung und die Gelegenheit, Ihnen einige Punkte aus meinem Tätigkeitsbericht für das Jahr 2023 vorzustellen, den ich Ihnen als Landesbeauftragte für Datenschutz und als Landesbeauftragte für Informationszugang im April 2024 übergeben habe.

Link zum 42. Tätigkeitsbericht des ULD: https://www.datenschutzzentrum.de/tb/tb42/

Unseren Überblick zu Zahlen und Fakten zur Tätigkeit meiner Dienststelle im Jahr 2023 habe ich Ihnen mitgebracht. Die Zahl der Beschwerden hat sich im Vergleich zu den Vorjahren auf hohem Niveau eingependelt: Im Jahr 2023 sind 1.344 schriftliche Beschwerden eingegangen, etwa ähnlich viele wie im Vorjahr (1.334). Die Zahl der Meldungen von Verletzungen des Schutzes personenbezogener Daten (kurz: Datenpannen) stieg weiter an: Mit 527 Meldungen ist die Vorjahreszahl (485) übertroffen worden, doch die durch mehrere Angriffswellen verursachte Höchstzahl von 649 aus dem Jahr 2021 ist noch nicht wieder erreicht worden.

Das Jahr 2023 war für meine Dienststelle ein besonderes als Vorsitz der Datenschutzkonferenz, der reihum unter den 18 Mitgliedern, den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Bayern ist mit zwei Behörden vertreten), wechselt. Die Vorsitzfunktion oblag im Jahr 2023 Schleswig-Holstein, und dies hat die Dienststelle ab dem 1. Januar 2023 geprägt.

Die Datenschutzkonferenz hat u. a. die Aufgabe, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen. Auf europäischer Ebene geschieht dies über den Europäischen Datenschutzausschuss, in dem die Aufsichtsbehörden Mitglied sind.

Die europäischen Vorgaben – nämlich die Grundrechte-Charta, die Datenschutz-Grundverordnung (DSGVO) und die Datenschutzrichtlinie für den Bereich Justiz und Inneres – sind die Basis für möglichst einheitliche Auslegungen des Datenschutzrechts. Seitdem die DSGVO gilt, ist die intensive Kommunikation zwischen den verschiedenen Aufsichtsbehörden mit geeinten Ergebnissen zur Rechtsauslegung noch wichtiger geworden. In der Zeit vor Geltung der DSGVO gab es nur zwei Tagungen im Jahr, doch unter meinem Vorsitz der Datenschutzkonferenz waren neun Tagungen und 40 wöchentliche Abstimmungstreffen zu leiten. Hinzu kamen zahlreiche Gespräche mit Stakeholdern, in denen es meine Rolle war, für die Datenschutzkonferenz zu sprechen.

Auf Bundesebene liegt der Entwurf für eine Novelle des Bundesdatenschutzgesetzes vor, in dem die Datenschutzkonferenz institutionalisiert wird. Das begrüße ich. Allerdings bleibt im Regelungsentwurf vieles offen: Zum Beispiel wird es nicht ohne eine Geschäftsstelle der Datenschutzkonferenz gehen, um eine Kontinuität der Arbeiten zu gewährleisten.

Wir Datenschutzaufsichtsbehörden planen auch Maßnahmen zur Entbürokratisierung, z. B. ein Portal zur erleichterten Erfüllung der Meldepflichten von Verletzungen des Schutzes personenbezogener Daten. Dies ließe sich ebenfalls über eine Geschäftsstelle umsetzen.

In der Diskussion für die Errichtung einer Geschäftsstelle der Datenschutzkonferenz ist eine Verwaltungsvereinbarung, die von den Ländern geschlossen werden müsste. Auch ein Staatsvertrag wäre denkbar. Dies möchte ich bereits jetzt in Ihr Bewusstsein rücken.

Die Einheitlichkeit in der Auslegung hängt allerdings auch von einer Harmonisierung der geltenden rechtlichen Vorgaben ab. Akteure aus dem Bereich der Medizinforschung hatten sich an uns gewandt, weil sie in Verbundvorhaben, die mehrere Länder betreffen, Schwierigkeiten hätten, die verschiedenen rechtlichen Anforderungen – z. B. aufgrund unterschiedlicher Krankenhausgesetze und Forschungsklauseln auf der Ebene von Bund und Ländern – zu erfüllen. In der Tat ist es zurzeit nicht einfach für Forschende, die verschiedenen Anforderungen umzusetzen, wenn sich in den Gesetzen schon Definitionen (als Beispiel: „Was sind Patientendaten?“) unterscheiden. Die Datenschutzkonferenz hat daher dazu eine Ausarbeitung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vorgelegt, die wir auch den Regierungen von Bund und Ländern übersandt haben.

Vieles kommt aus Europa: Für zahlreiche neue verabschiedete Gesetze auf EU-Ebene im Bereich des Digitalrechts besteht die Notwendigkeit, Zuständigkeiten und Rollen zu definieren. Für Deutschland bedeutet dies, dass auch entschieden werden muss, für welche Bereiche der Bund und wann die Länder zuständig sind. Das prominenteste Beispiel ist die KI-Verordnung (AI Act). Hier besteht die Notwendigkeit, die für die Marktüberwachung zuständigen Behörden festzulegen. Unsere Arbeit als Datenschutzaufsicht hat große Überschneidungsmengen mit dem Bereich der Künstlichen Intelligenz, denn sehr häufig werden personenbezogene Daten bei dem Training oder bei der Nutzung von KI-Modellen oder KI-Systemen eine Rolle spielen. Nach dem Vernehmen läuft es bei der Festlegung der Aufgabe der Marktüberwachung auf die Bundesnetzagentur zu. Nach den bisherigen Darstellungen würde diese Aufsicht für den Bereich KI dann aber auch die Aufsicht über KI in der Polizei oder im Bildungsbereich umfassen, sodass Länderinteressen tangiert wären. Der jetzige Vorsitz der Datenschutzkonferenz informiert zurzeit die Ministerpräsidentenkonferenz über diesen Umstand.

In jedem Fall wird es aber eine Herausforderung darstellen, die verschiedenen Aufsichtsbehörden im Bereich KI zu koordinieren. Während wir in der Datenschutzkonferenz einen Einigungsmechanismus erarbeitet haben, ist dies in anderen Bereichen (noch) nicht der Fall. Die Datenschutzaufsichtsbehörden hätten sich auch vorstellen können, selbst die Aufsicht nach KI-VO zu übernehmen, so wie diese

Aufgabe auf europäischer Ebene auch dem Europäischen Datenschutzbeauftragten zukommt und in mehreren Mitgliedstaaten wohl geplant ist. Das Modell ist vom Bundesgesetzgeber aber anscheinend nicht gewollt.

Zum parlamentarischen Datenschutz gab es im Jahr 2024 (also noch nicht im Bericht berücksichtigt) eine Neuerung durch ein Urteil des EuGH: Demnach ist eine Datenschutzaufsicht auch im parlamentarischen Bereich nötig, und im Zweifelsfall muss die vorhandene Datenschutzaufsichtsbehörde (also wir) diese Aufgabe übernehmen. Deswegen ist wesentlich, dass für den parlamentarischen Datenschutz eine eigene Aufsicht etabliert wird.

Es gibt aber noch einen weiteren Bereich, in dem die Aufsicht fehlt und auch nicht von uns wahrgenommen werden kann, nämlich den justiziellen Bereich. Hier hat die Datenschutzkonferenz schon vor längerer Zeit darauf hingewiesen, dass eine Lücke besteht, die geschlossen werden müsste, und den Kontakt zur Justizministerkonferenz aufgenommen. Allerdings teilte man unsere Ansicht nicht, dass diese Lücke geschlossen werden müsse. In einem Fall vor dem Schleswig-Holsteinischen Verwaltungsgericht hatte ein Kläger von uns ein Tätigwerden in einem Fall gefordert, in dem es um einen möglichen Datenschutzverstoß eines Gerichts im Rahmen seiner justiziellen Aufgaben ging, doch wir konnten hier nicht tätig werden. Dies wurde auch vom VG Schleswig so bestätigt.

Unser jährlicher Tätigkeitsbericht besteht aus zwei Teilen: dem Bericht als Landesbeauftragte für Datenschutz und dem Bericht als Landesbeauftragte für Informationszugang. Mit der Reform des Informationszugangsgesetzes Schleswig-Holstein haben wir ein Recht auf Beanstandung erhalten, von dem wir seitdem auch mehrfach Gebrauch gemacht haben. Wir setzen dort aber auch viel auf Beratung und übertragen das Prinzip des „Datenschutzes by Design“ auf die Transparenzanforderungen der Verwaltung durch Ausarbeitungen zu „Informationsfreiheit by Design“.

Vielfach lassen sich Probleme bei der Gestaltung von Verarbeitungen, aber auch in der Rechtsetzung durch eine frühzeitige Einbindung meiner Behörde vermeiden – das klappt teilweise ganz gut, aber dort hakt es auch immer mal wieder. Hier kann ich nur dafür werben, dass die Regierung uns einbezieht. Auch für Sie besteht natürlich unser Angebot, sich an uns zu wenden, wenn Fragen bestehen.

Vielen Dank für Ihre Aufmerksamkeit!
Für Fragen stehen Ihnen mein Team und ich gern zur Verfügung.

Dr. h. c. Marit Hansen
Landesbeauftragte für Datenschutz
Landesbeauftragte für Informationszugang

Ergänzende Materialien im Nachgang der Sitzung

Anlage 1: Schreiben des Vorsitzes der Datenschutzkonferenz vom 11.10.2024 an alle Ministerpräsidentinnen und Ministerpräsidenten zu den Vorschlägen der Bundesregierung zur KI-Aufsicht; Ausfertigung Schleswig-Holstein

Anlage 2: Urteil des Schleswig-Holsteinischen Verwaltungsgerichts vom 18.06.2024 – 8 A 89/22 – zur Aufgabe des Gesetzgebers, eine datenschutzrechtliche Kontrolle für den Bereich der justiziellen Tätigkeit zu schaffen

Anlage 3: Entschließung der Datenschutzkonferenz „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vom 23.11.2023, u. a. mit Bezug zu den verschiedenen Landeskrankenhausgesetzen

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT
Postfach 31 63 · 65021 Wiesbaden

Ministerpräsident des Landes
Schleswig-Holstein
Herrn Daniel Günther
Düsternbrooker Weg 104
24105 Kiel

Per E-Mail:
[redacted]@stk.landsh.de

DSK
DATENSCHUTZKONFERENZ
Vorsitz 2024
Der Hessische Beauftragte für
Datenschutz und Informationsfreiheit

Ansprechpartner: DSK-Team

E-Mail-Adresse:
dsk2024@datenschutz.hessen.de

Telefonnummer:
0611/1408-121

11. Oktober 2024

Vorschläge der Bundesregierung zur Zentralisierung der KI-Aufsicht

Sehr geehrter Herr Ministerpräsident,

nach Veröffentlichungen des Bundesministeriums für Wirtschaft und Klima vom 20. September 2024 (https://www.bmwk.de/Navigation/DE/Home/home.html) soll sich die Bundesregierung in einer zentralen Frage der nationalen Umsetzung der seit August 2024 in Kraft getretenen neuen KI-Verordnung bereits abschließend festgelegt haben: Sie will die Marktaufsicht über Systeme der Künstlichen Intelligenz (KI) nach der KI-Verordnung (KI-VO) vollständig der Bundesnetzagentur übertragen. Damit soll die Marktaufsicht in diesem zentralen Zukunftsbereich mit vielfältigen Auswirkungen auf Wirtschaft und Verwaltung vollständig in den Händen einer Bundesbehörde liegen. Dies betrifft insbesondere auch den Einsatz von KI-Systemen in der Landesverwaltung, obwohl diese Festlegung in wichtigen Bereichen den Regelungen der KI-Verordnung widerspricht. Damit treten für KI zusätzliche Aufsichtsbeziehungen für Unternehmen und öffentliche Stellen neben die bestehenden Zuständigkeiten der Datenschutzaufsicht.

Aus Sicht der Datenschutzaufsichtsbehörden des Bundes und der Länder sollten diese Vorschläge sowohl europarechtlich als auch verfassungsrechtlich überprüft und zur Vermeidung von Bürokratiebelastungen für die gesamte deutsche Wirtschaft grundlegend überarbeitet werden:

Soweit die Bundesregierung beabsichtigt, Aufgaben einer Marktüberwachungsbehörde des Bundes auch auf den Einsatz von KI durch Landesverwaltungen zu erstrecken, greift sie damit in föderale Grundprinzipien ein und beeinträchtigt die eigenständige Aufgabenwahrnehmung von Ländern und Kommunen. Im Ergebnis würde diese Konstruktion bedeuten, dass die Bundesnetzagentur z.B. den Einsatz von KI-Systemen durch die Landespolizeien, Schulen und Hochschulen beaufsichtigt und damit die Nutzung wichtiger KI-Innovation im Sicherheitsbereich – losgelöst von jeder Kontrolle der Landesparlamente – der Regulierung einer Bundesbehörde unterworfen würde.

Die Vorschläge für eine allumfassende KI-Marktüberwachung durch den Bund überschreiten zudem auch unionsrechtliche Handlungsspielräume: Soweit die Bundesregierung hier beabsichtigt, auch die Aufgaben der Bundesnetzagentur zuzuweisen, die die KI-VO in Art. 74 Abs. 8 den Datenschutzaufsichtsbehörden zuordnet, widerspricht dies dem Wortlaut und Regelungsziel der KI-VO. Sie missachtet dabei, dass die KI-VO für vier von acht Risikobereichen in Anhang III der KI-VO gemäß Art 74 Abs. 8 KI-VO die Marktaufsicht den Datenschutzaufsichtsbehörden überträgt. Dies betrifft Nr. 1 (Biometrie, sofern diese Systeme für Strafverfolgungszwecke, Grenzmanagement und Justiz und Demokratie eingesetzt werden), Nr. 6 (Strafverfolgung), Nr. 7 (Migration, Asyl und Grenzkontrolle) und Nr. 8 (Rechtspflege und demokratische Prozesse). Es ergibt Sinn, den Schutz von Demokratie und Rechtsstaat völlig unabhängigen Institutionen anzuvertrauen. Außerdem hat Art. 77 KI-VO i.V.m. Art. 1 Abs. 2 und Art. 51 DS-GVO für den Grundrechtsschutz ohnehin die Datenschutzbehörden vorgesehen.

Wer die Aufsicht in den anderen vier Risikobereichen ausüben soll, lässt die KI-VO offen. Nur hier besteht Entscheidungsspielraum der Mitgliedstaaten. Die derzeitigen Vorschläge der Bundesregierung sehen die Aufsicht der Bundesnetzagentur für alle acht Risikobereiche vor und wollen den Datenschutzbehörden die ihnen in Art. 74 Abs. 8 KI-VO übertragenen Aufsichtsaufgaben nehmen. Sie berufen sich dafür auf den Wortlaut der Vorschrift:

„[…] benennen die Mitgliedstaaten … als Marktüberwachungsbehörden entweder die nach der [DSGVO] oder der [JI-RL] für den Datenschutz zuständigen Aufsichtsbehörden oder jede andere gemäß denselben Bedingungen wie den in den Artikeln 41 bis 44 [JI-RL] festgelegten benannte Behörde“.

Art. 74 Abs. 8 KI-VO enthält jedoch keine Öffnungsklausel, nach der Mitgliedstaaten frei andere Behörden benennen können. Vielmehr ist diese Regelung ein Trilog-Kompromiss: Privilegien beim KI-Einsatz durch Strafverfolgungsbehörden wurden nur unter der Bedingung

akzeptiert, dass die für die JI-RL bereits zuständigen Behörden die Marktüberwachung wahrnehmen. In manchen Mitgliedstaaten sind dies andere als die Datenschutzbehörden. Die Bezugnahme auf die Art. 41 bis 44 JI-RL und die Vergangenheitsform der bereits „benannten“ Behörden sollen dies zum Ausdruck bringen. Die KI-VO überträgt also ohne Entscheidungsspielraum für die Mitgliedstaaten die Marktaufsicht über die genannten Risikobereiche den Datenschutzbehörden oder den bereits benannten Aufsichtsbehörden nach JI-RL. Die Mitgliedstaaten können nur benennen, welche Behörden dies sind.

Im Blick auf den KI-Einsatz durch Unternehmen und damit die Marktüberwachung in den weiteren Risikobereichen der KI-VO und damit im Übrigen auch den weiten Bereich der Betreiberpflichten von nicht risikoklassifizierten KI-Systemen bleibt zu berücksichtigen, dass die Datenschutzbehörden nach Art. 77 und Erwägungsgrund 157 KI-VO zunächst schon ohnehin für die Verarbeitung personenbezogener Daten in den Bereichen Nr. 3 (Bildung), Nr. 4 (Beschäftigung) und Nr. 5 (öffentliche Dienste und Leistungen) zuständig sind. Aufgrund dieser durch die DSGVO und Art. 77 KI-VO begründeten Aufgaben und Befugnisse der Datenschutzaufsichtsbehörden sowie der langjährigen Erfahrung im Bereich der Beratung, Beschwerdebearbeitung und Kooperation auf nationaler wie europäischer Ebene sollten daher in Deutschland grundsätzlich die nationalen Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden benannt werden.

Das Ziel einer einheitlichen Anwendung der KI-VO ist mit der Übertragung von Aufgaben der Marktüberwachung allein an eine zentrale Stelle nicht zu erreichen. Sowohl im Bereich der KI- als auch der Datenschutzaufsicht hätten Unternehmen und Behörden wie auch Betroffene dagegen bei einer Bündelung der Zuständigkeiten im Regelfall nur mit einer Aufsichtsbehörde zu tun. Zudem verfügen die Datenschutzaufsichtsbehörden nicht nur über einschlägige Fachkunde und die von der KI-VO geforderte Unabhängigkeit, sondern auch über funktionierende Kooperations- und Kohärenzmechanismen.

Verfassungsrechtlich ist zu beachten, dass die Zuständigkeiten für die Marktüberwachung nach der KI-VO Bund und Ländern nach den allgemeinen Regeln zugewiesen werden müssen: Während Landesbehörden im Grundsatz die Aufsicht führen, wird eine Bundesbehörde für die einheitliche Regelung gesamtstaatlicher Sachverhalte zuständig sein (Art. 83, 72 Abs. 2 GG). Dies entspricht auch der Struktur der Behörden im Produktsicherheitsrecht, welche die Marktüberwachungs-Verordnung umsetzen (§ 4 MÜG, § 25 ProdSG). Überzeugende Rechtfertigungsgründe für eine Abweichung von diesem Grundsatz durch Aufbau einer zentralen, im Regelfall weit vom tatsächlichen betrieblichen Einsatz und den damit einhergehenden Risiken für Verbraucherinnen und Verbraucher

entfernten Überwachungsbehörde des Bundes sind bislang nicht ersichtlich. Auch ist es für Unternehmen in den Ländern, die KI anwenden, von Vorteil, wenn sie von Aufsichtsbehörden überwacht werden, die die regionalen Besonderheiten kennen und mit denen sie in Datenschutzfragen in den relevanten Bereichen Bildung, Beschäftigung und öffentliche Dienste und Leistungen ohnehin zu tun haben.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sind einhellig der Auffassung, dass die von der Bundesregierung vorgesehene Aufgaben- und Zuständigkeitsverteilung in hohem Maße ineffektiv für Innovationsförderung und Grundrechtsschutz gleichermaßen sein wird, durch Doppelstrukturen volkswirtschaftlich vermeidbare Bürokratiebelastungen erzeugt und letztlich im Hinblick auf die Vorgaben des Art. 74 Abs. 8 KI-VO bereits europarechtswidrig ist.

Die Datenschutzkonferenz bittet deshalb die Landesregierungen, sich für eine Bündelung von Marktüberwachungsaufgaben und der Aufgaben der Datenschutzaufsicht bei den Datenschutzbehörden des Bundes und der Länder einzusetzen, wie sie eingehend in unseren Vorschlägen vom 3. Mai 2024 (20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf (datenschutzkonferenz-online.de) vorgestellt wurde. Gerne stehe ich gemeinsam mit meinen Kolleginnen und Kollegen der Datenschutzaufsichtsbehörden des Bundes und der Länder für weitere Erläuterungen zur Verfügung, um zu einer handlungsfähigen, effektiven und Bürokratiebelastungen vermeidenden Ausgestaltung der nationalen Aufsichtsregelungen für die Entwicklung und Nutzung Künstlicher Intelligenz beizutragen.

Mit freundlichen Grüßen

Prof. Dr. Alexander Roßnagel

Verteiler:
Vorsitzender der Ministerpräsidentenkonferenz
Vorsitzende des Bundesrats
Ministerpräsidentinnen und Ministerpräsidenten der Länder
Regierender Bürgermeister von Berlin
Bürgermeister der Freien Hansestadt Bremen
Präsident des Senats und Bürgermeister der Freien und Hansestadt Hamburg

SCHLESWIG-HOLSTEINISCHES VERWALTUNGSGERICHT

Az.: 8 A 89/22

IM NAMEN DES VOLKES

URTEIL

In der Verwaltungsrechtssache

- Kläger -

gegen

das Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel

- Beklagte -

Streitgegenstand: Datenschutzrecht

hat die 8. Kammer des Schleswig-Holsteinischen Verwaltungsgerichts auf die mündliche Verhandlung vom 18. Juni 2024 durch den Richter am Verwaltungsgericht als Einzelrichter für Recht erkannt:

Die Klage wird abgewiesen.

Der Kläger trägt die Kosten des Verfahrens.

Das Urteil ist wegen der Kosten vorläufig vollstreckbar.

Dem Kläger wird nachgelassen, die Vollstreckung durch Zahlung einer Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages abzuwenden, wenn nicht zuvor der Beklagte Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.

Tatbestand

Die Beteiligten streiten über ein datenschutzrechtliches Tätigwerden des Beklagten.

Der Kläger war Opfer einer Straftat und in dem Strafprozess als Zeuge und Adhäsionskläger beteiligt. Er hatte im Vorwege das Amtsgericht darum gebeten, seine Anschrift nicht zu nennen. In dem Urteil des Amtsgerichts Itzehoe vom 28.01.2022 wurde er dennoch als Neben- und Adhäsionskläger genannt und auch seine Anschrift angegeben.

Der Kläger wandte sich deshalb mit Schreiben vom 21. Februar 2022 an den Beklagten und bat darum, den Sachverhalt zu überprüfen. Er wies darauf hin, dass es eine melderechtliche Auskunftssperre gebe, die jetzt Makulatur sein dürfte.

Der Beklagte wies den Kläger mit Schreiben vom 28. Februar 2022 darauf hin, dass zwar auch das Datenschutzrecht für die Gerichte uneingeschränkt gelte. Allerdings sei der Datenschutzaufsichtsbehörde die Kontrolle der Gerichte entzogen. Eine Kontrolle über die rechtsprechende Gewalt sei nicht möglich. Dies ergebe sich aus dem verfassungsrechtlichen Grundsatz der Gewaltenteilung, sei aber auch ausdrücklich geregelt in § 2 Abs. 2 Satz 2 Landesdatenschutzgesetz bzw. Art. 55 Abs. 3 DSGVO.

Mit Schreiben vom 1. März 2022 ergänzte der Beklagte, dass es sich bei der Erstellung eines Urteils um eine justizielle Tätigkeit handele, die der datenschutzrechtlichen Kontrolle entzogen sei. Die Entscheidung von Rechtstreitigkeiten sei Kern richterlicher Tätigkeit. Eine Aufsicht über die rechtsprechende Tätigkeit dürfe der Beklagte als Behörde der vollziehenden Gewalt nicht vornehmen.

Der Kläger hatte sich auch an den überörtlichen behördlichen Datenschutzbeauftragten des Landgerichts Itzehoe gewandt. Dieser teilte dem Kläger mit Schreiben vom 19. Mai 2022 mit, dass er seinen Unmut über die Nennung seiner Anschrift im Urteil durchaus nachvollziehen könne. Eine Verletzung bestehender datenschutzrechtlicher Vorschriften sei aber nicht zu erkennen. Bei dem Urteil handele es sich hinsichtlich der Aussprüche im Adhäsionsverfahren um einen vollstreckbaren Titel. Als Vollstreckungstitel müsse das Urteil den Kläger richtigerweise mit den nach § 313 Abs. 1 Nr. ZPO erforderlichen Angaben (Name und Anschrift) im Rubrum oder in der Urteilsformel bezeichnen. Abschließend wurde darauf hingewiesen, dass ein Beschwerderecht beim Beklagten bestehe.

Mit Bescheid vom 17. Juni 2022 teilte der Beklagte dem Kläger mit, dass auch nach Auswertung des Schriftwechsels zwischen dem Kläger und dem Datenschutzbeauftragten des Landgerichts Itzehoe ein neuer Sachverhalt nicht erkennbar sei. Dass Name und Anschrift des Klägers in einem Urteil genannt worden sei, unterliege nicht der Kontrolle, weil es sich um eine justizielle Tätigkeit handele. Man könne deshalb in dieser Angelegenheit nicht tätig werden.

Dagegen hat der Kläger am 23. Juni 2022 Klage erhoben. Er macht geltend, dass der Begriff der justiziellen Tätigkeit alle Verarbeitungen im Zusammenhang mit der gerichtlichen Entscheidungsfindung, einschließlich deren Vorbereitung und Durchführung, umfasse. Die Angabe der Adresse des verletzten Straftatopfers sei aber für die Entscheidungsfindung des Gerichts nicht erforderlich. Im Übrigen ergebe es sich aus dem Erwägungsgrund 20 Satz 3 zur DSGVO, dass besondere Stellen im Justizsystem des Mitgliedsstaates zu schaffen seien, die die Einhaltung der Vorschriften der DSGVO sicherstellten. Auch in der Literatur werde die Einrichtung solcher besonderen Stellen zur Selbstkontrolle befürwortet.

Der Kläger beantragt sinngemäß,

> den Beklagten zu verpflichten, die Nennung seiner Anschrift in dem Urteil des Amtsgerichts Itzehoe vom 28.01.2022 (Az. 45 Ds 321 Js 20067/21) zu beanstanden bzw. tätig zu werden.

Der Beklagte beantragt,

> die Klage abzuweisen.

Er erwidert, dass man eine inhaltliche Auseinandersetzung mit der Beschwerde des Klägers nicht habe vornehmen können. Dies ergebe sich aus Art. 55 Abs. 3 DSGVO und § 2 Abs. 2 Satz 2 Landesdatenschutzgesetz. Nach Art. 55 Abs. 3 DSGVO sei man nicht zuständig für die von Gerichten im Rahmen ihrer justiziellen Tätigkeiten vorgenommenen Verarbeitungen personenbezogener Daten. Nach § 2 Abs. 2 Satz 2 Landesdatenschutzgesetz gelte Abschnitt 2 Unterabschnitt 4 des Landesdatenschutzgesetzes, der die Aufgaben und Befugnisse der Landesbeauftragten für Datenschutz regele, nicht für die Gerichte hinsichtlich ihrer justiziellen Tätigkeit. Die Beschwerde des Klägers richte sich gegen eine Verarbeitung von personenbezogenen Daten im Rahmen der justiziellen Tätigkeit des Amtsgerichts Itzehoe. Für die Auslegung des Begriffs der justiziellen Tätigkeit sei Erwägungsgrund 20 der DSGVO heranzuziehen. Danach solle die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleiben. Dies entspreche auch dem deutschen Verfassungsrecht mit den Grundsätzen der Gewaltenteilung und der richterlichen Unabhängigkeit. Sowohl alle die Entscheidung vorbereitenden Handlungen als auch die Entscheidung selbst, d.h. die Anfertigung von Urteilen und Beschlüssen, würden zur justiziellen Tätigkeit gehören. Zwar sollen die Mitgliedsstaaten nach Erwägungsgrund 20 der DSGVO besondere Stellen im Justizsystem schaffen und diese mit der Aufsicht über Datenverarbeitungsvorgänge im Rahmen der justiziellen Tätigkeit betrauen. Dieser Erwägungsgrund sei aber nicht umgesetzt worden. In Schleswig-Holstein sei weder durch Bundes- noch durch Landesrecht eine Stelle für die Kontrolle der Datenverarbeitung der Gerichte bestimmt worden.

Wegen der weiteren Einzelheiten wird auf die Gerichtsakte und die beigezogenen Verwaltungsvorgänge Bezug genommen.

Entscheidungsgründe

Die zulässige Klage hat keinen Erfolg. Der Kläger hat keinen Anspruch darauf, dass der Beklagte im Hinblick auf das Urteil des Amtsgerichts Itzehoe vom 28.01.2022 (Az. 45 Ds 321 Js 20067/21) datenschutzrechtlich im Wege der Aufsicht tätig wird bzw. eine Beanstandung ausspricht. Gemäß § 61 Abs. 2 Landesdatenschutzgesetz ist die Landesbeauftragte nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen. Dies ergibt sich gleichlautend auch aus Art. 55 Abs. 3 DSGVO.

Bei dem Urteil des Amtsgerichts Itzehoe und der darin enthaltenen Anschrift des Klägers als Neben- und Adhäsionskläger handelt es sich um eine personenbezogene Datenverarbeitung im Rahmen der justiziellen Tätigkeit im Sinne des § 61 Abs. 2 Landesdatenschutzgesetz bzw. Art. 55 Abs. 3 DSGVO. Dazu zählen Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch die Gerichte. Der Beklagte weist zu Recht darauf hin, dass dies aus der Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben erfolgt. Dazu gehört auch das Abfassen von Urteilen. Die justizielle Tätigkeit umfasst sowohl die vorbereitenden Handlungen für die Entscheidung als auch die Entscheidung selbst, d.h. das Urteil mit allen seinen Angaben und Daten (vgl. Kreul in: Gierschmann/Schlender/Stentzel/Veil, Kommentar zur Datenschutzgrundverordnung, Köln 2018, Art. 55 Rn. 18; Nguyen/Stroh in: Gola, DS-GVO, Kommentar, 2. Aufl., Art. 55 Rn. 17; von Lewinsky in: Auenhammer, DSGVO/BDSG, Kommentar, 6. Aufl., Art. 55 Rn. 7; Schaffland/Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung, Kommentar, Art. 55 Rn. 7).

Der Kontrolle sind im Hinblick auf die richterliche Unabhängigkeit sämtliche Tätigkeiten entzogen, die im Zusammenhang mit der gerichtlichen Entscheidungsfindung stehen. Dazu gehört auch das Abfassen eines Urteils und die darin enthaltenen personenbezogenen Daten. Nur soweit die Gerichte in Verwaltungsangelegenheiten tätig werden, unterfallen sie der Kontrolle der Datenschutzbehörden.

Es ist richtig, dass dort, wo die Zuständigkeit der Aufsichtsbehörden nicht besteht, besondere Stellen im Justizsystem des Mitgliedsstaates die Einhaltung der Vorschriften der DSGVO sicherstellen und entsprechende Beschwerden bearbeiten sollen (vgl. Erwägungsgrund 20). Es ist aber Aufgabe des Gesetzgebers, eine datenschutzrechtliche Kontrolle für den Bereich der justiziellen Tätigkeit zu schaffen. Eine solche Regelung ist aber bislang nicht geschaffen worden.

Die Klage ist deshalb mit der Kostenfolge aus § 154 Abs. 1 VwGO abzuweisen.

Die Entscheidung über die vorläufige Vollstreckbarkeit ergibt sich aus § 167 Abs. 2 VwGO i.V.m. den §§ 708 Nr. 11, 711 ZPO.

Rechtsmittelbelehrung

Gegen dieses Urteil ist das Rechtsmittel der Berufung statthaft, wenn diese von dem Oberverwaltungsgericht zugelassen wird. Die Zulassung der Berufung ist innerhalb eines Monats nach Zustellung dieses Urteils beim Schleswig-Holsteinischen Verwaltungsgericht, Brockdorff-Rantzau-Straße 13, 24837 Schleswig zu beantragen. Der Antrag muss das angefochtene Urteil bezeichnen. Innerhalb von zwei Monaten nach Zustellung dieses Urteils sind die Gründe, aus denen die Berufung zuzulassen ist, darzulegen. Die Begründung ist, soweit sie nicht bereits mit dem Antrag vorgelegt worden ist, bei dem Schleswig-Holsteinischen Oberverwaltungsgericht, Brockdorff-Rantzau-Straße 13, 24837 Schleswig einzureichen.

Im Berufungsverfahren - einschließlich des Antrages auf Zulassung der Berufung - müssen sich die Beteiligten durch Prozessbevollmächtigte im Sinne von § 67 VwGO vertreten lassen.

Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023

Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Medizinische Forschungsprojekte werden in Deutschland häufig nicht nur in einem Bundesland durchgeführt. Vielmehr sind zunehmend verschiedene Forschungseinrichtungen aus unterschiedlichen Ländern daran beteiligt (z. B. länderübergreifende Verbundforschung, multizentrische Studien). Je nach Forschungsstandort sind unterschiedliche datenschutzrechtliche Anforderungen zu beachten. Dies erschwert nicht nur die Forschung, sondern wirkt sich auch nachteilig auf den Datenschutz für die betroffenen Personen aus. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Bundesgesetzgeber und die Landesgesetzgeber daher auf, durch aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau den Datenschutz in der länderübergreifenden Forschung zu stärken. Hierfür hat sie Eckpunkte erarbeitet. Im Einzelnen:

In vielen Ländern enthalten verschiedene Landesgesetze, die beispielsweise die Datenverarbeitungen durch Krankenhäuser und Behörden des öffentlichen Gesundheitsdienstes betreffen, konkrete Befugnisse der jeweiligen Stellen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken, die den allgemeinen Vorgaben vorgehen. Diese gesetzlichen Regelungen stellen unterschiedliche datenschutzrechtliche Anforderungen. Bei länderübergreifender Forschung müssen von den Verantwortlichen die jeweils für sie geltenden Gesetze angewandt werden. Unterschiede bestehen insbesondere in Bezug auf die Zulässigkeit der Datenverarbeitung (gesetzliche Grundlage oder Einwilligung mit jeweils unterschiedlichen Anforderungen), die Definition von Schutzbereichen (u. a. Patientinnen und Patienten, Angehörige) und zulässige Zwecke der Verarbeitung. Die rechtliche Bewertung und Umsetzung der jeweils geltenden Rechtsgrundlage führte in der Vergangenheit zu einem gesteigerten Beratungsbedarf und zu Unsicherheiten bei den Forschenden und Rechtsanwendern. Auch ergeben sich aus unterschiedlichen Regelungen Herausforderungen

für eine transparente und verständliche Informationserteilung nach Artikel 13 und 14 der Datenschutz-Grundverordnung (DSGVO).

Das Bundesgesundheitsministerium hat mit dem Gesetzentwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorgeschlagen. Geplant ist insoweit eine Rechtsgrundlage für die „Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken“ durch eine Gesundheitseinrichtung für die bei ihr rechtmäßig gespeicherten Daten.

Das Verhältnis dieser geplanten Neuregelungen zu den Landeskrankenhausgesetzen ist jedoch unklar. Mit der Gesetzgebungskompetenz der Länder für den Bereich der Krankenhäuser hat sich der Gesetzentwurf nicht auseinandergesetzt. Daher bestehen erhebliche Zweifel, dass mit diesem Gesetzentwurf eine rechtssichere und tragfähige Neuregelung erreicht wird, die die länderübergreifende Forschung erleichtert.

Die DSK hat in ihrer Stellungnahme zum GDNG-Gesetzentwurf vom 14.08.2023 hierauf hingewiesen und weiteren Korrekturbedarf aufgezeigt.[1]

In dieser Stellungnahme und in der „Petersberger Erklärung“ vom 24.11.2022 hat die DSK wichtige Hinweise für gesetzliche Neuregelungen formuliert.[2] Sie beschreiben wesentliche Anforderungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, insbesondere zu den Rechtsgrundlagen und den besonderen Einwirkungsmöglichkeiten für betroffene Personen.

Um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren, sind konkrete Garantien und Maßnahmen gesetzlich festzulegen. Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden.[3] Abhängig von den jeweils verarbeiteten Datenarten – z. B. personenbezogenen Daten (Art. 4 Nr. 1 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder genetische Daten

[1] Die Stellungnahme der DSK vom 14.08.2023 zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) ist abrufbar unter https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.

[2] Die Entschließung der DSK vom 24.11.2022 (Petersberger Erklärung) ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.

[3] Vgl. Empfehlung Nr. 2 der Petersberger Erklärung.

(Art. 4 Nr. 13 DSGVO) – bedarf es eines angemessenen Schutz- und Vertrauensniveaus und spezifischer Regelungen für die Verarbeitungen in den jeweiligen Bereichen der Forschung.

Für besondere Forschungsgegenstände, bei denen eine ausreichende Anonymisierung nicht immer gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen sicherzustellen, z. B. durch zusätzliche technische und organisatorische Maßnahmen.

Darüber hinaus sind die Regelungen des Art. 9 Abs. 2 lit. j i. V. m. Art. 89 Abs. 1 DSGVO zu beachten. Insbesondere müssen im Gesetz selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden. Diese Festlegung der spezifischen Anforderungen darf nicht an die Verantwortlichen delegiert werden. Die Umsetzung darf sich auch nicht in generalklauselartigen oder in solchen Regelungen erschöpfen, die die DSGVO ohnehin für die Datenverarbeitung vorsieht, wie etwa die Betroffenenrechte nach Art. 15 ff. DSGVO oder Maßnahmen nach Art. 32 DSGVO. Stattdessen müssen konkrete Maßnahmen benannt werden.

Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (z. B. Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Art. 15 ff. DSGVO hinausgehender Betroffenenrechte (z. B. spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (z. B. bei einem Widerspruchsrecht),
- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,

- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,
- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

Diese Aufzählung ist nicht abschließend. Es ist die Aufgabe des Gesetzgebers, die Risiken zu erkennen, die mit einer Verarbeitung von Gesundheitsdaten verbunden sind, sie zu benennen und ihnen angemessene Schutzmaßnahmen für die Rechte und Interessen der betroffenen Personen gegenüberzustellen.

Die DSK weist darauf hin, dass medizinische personenbezogene Daten in bestimmten Fallkonstellationen dem absoluten Schutz des Kernbereichs privater Lebensgestaltung unterliegen.

Die Verarbeitung solcher menschenwürderelevanter Daten kann selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden.

Schließlich ist eine uneingeschränkte Datenschutzaufsicht in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten zu garantieren. Diese bietet Schutz für die betroffenen Personen. Etwaig bestehende Einschränkungen der Befugnisse der Datenschutzaufsichtsbehörden hinsichtlich der Verhängung von Bußgeldern und des Vollzugs gegenüber öffentlichen Stellen sind zumindest im Anwendungsbereich entsprechender Regelungen aufzuheben.

Die DSK setzt sich für die Schaffung eines hohen Datenschutzniveaus in der medizinischen Forschung durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein. Sie appelliert an die Gesetzgeber des Bundes und der Länder, durch klarstellende Regelungen einen wirksamen Kernbereichsschutz sicherzustellen.

Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.