„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

11/2023
November 2023

Compliance in der Wissenschaft. Probleme oder dornige Chancen?

Setzen Complianceanforderungen die Wissenschaftsfreiheit unter Druck oder schützen sie diese erst?

von Ole-Christian Tech

Hochschulen und Forschungseinrichtungen sind Adressaten zahlreicher Complianceanforderungen. Oft handelt es sich um Campusanlagen, die allein durch ihre Größe ganze Stadtteile prägen, oder deren Gebäude sich sogar auf verschiedene Städte verteilen. Sie haben nicht selten mehrere 10.000 Mitglieder und tausende Mitarbeiter und sind manchmal sogar der größte Arbeitgeber der Stadt. Kein Wunder also, dass sie ebenso Complianceanforderungen erfüllen müssen wie andere Unternehmen dieser Größe. Oder?

I. Was ist Compliance?

Compliance bezeichnet wörtlich die Regeltreue von Unternehmen. Sowohl präventiv als auch repressiv können dabei verschiedene Maßnahmen ergriffen werden, um die Vorgaben zu erfüllen.

Und genau hier besteht auf den ersten Blick ein gewisser Widerspruch: Die Wissenschaftsfreiheit ist verfassungsrechtlich in Art. 5 Abs. 3 S. 1 Grundgesetz (GG) garantiert und in der Rechtsprechung gerade von einer hohen Autonomie geprägt. Andererseits handelt es sich bei Hochschulen und Forschungseinrichtungen in der Regel auch um öffentliche Einrichtungen, die einer gesellschaftlichen Verantwortung und einer Erwartung an die Rechtstreue verbunden sind.

Im Rahmen der Compliance an Hochschulen kann grob zwischen drei Arten von Regeln unterschieden werden, die externen Vorschriften, die internen Vorschriften und übergreifende ethische Normen und Werte. Die folgenden Seiten sollen einen kurzen Überblick bieten und für die Vielfältigkeit von Compliance Themen sensibilisieren, sie verfolgen aber ausdrücklich keinen Anspruch auf Vollständigkeit.

1. Externe Vorschriften (Gesetze und Verordnungen)

Dass Gesetze und Verordnungen nicht nur für private Unternehmen, sondern umso mehr und selbstverständlich auch für Hochschulen als Körperschaften des öffentlichen Rechts gelten, folgt schon aus Art. 20 Abs. 3 GG. Sie müssen, neben den auch für Arbeitgeber und Unternehmen geltenden Vorschriften, spezielle Vorgaben erfüllen.

(a) Arbeits- und Umweltschutz

Im Bereich des Arbeitsschutzes tritt die Hochschule als Arbeitgeber auf und ist auf den Arbeitsschutz ihrer Arbeitnehmer verpflichtet. Dies umfasst unter anderem die Vorschriften des Arbeitsschutzgesetzes, Arbeitssicherheitsgesetzes und des Sozialgesetzbuches SGB VII. Daher muss der Arbeitgeber den Arbeitnehmer vor Gefahren aus der Tätigkeit schützen und dadurch Arbeitsunfälle vermeiden. Dabei gelten selbstverständlich die Vorschriften zum Schutz bestimmter Gruppen (Mutterschutz, Jugendschutz, Schutz von Schwerbehinderten). Es kann bei Unfällen zudem eine strafrechtliche Verantwortlichkeit in Betracht kommen.

Daneben muss jedoch auch die Einhaltung von Arbeits- und Urlaubszeiten beachtet werden. Unter anderem hat das Bundesarbeitsgericht (BAG) vergangenes Jahr entschieden, dass die Frist zur Verjährung von Urlaubsansprüchen erst dann zu laufen beginnt, wenn der Arbeitgeber den Arbeitnehmer über die verbleibenden Urlaubstage unterrichtet und über die potenzielle Verjährung informiert.[1] Ebenfalls vergangenes Jahr beschäftigte sich das BAG mit der Pflicht zur Arbeitszeiterfassung durch den Arbeitgeber.[2] Demnach besteht ohne eine konkretisierende gesetzliche Regelung die Pflicht zur Arbeitszeiterfassung, welche bereits aus § 3 Arbeitsschutzgesetz (und nicht aus dem Arbeitszeitgesetz) folgt. Dieser verpflichtet den Arbeitgeber generell auf den Schutz der Arbeitnehmer, woraus das BAG die konkrete Pflicht zur Führung eines Arbeitszeiterfassungssystems ableitet.

Im Hinblick auf Compliance im Umweltrecht gibt es zunächst zahlreiche öffentlich-rechtliche Vorschriften, die es zu beachten gilt. Demnach müssen die Vorgaben zum Immissions-, Wasser-, Boden, Natur-, Tier- und Pflanzenschutz eingehalten werden. Darüber hinaus gilt, mit dem Ziel der Nachhaltigkeit, auch die Pflicht zur ordnungsgemäßen Vermeidung, Wiederverwertung und Entsorgung von Abfall nach dem Kreislaufwirtschaftsgesetz. Zudem gibt es sogar strafrechtliche Vorgaben im sog. Umweltstrafrecht in §§ 324 ff. Strafgesetzbuch (StGB).

(b) Sozialversicherungsrecht

Im Sozialversicherungsrecht stellt sich insbesondere die Frage der Scheinselbstständigkeit. Diese liegt vor, wenn ein im Werk- oder Dienstvertrag als selbstständig bezeichneter Auftragnehmer faktisch abhängig beschäftigt ist, etwa weil er ausschließlich für einen Auftraggeber tätig ist, zur Nutzung bestimmter Hard- oder Software verpflichtet ist oder nur vor Ort tätig sein darf. Dieses Risiko besteht etwa bei externem Korrekturpersonal für Klausuren und gegebenenfalls auch bei Dozenten, die für bestimmte Veranstaltungen herangezogen werden.

(c) Datenschutz

Die Daten der im öffentlichen Dienst Beschäftigten dürfen nicht in unbegrenztem Maße veröffentlicht werden.[3] Dabei muss der Zweck der Veröffentlichung betrachtet werden und anhand dessen evaluiert werden, ob eine Veröffentlichung zur Zweckerreichung notwendig ist. Es ist insbesondere zu berücksichtigen, wie schwer die Veröffentlichung der Information in das Privatleben des Beschäftigten eingreift.

Beschäftigte des öffentlichen Dienstes sind in der Regel bereits per Tarifvertrag oder per Gesetz zur Wahrung der dienstlichen Verschwiegenheit verpflichtet.[4]

Als Arbeitgeber treffen Hochschulen auch Vorgaben des Beschäftigtendatenschutzes.[5] Dabei ist aufgrund einer Entscheidung des EuGHs zu berücksichtigen, dass aufgrund der naheliegenden Unionsrechtswidrigkeit der Erlaubnisnorm des § 26 Bundesdatenschutzgesetz auch im Beschäftigungsverhältnis auf die allgemeinen Erlaubnisnormen des Art. 6 Abs. 1 DSGVO zurückgegriffen werden sollte.[6] Durch die Entscheidung wurde die geltende Rechtslage zwar nicht verändert, jedoch kann eine Nutzung der Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO für Gewissheit über die Rechtmäßigkeit der Verarbeitung sorgen. Zudem ist eine Neuregelung durch den Gesetzgeber zu erwarten.

Außerdem ist nach einer EuGH-Entscheidung aus dem Jahr 2023 [7] unklar, ob Personalratsmitglieder zugleich Datenschutzbeauftragte einer Hochschule sein dürfen. Offen ist, ob der Personalrat im öffentlichen Dienst mit dem Betriebsrat in privaten Unternehmen vergleichbar ist und daher ein Interessenkonflikt wie im oben genannten EuGH Urteil vorliegen könnte. Grundsätzlich besteht ein weitgehender Unterschied: Das Recht der Betriebsräte wird durch Bundesrecht (BetrVG) geregelt, wohingegen das Recht der Personalräte im Personalvertretungsgesetz der Länder und des Bundes geregelt ist. Daher unterscheiden sich auch die konkreten

1 BAG, Urteil vom 20. Dezember 2022, Az. 9 AZR 266/20.

2 Siehe dazu Voget, Die letzte Stunde hat geschlagen!, DFN-Infobrief Recht 05/2023; John, Tick Tack – Finger ab?, DFN-Infobrief Recht 02/2020.

3 Hierzu auch Palenberg, Nicht für die Öffentlichkeit bestimmt, DFN-Infobrief Recht 09/2022.

4 So etwa für Beschäftigte im öffentlichen Dienst § Abs. 2 TV-L sowie für Beamte nach § 37 BeamtStG.

5 Siehe hierzu Müller, Beschäftigtendatenschutz von A bis Z, DFN-Infobrief Recht 06/23; Voget, Work Data Balance: Der Beschäftigtendatenschutz, DFN-Infobrief Recht 11/22.

6 John, Kurzbeitrag: Alles neu macht der EuGH, DFN-Infobrief Recht 06/23.

7 Tech, Betriebsratsmitglieder als Datenschutzbeauftragte? „Nein!? Doch! Ohh!“, DFN-Infobrief 09/23.

Befugnisse, aus denen ein Interessenkonflikt erwachsen könnte, von Land zu Land.

(d) Exportkontrolle

Hochschulen haben, genau wie private Wirtschaftsunternehmen, selbst auf den ersten Blick exotische Gesetze, wie die Vorschriften der Exportkontrolle nach dem Außenwirtschaftsgesetz, zu beachten.[8] Auch das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), das die zuständige Kontrollbehörde ist, weist darauf hin, dass es für die Exportkontrolle relevante Bereiche in Hochschulen gibt.[9] Besonders im Fokus sind derzeit sog. dual use-Güter, also solche Güter, die sowohl für zivile als auch militärische Zwecke genutzt werden können. Daher sollten Hochschulen in der Auswahl ihrer ausländischen Kooperationspartner wachsam sein und im Zweifelsfall eine Anfrage beim BAFA stellen.

(e) Informationssicherheit

In Zeiten stärkerer Digitalisierung und einer steigenden Anzahl an Cyberangriffen wird Informationssicherheit zunehmend wichtiger. Im Jahr 2023 ist die NIS 2-Richtlinie in Kraft getreten, die Deutschland zukünftig umsetzen muss.[10] Dabei soll unter anderem der Anwendungsbereich vereinheitlicht werden, da dieser in den Mitgliedsstaaten bei Geltung der NIS-Richtlinie sehr unterschiedlich definiert wurde. Die Anwendung auf Hochschulen selbst bleibt davon abhängig, ob der Gesetzgeber diese einbezieht. Bereits jetzt sind Unikliniken durch das IT-Sicherheitsgesetz als kritische Infrastruktur umfasst.

Es wird allerdings durch die NIS 2-Richtlinie eine Neuerung geben: Die Forschung muss als Teil einer nationalen Cybersicherheitsstrategie ebenfalls umfasst sein. Wie die konkreten Auswirkungen dieser Regelung aussehen werden, hängt jedoch ebenfalls von der nationalen Umsetzung ab.

(f) Gleichstellung (AGG)

Als Arbeitgeber müssen Hochschulen, wie sonstige Arbeitgeber, gegenüber ihren Arbeitnehmern die Vorgaben des AGG einhalten (§ 2 Abs. 1 Nr. 1 AGG). Darüber hinaus müssen jedoch auch gegenüber den Studentinnen und Studenten die Vorgaben des AGG eingehalten werden (§ 2 Abs. 1 Nr. 3, 7 AGG). Es darf demnach keine ungerechtfertigte Diskriminierung aufgrund eines durch das Gesetz geschützten Merkmals vorliegen, etwa bei der Bewertung von Prüfungsergebnissen oder der Studienplatzvergabe.

(g) Strafrecht

Selbst strafrechtliche Risiken können im universitären Umfeld auftreten. Neben den allgemeinen strafrechtlichen Fragestellungen, stellen sich hierbei auch exotische Fragestellungen, wie beim Test der informationstechnischen Systeme durch „gutwillige“ Hacks (sog. White-Hat-Hacking)[11].

Auch bei der Annahme von Subventionen treten Strafbarkeitsrisiken auf, wenn etwa falsche Angaben gemacht werden. Für die Verwirklichung des Straftatbestandes des Subventionsbetrugs (§ 264a StGB) ist es dabei nicht erforderlich, dass ein Schaden eintritt. Daher ist bei der Dokumentation von Kostenpunkten eines Forschungsprojekts sorgfältig zu arbeiten.

Bei drittmittelfinanzierter Forschung spielt das Strafrecht wieder eine wichtige Rolle: Tatbestandlich handelt es sich hierbei oftmals um einen Fall der Vorteilsannahme nach § 331 Abs. 1 StGB. Der Bundesgerichtshof (BGH) hat jedoch bereits 2002 entschieden, dass diese Arten der Kooperation mit der Privatwirtschaft dann von dem Straftatbestand ausgenommen sind, wenn die Hochschulen und Forschungseinrichtungen die Vorgaben des jeweiligen Hochschulrechts einhalten,[12] welche in vielen Bundesländern durch Verwaltungsvorschriften konkretisiert werden.[13]

---

8 https://www.bundestag.de/resource/blob/585612/5c5c05f6ada0c1c86830cba0d8601d6d/WD-5-157-18-pdf-data.pdf.

9 https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_technologietransfer.html S. 10.

10 Dazu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 04/23.

11 Hierzu Voget, Der Zweck heiligt die Mittel?, DFN-Infobrief Recht 07/23.

12 BGH Urteil vom 23.Mai 2002, Az. 1 StR 372/01.

13 Statt aller exemplarisch Baden-Württemberg: https://www.landesrecht-bw.de/jportal/?quelle=jlink&query=VVBW-WK-20161221-SF&psml=bsbawueprod.psml&max=true&aiz=true.

(h) Ausschreibungen

Bei Ausschreibungen sind Hochschulen auch an die Grundsätze der Vergabe nach § 97 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) gebunden, da sie unter § 99 GWB fallen. Dies verpflichtet sie unter anderem zu transparenten Vergabeverfahren und Gleichbehandlung aller Teilnehmer Dieses Verfahren beinhaltet aber auch detaillierte Vorgaben, welche verstärkt berücksichtigt werden müssen.

Zudem gibt es landesrechtlich weitere Voraussetzungen. In NRW gilt beispielsweise das Tariftreue- und Vergabegesetz NRW, nach dem nur Unternehmen den Zuschlag erhalten, die tarifgebunden sind. Außerdem gibt es eine Vergaberichtlinie für Hochschulen im Rahmen des § 8 Hochschulwirtschaftsführungsverordnung NRW.

2. Interne Regeln und Vereinbarungen

Im Bereich der nicht zwingenden Regeln gibt es verschiedene Bereiche, die einen Einfluss haben. Unter anderem sind dies die internen Regeln und Vereinbarungen wie die Universitätsverfassung, der Hochschulentwicklungsplan oder Struktur- und Entwicklungspläne der Fachbereiche. Beispiele hierfür sind etwa sogenannte Code of Conducts, in denen sich Einrichtungen selbst zu Zielen wie Diversität und Gleichstellung gegen Mobbing und Diskriminierung u.a. verpflichten.[14]

Zudem gibt es auch interne Vorschriften für Wissenschaftler wie beispielsweise eine Ordnung zur Sicherung guter Wissenschaftlicher Praxis.

Darüber hinaus sind jedoch auch externe Papiere wie beispielsweise ein Vorschlag des Bundesamts für Sicherheit in der Informationstechnik zur Cybersicherheit an Hochschulen[15] zu nennen.

3. Ethische Normen und Werte

Auch im nicht-rechtlichen Bereich gibt es Kodizes, Werte und Normen, denen sich die Hochschulen verpflichten. Dabei ist insbesondere der Kodex für gute wissenschaftliche Praxis zu nennen. Unter anderem ist für die Nutzung von Bundes- oder DFG-Mitteln (also der deutschen Forschungsgemeinschaft) erforderlich, dass auch organisatorische Strukturen vorgehalten werden, um die Einhaltung dieses Kodex zu gewährleisten.[16] Eine reine Versicherung der guten wissenschaftlichen Praxis genügt somit nicht.

Zuletzt geben sich viele Universitäten selbst sog. Mission Statements, die beispielsweise auf Aspekte wie Nachhaltigkeit oder Diversität verpflichten.

(a) Ethik in der medizinischen Forschung

Bei der Durchführung medizinischer Forschung sind aufgrund der Risiken für die Studienteilnehmer und der erheblichen Gefahr von Imageschäden, die der Akzeptanz für Gesundheitsforschung insgesamt schaden könnten, bestimmte Standards anzulegen.[17] Seit 1964 bildet die Deklaration von Helsinki[18] die ethische Grundlage einer medizinischen Forschung am Menschen. Insbesondere muss der Arzt bei Durchführung der Studie im besten Interesse des Patienten handeln sowie dessen Wohlergehen und Rechte fördern. Diese werden noch durch die „Gute Klinische Praxis“[19] konkretisiert.

(b) Tierschutz

Der Tierschutz spielt bei der Compliance von Hochschulen vor allem eine Rolle im Rahmen von Tierversuchen. Rechtliche Vorgaben für diese ergeben sich durch das Tierschutzgesetz (TierSchG) und die Tierschutz-Versuchstierverordnung (TierSchVersV). Als Grundsatz gilt dabei stets, dass einem Tier nicht ohne vernünftigen Grund Schmerzen, Leiden oder Schaden zugefügt werden

14 Für die WWU Münster z.B.: https://www.uni-muenster.de/profil/compliance/code_of_conduct.html.

15 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Hochschulen.pdf?__blob=publicationFile&v=2.

16 https://www.dfg.de/download/pdf/foerderung/rechtliche_rahmenbedingungen/gute_wissenschaftliche_praxis/kodex_gwp.pdf.

17 Siehe dazu die Übersicht des Arbeitskreises Medizinischer Ethik Kommissionen: https://www.akek.de/forschungsethische-prinzpien/.

18 https://www.bundesaerztekammer.de/fileadmin/user_upload/_old-files/downloads/pdf-Ordner/International/Deklaration_von_Helsinki_2013_20190905.pdf.

19 https://projekttraeger.dlr.de/media/gesundheit/GF/Grundsaetze_Verantwortlichkeiten_Klinische_Studien.pdf.

darf (§ 1 TierSchG). Tierversuche dürfen daher nur zu bestimmten Zwecken durchgeführt werden (§ 7a TierSchG). Auch bedarf es in der durchführenden Einrichtung eines Tierschutzbeauftragten sowie eines Tierschutzausschusses. Zudem müssen nach der TierSchVersV bestimmte Angaben zu den im Versuch genutzten Tieren angegeben werden.

II. Fazit: Compliance ein Thema auch für Forschungseinrichtungen und Hochschulen

Im Ergebnis zeigt sich, dass Compliance nicht nur ein Thema für multinationale Konzerne ist, sondern auch und gerade Hochschulen und Forschungseinrichtungen beschäftigt. Die Vielfältigkeit an Regeln erscheint auf den ersten Blick zwar als Hemmnis für den freien Forschungsbetrieb, ermöglicht aber bei genauer Betrachtung erst eine freie Wissenschaft, indem Haftungsrisiken vermieden, Akzeptanz und wissenschaftlicher Wettbewerb und Qualität gewahrt werden.

In einer sich stetig weiterentwickelnden und zunehmend digitalisierten Forschungswelt werden außerdem künftig die zahlreichen neuen Anforderungen aus der europäischen Digitalgesetzgebung eine übergeordnete Rolle im Compliance Bereich spielen. Vom Digital Services Act, über den AI Act, den Data Act und den Data Governance Act bis hin zu den sektorspezifischen Datenräumen wie dem European Health Data Space werden hier zahlreiche neue Regelungen auf Hochschulen und Forschungseinrichtungen zukommen.[20]

20 Einleitend etwa Rennert, Brüssel reguliert das schon, EU-Institutionen einigen sich final auf DMA und DSA sowie Tech Datenstaat oder Datensalat?, Eine Übersicht über die aktuelle datenrechtliche Regulierungslandschaft in der EU.

Wir sind auch verantwortlich, für das, was wir nicht tun

EGMR zur Verantwortlichkeit des Inhabers einer Facebook-Seite für fremde Hasskommentare

von Johannes Müller

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat sich in seiner Entscheidung (Az. 45581/15) damit beschäftigt, ob der Inhaber einer Facebook-Seite für Hasskommentare anderer Nutzer auf der Seite zur Verantwortung gezogen werden kann. In seiner Abwägung kam der EGMR zu dem Ergebnis, dass die Pflicht zur Kontrolle der eigenen Seite zur Verhinderung von Hassrede und Gewaltaufrufen im Einzelfall schwerer gewichtet werden kann als die individuelle Meinungsfreiheit.

I. Hasskommentare in sozialen Medien

Das Internet ist zur essentiellen Bühne des öffentlichen Meinungsaustausches geworden. Insbesondere soziale Netzwerke bieten die Möglichkeit, eigene Meinungen mit einer Vielzahl anderer Personen zu teilen und mit diesen zu interagieren. Auch ein großer Anteil des politischen Meinungsaustausches findet im Internet statt. Hierbei werden soziale Nerzwerke auch häufig zum Tatort von Straftaten. Die scheinbare Anonymität des Internets scheint insbesondere die Hemmschwelle für das Begehen von Delikten gegen die Ehre zu senken.[1] So wurden etwa in Deutschland im Jahr 2022 17.7576 Beleidigungen registriert, die über das Tatmittel Internet begangen wurden.[2] Die Dunkelziffer scheint jedoch deutlich höher zu sein, da nur etwa 1 Prozent der persönlichen Beleidigungen im Internet zur Anzeige gebracht wird.[3]

Auch Wissenschaftler werden immer häufiger Opfer von Angriffen im Internet aufgrund ihrer Wissenschaftskommunikation. Insbesondere während der Corona-Pandemie waren öffentlich tätige Wissenschaftler Hass und Hetze im Internet ausgesetzt. Aber auch in anderen gesellschaftlich kontrovers diskutierten Forschungsgebieten besteht ein erhöhtes Risiko, als Wissenschaftler im Internet zum Opfer von Straftaten zu werden. Zur Unterstützung von Wissenschaftlern im Umgang mit Anfeindungen ist jüngst die Scicomm-Support Plattform[4] ins Leben gerufen worden. Auf der Plattform werden Informationen, Ressourcen und Trainingsangebote zum Umgang mit unwissenschaftlicher Kritik und Anfeindungen im Internet zur Verfügung gestellt. Darüber hinaus bietet Scicomm-Support Betroffenen auch persönliche kostenlose Beratung an.

---

1 Vgl. zu Hassreden im Internet, Schaller, Machtwort gegen Hass und Hetze, DFN-Infobrief Recht 04/2022; Schaller, Kurzbeitrag: Künast die Dritte, DFN-Infobrief Recht 06/2022.

2 Bundesministerium des Innern und für Heimat, Polizeiliche Kriminalstatistik 2022. Ausgewählte Zahlen im Überblick, 23, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2022.pdf?__blob=publicationFile&v=4#%5B%7B%22num%22%3A40%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitH%22%7D%2C797%5D (zuletzt abgerufen am 22.09.2023).

3 Bundesministerium des Innern und für Heimat, Polizeiliche Kriminalstatistik 2022. Ausgewählte Zahlen im Überblick, 23, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/pks-2022.pdf?__blob=publicationFile&v=4#%5B%7B%22num%22%3A40%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitH%22%7D%2C797%5D (zuletzt abgerufen am 22.09.2023.).

4 Auffindbar unter https://scicomm-support.de (zuletzt abgerufen am 22.09.2023).

II. Die Verurteilung eines französischen Kommunalpolitikers für fremde Kommentare auf seiner Facebook-Seite

Der EGMR hatte zu entscheiden, ob das Strafurteil eines französischen Gerichts mit der in Art. 10 der Europäischen Menschenrechtskonvention (EMRK) garantierten Freiheit der Meinungsäußerung vereinbar ist. Der Beschwerdeführer war Gemeinderatsmitglied in Frankreich und kandidierte für die Partei Front National (heute Rassemblement National) als Bürgermeister und als Vorsitzender der regionalen parlamentarischen Vertretung. Er platzierte auf seiner Facebook-Seite eine Bemerkung gegen seinen politischen Gegenkandidaten. Daraufhin gaben zwei weitere Nutzer Kommentare unter dem Post ab, in denen sie sich stark herabsetzend über muslimische Migranten äußerten. Hierfür wurden die Verfasser und auch der Beschwerdeführer vom Landgericht (LG) Nimes wegen Aufstachelung zum Hass oder Gewalt gegen eine Personengruppe wegen ihrer Herkunft oder Zugehörigkeit zu einer Ethnie, Nation, Rasse oder Religion zu einer Geldstrafe verurteilt. Bemerkenswert war hieran vor allem die Verurteilung des Beschwerdeführers, der die strafbaren Kommentare nicht selbst abgegeben hat. Ihm wurde in der Verurteilung vorgeworfen, dass er die strafbaren Inhalte nach ihrer Kenntnisnahme nicht schnell entfernt habe. Hiergegen wehrte sich der Kommunalpolitiker vor dem EGMR.

III. Das Urteil des EGMR

Die große Kammer des EGMR kam zu dem Ergebnis, dass der Beschwerdeführer durch das Strafurteil nicht in seinem Recht auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK verletzt werde.

Zunächst qualifizierte der EGMR, ebenso wie die französischen Gerichte, die streitgegenständlichen Äußerungen als Hassrede. Das Gericht betont, dass das Recht auf freie Meinungsäußerung, insbesondere für Politiker, ein besonders schützenswertes Gut sei. Dennoch gelte der Schutz nicht uneingeschränkt, da es in einer demokratischen und pluralistischen Gesellschaft erforderlich sein könne, Äußerungen zu bestrafen oder zu verhindern, die auf der Grundlage von Intoleranz Hass propagieren. Insbesondere Politiker hätten auch die besondere Verantwortung, Reden zu vermeiden, durch die Intoleranz gefördert werde. Zwar seien im Wahlkampf lebhafte Äußerungen üblicher, diese erhielten im Wahlkampf aber auch eine stärkere Wirkung. Auf Grundlage der Rechtsprechung des EGMR müsse geprüft werden, ob Äußerungen in einem gespannten politischen oder sozialen Umfeld als direkter oder indirekter Aufruf zu Gewalt oder Rechtfertigung von Gewalt, Hass oder Intoleranz verstanden werden könne. Bei Äußerungen, die im Internet getätigt würden, müsse zudem beachten werden, dass sie auf der ganzen Welt verbreitet werden würden und zum Teil lange online verfügbar seien. Im konkreten Fall nahm der EGMR rechtswidrige Hassrede durch die Äußerungen an, da durch diese Muslime mit beleidigenden und verletzenden Ausdrücken in Verbindung gebracht werden. Insbesondere beabsichtigten die Ausdrücke, Muslime mit Kriminalität zu assoziieren. Diese Wirkung werde dadurch verstärkt, dass die Äußerungen im Wahlkampf getroffen wurden und auf Spannungen innerhalb der Bevölkerung treffen würden.

Der EGMR setzte sich auch mit der Frage auseinander, ob es mit der Meinungsfreiheit vereinbar wäre, dass eine Person für Kommentare Dritter auf einem Profil strafrechtlich zur Verantwortung gezogen werden kann. Er stellte fest, dass einen Seitenbetreiber nicht die gleichen Pflichten träfen wie etwa ein großes Nachrichtenportal. Dennoch sei er nicht von aller Verantwortung für die Kommentare auf seiner Seite befreit.

Der EGMR stellte die möglichen Folgen eines Abwägungsergebnisses gegenüber: Eine Verurteilung für fremde Kommentare könnte eine abschreckende Wirkung auf die Meinungsausübung anderer Nutzer, auch auf anderen Diskussionsplattformen, zur Folge haben. Zudem sei die Freiheit der Meinungsäußerung gerade für gewählte Volksvertreter, politische Parteien und ihre Mitglieder besonders wertvoll. Dem stehe aber ein erhöhtes Risiko gegenüber, dass es ohne Kontrolle über die eigene Facebook-Seite zu einer Zunahme an Hassreden und Gewaltaufrufen auf den einschlägigen sozialen Netzwerken kommen könnte. Mit dem Nutzen der Facebook-Seite für politische Tätigkeiten gehe eine besondere Verantwortung für die auf der Seite öffentlich geführte Debatte einher. Aufgrund der erhöhten Bekanntheit und Repräsentativität bestehe für Politiker eine Pflicht zur größeren Wachsamkeit hinsichtlich rechtswidriger Äußerungen. Eine Privatperson habe hingegen geringere Pflichten für die eigene Seite. Im gegebenen Fall sei dem Beschwerdeführer auch bewusst gewesen, dass auf seiner Seite problematische Kommentare veröffentlicht werden. Somit sei auch die Verurteilung für fremde Kommentare mit dem Recht auf freie Meinungsäußerung vereinbar.

IV. Die Relevanz von Urteilen des EGMR

Der EGMR wacht über die Einhaltung der Europäischen Menschenrechtskonvention (EMRK). Die EMRK ist kein EU-Recht, ebenso handelt es sich beim EGMR nicht um ein Organ der EU. Stattdessen ist die EMRK ein völkerrechtlicher Vertrag, in dem sich die Mitglieder des Europarats durch die Unterzeichnung zur Einhaltung der in der EMRK garantierten Menschenrechte verpflichten. Als bloßer völkerrechtlicher Vertrag kommt der EMRK grundsätzlich nur die Wirkung eines einfachen Bundesgesetzes zu. Allerdings steht das deutsche Grundgesetz unter dem Grundsatz der völkerrechtsfreundlichen Auslegung. Dies bedeutet, dass die Normen des Grundgesetzes derart ausgelegt werden sollen, dass sie nicht im Widerspruch zu den völkerrechtlichen Verpflichtungen von Deutschland stehen. Daher sind die Grundrechte des Grundgesetzes im Einklang mit der Rechtsprechung des EGMR zur EMRK auszulegen. Bei der Auslegung der Meinungsfreiheit gemäß Art. 5 Abs. 1 S. 1 Var. 1 GG ist also die Rechtsprechung des EGMR zu Art. 10 EMRK zu beachten.

V. Die Bedeutung des Urteils für die deutsche Praxis

Die verschiedenen Inhalte des Urteils lassen sich unterschiedlich stark auf die deutsche Rechtslage übertragen. Besondere Relevanz haben die Ausführungen zur Meinungsfreiheit innerhalb eines politischen Wahlkampfes. Sie betonen, dass auch für Politiker die Meinungsfreiheit nicht uneingeschränkt gilt und Äußerungen, die gezielt bestimmte Personengruppen diffamieren und zum Hass aufstacheln, nicht von der Meinungsfreiheit geschützt sein müssen.

Mit höherem Aufwand ist die Übertragung der Bewertung der strafrechtlichen Verantwortlichkeit für fremde Hasskommentare verbunden. Das Urteil kommt zu dem Ergebnis, dass die strafrechtliche Verurteilung des Seiteninhabers nicht gegen sein Recht auf freie Meinungsäußerung verstößt. Anders als in Frankreich besteht in Deutschland jedoch kein Tatbestand, auf dessen Grundlage der Inhaber einer Facebook-Seite für fremde Kommentare strafrechtlich zur Verantwortung gezogen werden kann. In der Theorie lässt sich eine Strafbarkeit evtl. über Umwege begründen. Allerdings ist eine solche Strafbarkeit nach geltendem Recht hochstrittig, tatsächliche Verurteilungen sind nicht bekannt.

Nach deutscher Rechtslage kann vor allem der Plattformbetreiber sanktioniert werden. Soziale Netzwerke, die fremde Inhalte auf ihren Plattformen speichern, können gemäß § 10 Telemediengesetz (TMG) etwa zivilrechtlich zur Verantwortung gezogen werden, wenn sie Kenntnis von gespeicherten rechtswidrigen Inhalten haben und diese nicht unverzügliche nach Kenntnisnahme entfernen. Das Netzwerkdurchsuchungsgesetz (NetzDG) sieht zudem Bußgelder vor, sofern kommerzielle Anbieter von sozialen Netzwerken kein effektives Verfahren zur Löschung von rechtswidrigen Inhalten bereithalten. Ab Februar 2024 finden primär die Regelungen des Digital Services Act (DSA) Anwendung, der ebenso die Verantwortlichkeit für fremde gespeicherte Inhalte normiert und auch die Pflichten von Betreibern sozialer Netzwerke regelt. Im Rahmen dieser Regelungen können die Wertungen des Urteils des EGMRs auch zu beachten sein, das die Grenzen der Meinungsfreiheit im Internet betont und auch eine erhöhte Verantwortlichkeit für fremde Inhalte vorsieht.

VI. Relevanz für wissenschaftliche Einrichtungen

Die aufgezeigten Wertungen sind auch für wissenschaftliche Einrichtungen relevant. Bereits nach geltendem Recht sind sie dazu verpflichtet, rechtswidrige Inhalte, die auf ihren Servern gespeichert sind zu entfernen, sobald sie Kenntnis von der Rechtswidrigkeit erhalten. Das Urteil des EGMR betont diese Verantwortlichkeit für fremde Inhalte besonders und zeigt auf, dass die Meinungsfreiheit im Internet nicht unbegrenzt gilt und unterschiedlichen Instanzen Verantwortung zukommen kann, Hassrede im Internet zu unterbinden.

Im Hamsterrad gefangen

Regelungen zur Vorratsdatenspeicherung erneut vor dem BVerwG und EuGH

Von Klaus Palenberg

Die höchsten Gerichte haben sich wieder mit der sogenannten Vorratsdatenspeicherung befasst. Das Bundesverwaltungsgericht (BVerwG, Urteile vom 14. August 2023, Az. 6 C 6/22 und 6 C 7/22)[1] urteilte dabei, dass die gesetzliche Verpflichtung von Telekommunikationsanbietern zur Speicherung von Verkehrsdaten nicht mehr anwendbar ist. Der Europäische Gerichtshof stellte klar (EuGH, Urteil vom 07. September 2023 in der Rechtssache C-162/22), dass Daten, die zur Bekämpfung schwerer Kriminalität gesammelt wurden, nicht zum Beweis bei Dienstvergehen genutzt werden dürfen. Auch der Generalanwalt beim EuGH stellte jüngst zu diesem Thema Schlussanträge (Schlussanträge des Generalanwalts Maciej Szpunar vom 28. September 2023 in der Rechtssache C-470/21), worin er eine Anpassung der bisherigen Rechtsprechung des EuGHs vorschlägt. Derweil hat die Bundesregierung sich immer noch nicht auf eine europarechtskonforme Neuregelung der Vorratsdatenspeicherung einigen können.

I. Schicksal der Vorratsdatenspeicherung in Deutschland

Mit der jüngsten EuGH-Entscheidung zu den deutschen Regelungen einer Verpflichtung von Telekommunikationsanbietern zur Speicherung von Verkehrs- und Standortdaten[2] sah die Vorratsdatenspeicherung einem ähnlichen Schicksal entgegen wie der Feldhamster in Deutschland. Ihr Bestand war extrem gefährdet und sie war vom Aussterben bedroht.[3]

II. Die Entscheidung des Bundesverwaltungsgerichts

Diesen Befund hat das BVerwG nun bestätigt und die Vorratsdatenspeicherung für unanwendbar erklärt. Es sieht in den Regelungen in § 177 Abs. 1 Nr. 3 i.V.m. § 174 Abs. 1 Satz 3 Telekommunikationsgesetzes (TKG) eine anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Vorratsspeicherung eines Großteils der Verkehrs- und Standortdaten. Dies widerspreche jedoch den europarechtlichen Vorgaben, wie der EuGH als Antwort auf die Vorlagefragen klargestellt habe.[4] Es bestünden keine objektiven Kriterien nach denen sich bestimmen ließe zu welchen konkreten Zwecken die zu speichernden Daten erhoben würden. Die Begrenzungen der Verwendungszwecke in § 177 Abs. 1 TKG griffen zu kurz und erfüllten die unionsrechtlichen Anforderungen gerade nicht.

In Hinblick auf die Verpflichtungen in Zusammenhang mit der Übermittlung von Nachrichten betont das BVerwG außerdem die fehlende, strikte Begrenzung auf den Zweck des Schutzes der nationalen Sicherheit. Auch hinsichtlich der Speicherung von IP-Adressen umfassten die Regelungen unionsrechtlich unzulässige Zwecke.

1 Volltexte zum Zeitpunkt des Redaktionsschlusses noch nicht verfügbar.

2 Siehe hierzu Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022 mwN.

3 https://www.bund.net/themen/tiere-pflanzen/tiere/saeugetiere/feldhamster/ (zuletzt abgerufen am 04.10.2023); https://www.rote-liste-zentrum.de/de/Vom-Aussterben-bedroht-Feldhamster-auf-der-Roten-Liste-1866.html (zuletzt abgerufen am 04.10.2023).

4 Siehe hierzu Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022.

Zudem hat das BVerwG entschieden, dass eine unionsrechtskonforme Auslegung der deutschen Regelungen in § 177 Abs. 1 Nr. 3 i.V.m. § 174 Abs. 1 Satz 3 TKG nicht möglich sei. Deshalb dürften sie wegen des Anwendungsvorrangs des Unionsrechts nicht angewendet werden. Hintergrund dieser Einschätzung ist, dass die Regelungen nach den Feststellungen des EuGHs im Vorabentscheidungsverfahren europarechtswidrig sind. Grundsätzlich käme dann lediglich eine unionsrechtskonforme Auslegung der Regelungen in Betracht, so dass sie trotzdem eingeschränkt weiterhin angewendet werden könnten. Allerdings hatte der EuGH angesichts der betroffenen Grundrechte hohe Anforderungen an die Bestimmtheit und Klarheit der in Rede stehenden Normen gestellt. Hierin sieht das BVerwG nun eine derart hohe Hürde, dass eine Auslegung hier nicht möglich sei.

Europarechtliche Regelungen genießen grundsätzlich in der Normenhierarchie Vorrang vor nationalen Regelungen. Da das Europarecht aber in diesem Fall einer Vorratsdatenspeicherung, wie sie nach den deutschen Regelungen vorgesehen ist, widerspricht, bedeutet dies für die nationale Regelung, dass sie dahinter zurücktreten muss. Daher hat das BVerwG sie im Ergebnis für unanwendbar erklärt.

III. Das Urteil des Europäischen Gerichtshofs

Auch vor dem EuGH (Urteil vom 07. September 2023 in der Rechtssache C-162/22) ging es erneut um die Vorratsdatenspeicherung. Diesmal ging es allerdings nicht darum, was oder wie gespeichert werden darf, sondern darum, wozu die gespeicherten Daten genutzt werden dürfen. Dabei stellte der EuGH klar, dass die Daten nur zu den Zwecken verwendet werden dürfen, zu denen sie ursprünglich rechtmäßig gespeichert wurden.

1. Der Sachverhalt und die Vorlagefrage

Der Ausgangsfall spielt in Litauen. Auch dort waren die Betreiber elektronischer Kommunikationsdienste, jedenfalls zur Zeit des Ausgangsverfahrens, verpflichtet, gewisse Verkehrs- und Standortdaten auf Vorrat zu speichern und gegebenenfalls an die zuständigen Behörden zur Bekämpfung schwerer Kriminalität weiterzugeben.

Die litauische Generalstaatsanwaltschaft verdächtigte einen Staatsanwalt der Korruption. Er sollte im Rahmen einer von ihm geleiteten Ermittlung dem Verdächtigen und seinem Anwalt relevante Information über das Verfahren mitgeteilt haben. Im Ergebnis ergab die eingeleitete Untersuchung ein Dienstvergehen durch den Staatsanwalt. Gestützt wurden diese Erkenntnisse insbesondere auf Daten aus einer Überwachung elektronischer Kommunikationsnetze, nämlich, dass Telefonate zwischen dem Staatsanwalt und dem Anwalt des Verdächtigen stattgefunden hatten. Die Überwachung erfolgte auf Grundlage gerichtlicher Beschlüsse und umfasste auch die Aufzeichnung der Inhalte der Telefonate.

Nachdem der Staatsanwalt seines Amtes enthoben war, legte er gegen diese Entscheidung Rechtsmittel bei den litauischen Gerichten ein. Dabei rügte er insbesondere, dass die Disziplinarmaßnahmen vor allem auf Erkenntnissen aus der elektronischen Überwachung im Rahmen strafrechtlicher Ermittlungen gestützt wurden. Die Überwachungen selbst waren auf Grund der richterlichen Anordnungen soweit nach litauischem Recht aber zulässig.

Allerdings sah das litauische Recht in Bezug auf kriminalpolizeiliche Erkenntnisgewinnung die Möglichkeit vor, dass gewonnene Informationen aus einer strafrechtlichen Ermittlung auch im Rahmen von Ermittlungen wegen Disziplinar- oder Dienstvergehen im Zusammenhang mit Korruption verwendet werden durften. Das wiederum nahm das vorlegende Gericht (Oberstes Verwaltungsgericht von Litauen) zum Anlass den EuGH zu fragen, ob die darauf fußende behördliche Praxis, die in diesem Fall zu den Disziplinarmaßnahmen geführt hatte, mit dem Europarecht vereinbar sei.

2. Die Entscheidung des EuGHs

Der EuGH verstand die Vorlagefrage so, dass es allein auf die Frage ankam, ob Vorratsdaten, die zur Bekämpfung schwerer Kriminalität gespeichert und den Behörden zur Verfügung gestellt wurden, von diesen Behörden auch für Untersuchungen wegen Dienstvergehen im Zusammenhang mit Korruption verwendet werden durften.

Dazu stellt er zunächst klar, dass die Betreiber elektronischer Kommunikationsdienste den Behörden nur Zugang zu den Daten gewähren dürften, wenn sie sie zuvor rechtmäßig gespeichert

hätten. Rechtmäßig hieße in diesem Zusammenhang immer in Einklang mit Art 15 Abs. der Richtlinie 2002/58. Dies ist nach der Rechtsprechung des EuGHs nur der Fall, wenn sie zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit notwendig seien. Neben dieser Voraussetzung fordert der EuGH zudem weitere Einschränkungen, wie beispielsweise objektive und nichtdiskriminierende Kriterien, für die Zulässigkeit einer gezielten Vorratsspeicherung.[5]

Neben der unionsrechtskonformen Speicherung trete, nach Ansicht des EuGHs, die unionsrechtskonforme Weitergabe der gespeicherten Daten an die Behörden. Hierzu enthält das Urteil des EuGHs zunächst Ausführungen zu Zielen, die mit einer Nutzung der auf Vorrat gespeicherten Daten verfolgt werden. So gebe es Gründe, die Ausnahmen von der Vertraulichkeit personenbezogener Daten zuließen. Hierunter fiele beispielsweise die nationale Sicherheit, aber auch die Verfolgung von Straftaten. Diese Ausnahmen dürften aber nicht zur Regel werden. Deshalb sei die Aufzählung der Ziele in Art. 15 Abs. 1 S. 1 der Richtlinie 2002/58 abschließend.

Innerhalb dieser Ziele bestünde daneben auch eine klare Hierarchie entsprechend ihrer jeweiligen Bedeutung für das Gemeinwohl. An der Spitze dieser Hierarchie stehe der Schutz der nationalen Sicherheit, wofür auch schwerere Grundrechtseingriffe zulässig wären. Darunter reihe sich unter anderem die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten ein. Hierbei wiederum stehe die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit hierarchisch über der Bekämpfung von Straftaten im Allgemeinen und der Verhütung leichter Bedrohungen der öffentlichen Sicherheit. Sie rechtfertige daher nur nicht schwere Eingriffe in die entsprechenden Grundrechte.

Zur Weitergabe der gespeicherten Daten an die Behörden stellt der EuGH darauf aufbauend fest, dass sie nur zur Erreichung desjenigen Zieles erfolgen dürfe, zu dem die Daten ursprünglich gespeichert wurden. Einzige Ausnahme hiervon gelte für Ziele, die in der Hierarchie über den Zielen stünden, zu deren Erreichung die Daten gespeichert wurden. Das heißt, dass Daten, die zur Bekämpfung von Straftaten gespeichert wurden, zum Schutz der nationalen Sicherheit genutzt werden dürften, andersherum Daten, die zum Schutz der nationalen Sicherheit gespeichert wurden, aber nicht zur Bekämpfung von Straftaten genutzt werden dürften.

Diese Überlegungen überträgt der EuGH dann auf die spätere Nutzung der Verkehrs- und Standortdaten. Dementsprechend urteilt er im Ergebnis, dass Daten, die zur Bekämpfung schwerer Kriminalität auf Vorrat gespeichert und an die zuständigen Behörden weitergegeben wurden, nicht an andere Behörden übermittelt und dazu genutzt werden dürften, um dem Ziel der Bekämpfung von Dienstvergehen zu dienen. Diese Nutzung widerspreche nämlich der zuvor dargestellten Hierarchie der dem Gemeinwohl dienenden Ziele.

Abschließend weist er noch daraufhin, dass die Ahndung von Disziplinar- oder Dienstvergehen in den Bereich des Verwaltungsrechts und nicht des Strafrechts fiele und daher auch nicht unter den Ausnahmenkatalog des Art. 15 Abs. 1 der Richtlinie 2002/58 zu fassen sei.

IV. Die Schlussanträge des Generalanwalts

In der Rechtssache C-470/21 hat der Generalanwalt Maciej Szpunar am 28. September 2023 seine Schlussanträge vorgelegt. Es sind in diesem Verfahren bereits die zweiten Schlussanträge, da der EuGH die mündliche Verhandlung nach den ersten Schlussanträgen entgegen seiner üblichen Praxis wiedereröffnet hatte (Beschluss vom 23. März 2023). Nun wird sich das Plenum aus allen 27 Berufsrichtern am EuGH mit der Sache befassen. Dies erfolgt nur, wenn die Rechtssache von außergewöhnlicher Bedeutung ist. Der Generalanwalt schlägt in seinen Schlussanträgen vor, die Zulässigkeit einer Speicherung auf Vorrat von der Schwere des Eingriffs in die Grundrechte abhängig zu machen. So hält er die Erhebung von Daten im Zusammenhang mit einer Zuordnung zu einer IP-Adresse, wenn sie zur Aufdeckung und Verfolgung einer Straftat unentbehrlich ist, für zulässig. Insofern hält er eine begrenzte Weiterentwicklung der Rechtsprechung des EuGHs für notwendig. Konkret geht es in dem Verfahren um den Umgang einer französischen Verwaltungsbehörde („Hadopi“: Haute autorité pour la diffusion des œuvres et la protection des droits sur internet [Hohe Behörde für die Verbreitung von Werken und den Schutz von Rechten im Internet]) mit Urheberrechtsverstößen, die ausschließlich im Internet erfolgen.

5 Zu sämtlichen Anforderungen im Einzelnen: Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022.

V. Der Stand der Gesetzgebung zur Vorratsdatenspeicherung

Die Fronten in der politischen Debatte um eine Neuregelung einer Vorratsdatenspeicherung in Deutschland sind weiterhin verhärtet. Weder konnte sich bislang Bundesinnenministerin Nancy Faeser mit ihrer Forderung nach einer anlasslosen Vorratspeicherung von IP-Adressen, noch Justizminister Marco Buschmann mit seiner Forderung nach dem sogenannten Quick-freeze-Verfahren durchsetzen.[6]

Auch die jüngste Bundestagsdebatte am 20. September 2023 zu diesem Thema lieferte keine weiteren neuen Erkenntnisse, wie eine künftige Regelung ausgestaltet sein könnte.

VI. Folgen der Entscheidungen

Das Thema der Vorratsdatenspeicherung wird uns auch in Zukunft beschäftigen. Endgültig geklärt ist nun aber der Bestand der aktuellen Regelungen in Deutschland. Sie sind unionsrechtswidrig und dürfen auch nicht mehr angewendet werden. Eine gültige Verpflichtung zur Speicherung von Verkehrs- oder Standortdaten für Anbieter öffentlich zugänglicher Telekommunikationsdienste gibt es in Deutschland zurzeit nicht. Ob und wie eine solche in Zukunft geregelt werden könnte, ist angesichts der politischen Uneinigkeit, auch innerhalb der Ampel-Koalition, noch vollkommen offen.

Währenddessen ergehen auf europäischer Ebene wichtige Entscheidungen zum künftigen Umgang mit einer rechtmäßigen Form einer Vorratsdatenspeicherung, wie sie auch in Deutschland von vielen Seiten gefordert wird.

Die Auswirkungen auf Hochschulen hängen daher weiterhin von der konkreten Ausgestaltung einer vermutlich kommenden künftigen Regelung ab. Sie sind dementsprechend derzeit noch nicht vorhersehbar, aber im Blick zu behalten.

6 Zu den einzelnen Vorschlägen eingehend: Palenberg, Hamstern verboten, DFN-Infobrief Recht 11/2022.

Kurzbeitrag: Protect me if you can

Die Bundesregierung legt ein Eckpunktepapier für die Reform des Beschäftigtendatenschutzes vor

von Nicolas John

Fragen im Beschäftigtendatenschutzrecht sind ein Dauerbrenner.[1] Im April 2023 legten das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) ein Eckpunktepapier mit Vorschlägen für ein Beschäftigtendatenschutzgesetz vor. Zeit, einen Überblick über den aktuellen Stand des Beschäftigtendatenschutzes, den Entwurf der Bundesregierung und kommende Entwicklungen zu schaffen.

I. Überblick zum aktuellen Beschäftigtendatenschutz

Auf europarechtlicher Ebene gibt es keinen speziellen Beschäftigtendatenschutz. Vielmehr überlässt es Art. 88 Datenschutz-Grundverordnung (DSGVO) den Mitgliedstaaten, selbst spezifische Regelungen in diesem Bereich zu treffen. Diesen Spielraum der Öffnungsklausel füllt bislang § 26 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) als zentrale Rechtsgrundlage und Generalklausel des deutschen Beschäftigtendatenschutzrechts.

Nach dem Urteil des Gerichtshofs der Europäischen Union (EuGH)[2] vom 30. März 2023 wird nun die Europarechtskonformität der Generalklausel zunehmend in Zweifel gezogen. Zwar betraf das Urteil nicht unmittelbar das BDSG; der EuGH entschied allerdings, dass sich nationale Regelungen zum Beschäftigtendatenschutz zwingend von den allgemeinen Regelungen der DSGVO unterscheiden müssen, um dem unionsrechtlichen Wiederholungsverbot und dem Auslegungsmonopol des EuGHs gerecht zu werden. Bei Generalklauseln wie dem § 26 BDSG bestehen daher Zweifel an der Europarechtskonformität. Die Entscheidung des Verwaltungsgerichts (VG) Wiesbaden, in deren Rahmen der EuGH angerufen wurde, steht bislang noch aus.[3]

II. Das Eckpunktepapier der Bundesregierung

Die Unsicherheiten des Beschäftigtendatenschutzes kommen nicht überraschend. Nachdem zuletzt 2010 ein Regierungsentwurf scheiterte, setzte sich auch die Ampelregierung in ihrem Koalitionsvertrag 2021 das Ziel, „Regelungen zum Beschäftigtendatenschutz zu schaffen, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen“.[4] Etwa einen Monat, nachdem sich aufgrund des Urteils des EuGHs Zweifel am bisherigen status quo des Beschäftigtendatenschutzes verfestigten, veröffentlichten

1 Z.B. Müller, Beschäftigtendatenschutz von A bis Z, DFN-Infobrief Recht 6/2023; John, Kurzbeitrag: Alles neu macht der EuGH, DFN-Infobrief Recht 6/2022; Voget, Work Data Balance: Der Beschäftigtendatenschutz, DFN-Infobrief Recht 11/2022; John, Die Beschäftigung mit den Beschäftigtendaten, DFN-Infobrief Recht 10/2022; Gielen, 2020: Odyssee im Beschäftigtendatenschutz, DFN-Infobrief Recht 5/2021.

2 Siehe hierzu John, Kurzbeitrag: Alles neu macht der EuGH, DFN-Infobrief Recht 6/2023; John, Die Beschäftigung mit den Beschäftigtendaten, DFN-Infobrief Recht 10/2022.

3 Hierzu John, Die Beschäftigung mit den Beschäftigtendaten, DFN-Infobrief Recht 10/2022.

4 Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP), S. 17.

das BMAS und BMI nun im April ein Eckpunktepapier mit ersten konkreteren Vorschlägen.[5]

Geplant ist demnach ein eigenständiges Beschäftigtendatenschutzgesetz, dessen Entwurf noch in der ersten Hälfte der Legislaturperiode veröffentlicht werden soll. Das Gesetz soll, wie auch die DSGVO, grundsätzlich einen technologieneutralen Ansatz verfolgen und in seinem Anwendungsbereich weit gefasst sein. So sollen auch etwa solo-selbstständige Plattformtätige miteinbezogen werden, um der strukturellen Unterlegenheit von Arbeitnehmer:innen im Beschäftigungskontext gerecht zu werden.

Neue Regelungen sollen außerdem zu besonders risikoreichen Datenverarbeitungssituationen getroffen werden. Ein Schwerpunkt liegt dabei im Bereich der Mitarbeiter:innenüberwachung: Eine dauerhafte Überwachung soll nur in Ausnahmefällen unter strengen Voraussetzungen zulässig sein. Genauso sollen verdeckte Überwachungsmaßnahmen gemäß der bereits geltenden Rechtsprechung nur ausnahmsweise möglich sein. Für offene Überwachungsmaßnahmen sollen klare Bedingungen vorgegeben werden.

Eine weitere risikoreiche Verarbeitung besteht in konzerninternen Datenübermittlungen, die allerdings aus Effizienzgründen oft notwendig sind. In diesem Bereich sollen bürokratische Hürden gesenkt werden und Verarbeitungsprozesse für die Beschäftigten kontrollierbarer werden. Berücksichtigen soll das Beschäftigtendatenschutzgesetz auch die erhöhte Schutzbedürftigkeit von Arbeitnehmer:innen, die etwa während des Bewerbungsverfahrens besteht oder aus dem Einsatz von KI resultieren kann. Insbesondere die Diskriminierung durch algorithmische Datenverarbeitungen sollen nach dem Eckpunktepapier verhindert werden, indem die Transparenz für Beschäftigte gestärkt wird. Im Bewerbungsverfahren sollen dagegen klare Anforderungen für mehr Rechtssicherheit sorgen, z.B. mit einem Katalog an verbotenen Fragen. Für den Umgang mit besonders sensiblen Daten sollen typische Fallgruppen konkret zu mehr Sicherheit führen.

Ein weiterer Regelungspunkt stellt die Vorgabe von Kriterien für Interessenabwägungen dar. Durch diese Regelungen soll die Durchführung solcher Abwägungen für alle Beteiligten einfacher und verständlicher werden. Neben diesen Interessenabwägungen müssen Arbeitgeber:innen regelmäßig auch Einwilligungen von den Beschäftigten für Datenverarbeitungen einholen. Auch hierzu sieht das Eckpunktepapier die Vorgabe klarer Maßstäbe für die Anforderungen an diese Einwilligungen vor, insbesondere mit Blick auf die Freiwilligkeit.

Neben diesen Regulierungsvorschlägen soll auch die Rechtssicherheit für interne Datenverarbeitungen gestärkt werden. Hierzu sind Fallgruppen vorgesehen, welche die Zulässigkeit von Datenverarbeitungen klären sollen. Zusätzlich sollen auch die Betroffenenrechte der DSGVO ergänzt werden, die Bundesregierung sieht hier insbesondere Handlungsbedarf bei Löschpflichten von Bewerbungsunterlagen.

Schließlich sind auch Konkretisierungen hinsichtlich der gängigen „Bring Your Own Device"-Praxis sowie Erweiterungen bezüglich der Mitbestimmung der Betriebsräte geplant, um die Rechtsklarheit in diesen Bereichen zu erhöhen.

III. Fazit

Die Unwirksamkeit der Generalklausel des § 26 Abs. 1 S. 1 BDSG lässt sich bislang zwar nur mittelbar aus dem Urteil des EuGHs ableiten, scheint aber nicht fernliegend. Insoweit bleibt das Urteil des VG Wiesbaden abzuwarten. Der Eckpunkteplan der Bundesregierung lässt ein ambitioniertes Gesetzesvorhaben erahnen. Der Vorschlag des BMAS und BMI lässt allerdings noch viele Punkte offen und abstrakt. Man darf also auf den tatsächlichen Gesetzesentwurf gespannt bleiben.

5 BMAS/BMI, Vorschläge für einen modernen Beschäftigtendatenschutz v. 13.4.2023, abrufbar unter: https://fragdenstaat.de/anfrage/aktueller-stand-beschaeftigtendatenschutz/804753/anhang/vorschlge-beschftigtendatenschutz.pdf (zuletzt abgerufen am 28.09.2023).

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn