NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

11/2022
November 2022

Work Data Balance: Der Beschäftigtendatenschutz

Aktuelle Fragestellungen und Entscheidungen rund um den Datenschutz der Beschäftigten

Data Unchained

Zum Stand der europäischen Open Data Regelungen

Hamstern verboten

Die aktuelle Regelung zur Vorratsdatenspeicherung in Deutschland ist unzulässig

Selbst ist (nicht) die Kontrolle

Bußgeld gegen Berliner Unternehmen wegen fehlender Unabhängigkeit des Datenschutzbeauftragten

Work Data Balance: Der Beschäftigtendatenschutz

Aktuelle Fragestellungen und Entscheidungen rund um den Datenschutz der Beschäftigten

von Johanna Voget

Obwohl die Datenschutz-Grundverordnung (DSGVO) keine speziellen Regelungen konkret für den Beschäftigtendatenschutz vorsieht, hat das Thema für den Arbeitgeber oftmals weiterreichende Auswirkungen. Grund hierfür ist insbesondere die Angst vor Bußgeldern, die Sensibilität in der Belegschaft und entsprechende Erwartungen an den Arbeitgeber. Die Thematik ist daher auch von großer Bedeutung für Hochschulen und Forschungseinrichtungen und immer wieder Gegenstand der Rechtsprechung. Hierzu informierte der DFN-Verein und die Forschungsstelle Recht bereits in der Vergangenheit.[1] Dieser Beitrag soll einen allgemeinen Überblick über die neuen Entscheidungen und Vorgaben an der Schnittstelle von Arbeitsrecht und Datenschutzrecht verschaffen.

I. Auskunftsanspruch nach Art. 15 DSGVO

Art. 15 Abs. 1 DSGVO normiert das Auskunftsrecht der betroffenen Person hinsichtlich der Verarbeitung personenbezogener Daten. Zu den allgemeinen Voraussetzungen und dem Umgang mit dem Auskunftsanspruch wird auf die Ausführungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verwiesen.[2] Korrespondierend hiermit besteht nach Art. 15 Abs. 3 DSGVO auch ein Anspruch auf Herausgabe von Kopien der verarbeiteten Daten. Die Ansprüche werden in der Praxis zunehmend als taktisches Mittel in der gerichtlichen Auseinandersetzung eingesetzt. Hoch umstritten sind die Reichweite und der Umfang der Ansprüche. Dies ist vor dem Hintergrund drohender Schadensersatzansprüche nach Art. 83 Abs. 5 lit. b) DSGVO problematisch.

1. Bestimmtheit

Zu der Frage, wie bestimmt ein Antrag auf Auskunftserteilung bzw. Herausgabe von Kopien sein muss, traf das Bundesarbeitsgericht (BAG) im Frühjahr letzten Jahres eine Entscheidung (Urt. v. 27.4.2021 – 2 AZR 342/20). In dem zugrundeliegenden Fall hatte ein während der Probezeit gekündigter Arbeitnehmer auf Auskunft und Herausgabe von Mail-Kopien geklagt. Während ihm die Auskunft vom Arbeitgeber erteilt wurde, wurden die Kopien der Mails zurückgehalten. Das BAG verhielt sich inhaltlich nicht zu Art. 15 Abs. 3 DSGVO, sondern wies die Klage bereits wegen mangelnder Bestimmtheit des Klageantrags gem. § 253 Abs. 2 Nr. 2 Zivilprozessordnung (ZPO) ab. Die abstrakte Benennung von Kategorien der Mails sei ungenügend, vielmehr sei eine konkrete Benennung der einzelnen Korrespondenz für das Zwangsvollstreckungsverfahren notwendig.

---

1 Siehe hierzu Gielen, 2020: Odyssee im Beschäftigtendatenschutz, DFN-Infobrief Recht 05/2021; John, Die Beschäftigung mit Beschäftigtendaten, DFN-Infobrief Recht 10/2022; Handlungsempfehlung zum Beschäftigtendatenschutz.

2 https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Kurzpapiere/20170726_Kurzpapier_6_Auskunftsrecht.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 21.10.2022).

In diesem Sinne entschieden die obersten Richter der arbeitsrechtlichen Gerichtsbarkeit abermals im Dezember 2021 (Urt. v. 16.12.2021 - 2 AZR 235/21). Ein Klageantrag, der auslegungsbedürftige Begriffe enthalte, über deren Inhalt Zweifel nicht ausgeräumt werden können, sei nicht hinreichend bestimmt. Es genüge also für die Bestimmtheit des Klageantrags nach § 253 Abs. 2 Nr. 2 ZPO nicht, dass der Arbeitnehmer abstrakt bestimme, welche Art von Informationen („Leistungs- und Verhaltensdaten") er begehrt. Anstatt also nur abstrakt die Herausgabe von Unterlagen zu fordern, in denen Aussagen über den Arbeitnehmer, seine Leistung und sein Verhalten, getroffen werden, müsse zum Beispiel die korrekte E-Mail-Korrespondenz, mit Adressaten oder Daten aufgeführt werden.

2. Umfang

Bemerkenswerterweise sieht der BGH dies wohl ganz anders: Es scheint dem Senat für die Bestimmtheit des Klageantrags nach § 253 Abs. 2 Nr. 2 ZPO vielmehr zu reichen, dass der Beklagte schlicht geltend macht, er begehre Auskunft über die ihn betreffenden personenbezogenen Daten. Mit einem Urteil aus dem letzten Jahr entschied der Bundesgerichtshof (BGH) so deutlich wohlwollender zugunsten der betroffenen Arbeitnehmer hinsichtlich der Reichweite der Ansprüche aus Art. 15 DSGVO (Urt. v. 15.6.2021 – VI ZR 576/19). In dem Verfahren stritten die Parteien, ein Versicherungsnehmer und der Versicherer, um die Vorlage von Unterlagen wie E-Mails und interner Vermerke. Der BGH legte hier ein weites Verständnis von Art. 15 DSGVO zugrunde: Es seien „alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen (umfasst), unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt". Nicht erforderlich sei es, dass es sich um „signifikante biografische Informationen" handelt, die im Vordergrund des fraglichen Dokuments stehen. Auch die Tatsache, dass die Daten dem Betroffenen bereits bekannt sind, schließe den Auskunftsanspruch nicht per se aus. Sinn und Zweck des Anspruchs auf Auskunft und Herausgabe von Kopien ist es, die Möglichkeit für den Betroffenen zu schaffen, sich zu vergewissern, dass die ihn betreffenden Daten korrekt sind und in rechtmäßiger Art und Weise verarbeitet wurden. Hierbei sind auch rein interne Vermerke oder Bewertungen umfasst, soweit sie personenbezogene Daten enthalten. Auf dieser Linie lag auch noch die Entscheidung des Landesarbeitsgerichts (LAG) Baden-Württemberg (Urt. v. 17.3.2021 Az. 21 Sa 43/20), welche im Anschluss jedoch vom BAG in der bereits dargestellten Entscheidung (Az. 2 AZR 235/21) kassiert wurde.

3. Verhältnis zwischen Art. 15 Abs. 1 und 3 DSGVO

Darüber hinaus ist auch das Verhältnis der Ansprüche des Art. 15 DSGVO untereinander nicht abschließend geklärt. Nach zivil- und verwaltungsgerichtlicher Rechtsprechung bestehen die Ansprüche nebeneinander (vgl. Oberverwaltungsgericht (OVG) Münster v. 8.6.2021 – 16 A 1582/20): Ziel des Art. 15 Abs. 1 DSGVO ist es, dem betroffenen Arbeitnehmer durch die Auskunft zu ermöglichen, weitere Rechte wie die Berichtigung gem. Art. 16 DSGVO, Löschung gem. Art. 17 DSGVO, oder eben Schadensersatz nach Art. 82 DSGVO geltend zu machen. Zweck des danebenstehenden Art. 15 Abs. 3 DSGVO ist das Bilden eines umfassenden Eindrucks und so die Überprüfung, ob die erteilte Auskunft korrekt ist. Nach dieser Ansicht wird der Anspruch auf Herausgabe von Kopien nicht durch den Auskunftsanspruch inhaltlich begrenzt. In der arbeitsgerichtlichen Rechtsprechungspraxis geht Art. 15 Abs. 3 DSGVO hingegen nur so weit, wie auch Art. 15 Abs. 1 DSGVO reicht. Zuletzt bestätigte das LAG Niedersachsen diese Ansicht (Urt. v. 22.10.2021 – 16 Sa 761/20). Entscheidend hierfür spreche der Erwägungsgrund 63 zur DSGVO, nach dem für den Regelungszweck des Auskunftsrechts keine umfassende Vorlegung von Kopien aller Informationen, die personenbezogene Daten beinhalten, erforderlich sei. Zudem beziehe sich Art. 15 Abs. 3 DSGVO auf die personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Gerade diese seien eben auch von Art. 15 Abs. 1 DSGVO erfasst.

II. Schadensersatz nach Art. 82 Abs. 1 DSGVO

Eine große Rechtsunsicherheit bei der Frage nach dem Bestehen von Schadensersatzansprüchen bei Datenschutzverstößen im Rahmen von Arbeitsverhältnissen besteht hier in dem Fehlen konkreter Bemessungskriterien. Insbesondere die Problematik, ob es für die Geltendmachung eines Anspruchs einer gewissen Erheblichkeit der Rechtsbeeinträchtigung bedarf, ist immer wieder Gegenstand gerichtlicher Auseinandersetzung. Die Rechtsprechung stellt in der Kasuistik hieran sehr unterschiedliche Anforderungen. Das Amtsgericht (AG) Goslar (Urt. v. 27.09.2019 – 28 C 7/19) hatte eine solche Erheblichkeit gefordert, die Entscheidung

wurde anschließend jedoch vom Bundesverfassungsgericht (BVerfG) aufgehoben (Beschluss. v. 14.1.2021 – 1 BvR 2853/19). Die Begründung der Verfassungshüter in Karlsruhe hierzu lautete, dass die Frage nach einer Schwelle der Rechtsbeeinträchtigung wiederum Frage der Auslegung von Unionsrecht ist und somit dem Europäischen Gerichtshof (EuGH) vorzulegen sei. Da keine Ausnahme von der Pflicht zur Vorlage an den EuGH, sog. acte éclairé oder acte clair, vorliege, verletze das AG Goslar nach den Feststellungen des BVerfG mit der Nichtvorlage das Recht des Klägers auf den gesetzlichen Richter nach Art. 101 Abs. 1 Satz 2 Grundgesetz (GG). Bislang hat das AG Goslar in dem Verfahren nicht erneut entschieden oder eine Vorlage an den EuGH vorgenommen. Die zugrundeliegende Frage, ob konkrete Schwellenwerte für einen Schadensersatzanspruch erforderlich sind, bleibt somit ungeklärt. Das LAG Hamm stellte zur Bemessung auf das Vorliegen einer „Hartnäckigkeit" der Rechtsverletzung ab (Urt. v. 11.5.2021 – 6 Sa 1260/20).

Nun könnte eine Klärung der Problematik durch die Vorlage des BAG an den EuGH herbeigeführt werden (Vorlagebeschluss v. 26.8.2021 – 8 AZR 253/20). Konkret formulierte das BAG hier unter anderem die Vorlagefrage, ob bei der Bemessung der Höhe des zu ersetzenden Schadens im Rahmen des Art. 82 Abs. 1 DSGVO der Grad des Verschuldens bei der Rechtsbeeinträchtigung zu berücksichtigen ist.

Insgesamt werden in der Praxis überwiegend eher strenge Maßstäbe angelegt und niedrige Beträge zugesprochen.

III. Datenschutzbeauftragter im Betrieb

Die DSGVO sieht in Art. 88 eine Öffnungsklausel für die Datenverarbeitung im Beschäftigungskontext vor. Dies erfasst jedoch nicht Regelungen betreffend den Datenschutzbeauftragten, da die Vorschriften in Art. 37-39 DSGVO diesbezüglich abschließend sind. Trotzdem sieht das Bundesdatenschutzgesetz (BDSG) in §§ 5-7 Sonderregeln vor. Die wichtigste Abweichung stellt der starke Abberufungs- und Kündigungsschutz des Beauftragten nach § 6 Abs. 4 BDSG dar. Die Abberufung ist danach nur unter entsprechender Anwendung des § 626 Bürgerliches Gesetzbuch (BGB) möglich, eine Kündigung ebenfalls nur aus wichtigem Grund. Die Vorschrift des Art. 38 Abs. 3 Satz 2 DSGVO entfaltet einen wesentlich schwächeren Schutz: Wegen der Erfüllung seiner Aufgaben darf der Beauftragte nicht abberufen oder benachteiligt werden, die kausale Verknüpfung zwischen Aufgabenwahrnehmung und Abberufung ist also ausgeschlossen. Betriebsbedingte Abberufungen sind im Umkehrschluss ohne weiteres möglich, auch enthält die Vorschrift keinen expliziten Kündigungsschutz. Sofern ein Beauftragter nicht abberufen werden darf, kann aber selbstredend auch keine Kündigung erfolgen. Implizit besteht also Kündigungsschutz auch für den Fall der Verknüpfung der Aufgabenwahrnehmung mit der Abberufung.

Das BAG (Beschluss v. 27.4.2021 – 9 AZR 621/19) hat dem EuGH in einem Fall der Abberufung eines Datenschutzbeauftragten die Frage vorgelegt, ob der deutsche Gesetzgeber befugt ist, über die DSGVO hinaus strengere Regelungen vorzusehen.

Relevant wird an dieser Stelle auch die Frage, ob die Europäische Union (EU) überhaupt die Kompetenz für Regelungen des Arbeitsverhältnisses des Datenschutzbeauftragten hat oder ob es sich um materielles Arbeitsrecht handelt. In diesem Sinne legte das BAG bereits im Vorfeld zu dem aktuellen Verfahren dem EuGH eine Vorlagefrage zur Entscheidung vor (Beschluss v. 30.7.2020 – 2 AZR 225/20). Auch in diesem Fall war der EuGH also schon mit der Frage befasst, inwiefern der Bundesgesetzgeber im BDSG weitergehende Vorschriften zur Kündigung des Datenschutzbeauftragten vorsehen kann. Der EuGH entschied hierzu (Urt. v. 22.06.2022 – C 534/20), dass Art. 38 Abs. 3 Satz 2 DSGVO so auszulegen sei, dass er einer nationalen Regelung nicht entgegensteht, die vorsieht, dass ein Datenschutzbeauftragter nur aus wichtigem Grund gekündigt werden kann, auch wenn die Kündigung nicht mit der Erfüllung seiner Aufgaben zusammenhängt, sofern diese Regelung die Verwirklichung der Ziele der DSGVO nicht beeinträchtigt.[3] Eine abweichende Entscheidung im nun vorliegenden zweiten Verfahren ist nicht zu erwarten, sodass der starke Kündigungsschutz von Datenschutzbeauftragten nach nationalem Recht aufrecht erhalten bleiben dürfte.

IV. Vereinbarkeit von § 26 BDSG mit Art. 88 DSGVO

Das Verwaltungsgericht (VG) Wiesbaden (Beschluss v. 21.12.2020 – 23 K 1360/20.WI.PV) hat dem EuGH darüber hinaus die Frage vorgelegt, ob die Vorschrift des § 23 Abs. 1 Satz 1 des hessischen

3 Siehe hierzu John, Kurzbeitrag: Strenger geht's immer!, DFN-Infobrief Recht 08/2022.

Datenschutz- und Informationsfreiheitsgesetz (HDSiG), der wortlautgleich mit § 26 Abs. 1 Satz 1 BDSG ist, den Anforderungen des Art. 88 DSGVO genügt. § 26 BDSG stellt eine der zentralen Normen im Umgang mit den Beschäftigtendaten dar und normiert, dass personenbezogene Daten von beschäftigten verarbeitet werden dürfen, wenn dies im Zusammenhang mit der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses „erforderlich ist". Hierzu berichtete die Forschungsstelle Recht bereits in der Ausgabe des DFN-Infobrief Recht im letzten Monat.[4] Nach den Schlussanträgen des Generalanwalts Manuel Campos Sánchez-Bordona am 22. September 2022 ist nun die Entscheidung mit Spannung zu erwarten. Sollte sich der EuGH in dem Vorlageverfahren der Auffassung des VG Wiesbaden und des Generalanwalts anschließen, wäre § 23 Abs. 1 Satz 1 HDSiG unanwendbar, was mittelbar auch zu einer Unanwendbarkeit von § 26 Abs. 1 Satz 1 BDSG führen würde. Es käme somit allein auf die Regelungen der DSGVO, insbesondere den Erlaubnistatbestand des Art. 6 DSGVO, an. Dies dürfte die Diskussion um ein neues Beschäftigtendatenschutzrecht vertiefen, da Abhilfe nur durch eine neue spezielle Regelung des deutschen Gesetzgebers geschaffen werden kann.

V. Arbeitszeiterfassung

Zuletzt ist im Zusammenhang mit dem Datenschutz der Beschäftigten auch der hochaktuelle Beschluss des BAG zur Arbeitszeiterfassung (Beschluss v. 13.9.2022 – 1 ABR 22/21) anzuführen. Nach der Entscheidung der Richter in Erfurt sollen die Arbeitgeber nach § 3 Abs. 2 Nr. 1 Arbeitsschutzgesetz (ArbSchG) verpflichtet sein, ein System einzuführen, mit dem die Arbeitszeit der Arbeitnehmer gemessen werden kann. Hierbei nahm das Gericht eine unionsrechtskonforme Auslegung auf Grundlage der Entscheidung des EuGH zur EU-Arbeitszeitrichtlinie vor (Urt. v. 14.5.2019 – C-55/18). In den Reaktionen in Presse und Medien wird hierin ein Ende der Vertrauensarbeitszeit gesehen. In der Vergangenheit urteilten das Arbeitsgericht (ArbG) Berlin und das LAG Berlin-Brandenburg bereits zur Ausgestaltung eines Arbeitszeiterfassungssystems durch Fingerprint ohne Einwilligung des Arbeitnehmers.[5] Die konkrete, rechtlich zulässige und gleichzeitig praktisch umsetzbare Ausgestaltung der Systeme zur Erfassung der Arbeitszeit der Arbeitnehmer, insbesondere vor dem Hintergrund des pandemiebedingten vermehrten Arbeitens aus dem Homeoffice, bleibt nun abzuwarten. Dies sollte primär möglichst zeitnah durch den Gesetzgeber erfolgen, anderenfalls wird sich in der Rechtsprechung erneut eine Kasuistik zu zulässigen Systemen herausbilden.

VI. Ausblick und Reformbedarf

Hervorzuheben ist an dieser Stelle, dass die Ampel-Regierung im Koalitionsvertrag eine separate Regelung des Beschäftigtendatenschutzes vorgesehen hat.[6] Die Parteien des Deutschen Gewerkschaftsbundes (DGB) legten Anfang dieses Jahres einen Vorschlag für ein Beschäftigtendatenschutzgesetz vor.[7] Als Begründung für den Bedarf eines neuen Gesetzes wird vorgebracht, dass die DSGVO und die nationalen Vorschriften den praktischen Gegebenheiten im Beschäftigungskontext nicht hinreichend gerecht werden.

Auch für die Arbeitszeiterfassung ist eine gesetzliche Regelung im Koalitionsvertrag vorgesehen und ein erster Gesetzentwurf Anfang dieses Jahres von Arbeitsminister Heil vorgelegt worden. Durch das Urteil des BAG wurde der Gesetzgeber überholt und jedenfalls das „Ob", also die Pflicht zur Erfassung der Arbeitszeit, bereits aus den bestehenden Regelungen abgeleitet.

Zuletzt sei auch auf die Themenkomplexe der datenschutzrechtlichen Anforderungen bei der Datenverarbeitung durch den Betriebsrat sowie die Bemessung von Bußgeldern bei Verstößen gegen den Beschäftigtendatenschutz hingewiesen. Die Entwicklung und Darstellung dieser Problematiken wird auch Gegenstand der zukünftigen Forschungsarbeit der Forschungsstelle Recht sein.

---

4 Siehe hierzu John, Die Beschäftigung mit Beschäftigtendaten, DFN-Infobrief Recht 10/2022.

5 Siehe hierzu John, Tick Tack – Finger ab?, DFN-Infobrief Recht 02/2020.

6 Koalitionsvertrag 2021 – 2025 von SPD/Grünen/FDP, abrufbar unter: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (zuletzt abgerufen am 04.10.2022).

7 Gesetzentwurf des DGB, abrufbar unter: https://www.dgb.de/uber-uns/dgb-heute/recht/++co++d8c37b52-88e2-11ec-acce-001a4a160123 (zuletzt abgerufen am: 04.10.2022).

VII. Bedeutung für wissenschaftliche Einrichtungen

Beschäftigte von Hochschulen und Forschungseinrichtungen und die öffentlichen Stellen als Arbeitgeber selbst sind von den aktuellen Entscheidungen und Reformen rund um den Beschäftigtendatenschutz betroffen. Insbesondere für die Arbeitgeber sind eindeutige Vorgaben wünschenswert, um Bußgelder und arbeitsrechtliche Streitigkeiten zu vermeiden.

Mit Spannung abzuwarten bleiben daher nun die ausstehenden Entscheidungen des EuGH und die Ausgestaltung der angekündigten speziellen Regelungen in einem separaten Gesetz zum Beschäftigtendatenschutz. Zu hoffen ist, dass die rechtlichen Unsicherheiten hierdurch ausgeräumt werden können.

Data Unchained

Zum Stand der europäischen Open Data Regelungen

von Owen Mc Grath

Daten haben in unserem Zeitalter einen überragenden Stellenwert. Entsprechend wertvoll ist der Zugang zu diesen. Bei Daten, die durch öffentliche Einrichtungen und somit über Steuergelder generiert werden, drängt sich die Frage auf, wem diese Daten zugänglich sein sollten. Dieser Frage hat sich der europäische Gesetzgeber in mehreren Rechtsakten angenommen. Der folgende Beitrag soll einen Überblick über den Stand der Gesetzgebung zu sogenannter „Open Data“ geben.

I. Open Data

Mit Open Data werden solche Daten bezeichnet, die der Öffentlichkeit zugänglich sind und von jedermann genutzt werden können. Von dem Begriff sind grundsätzlich Daten jeglicher Art und Güte umfasst. Der Beitrag nimmt vorrangig die Regulierung von „Open Government Data“ in den Fokus. Gemeint sind damit öffentlich zugängliche Verwaltungsdaten. Der Bereich der Open Science steht damit nicht im Mittelpunkt der folgenden Auseinandersetzung.[1]

Die allgemeine Zugänglichmachung von Daten, die durch die öffentliche Hand oder in dessen Auftrag generiert werden, hat mehrere Vorteile. Zum einen wird durch die so geschaffene Transparenz das Vertrauen der Bürger in den Staatsapparat gestärkt. Schließlich ist konkret ersichtlich, wofür Steuergelder eingesetzt werden und es ergibt sich eine unmittelbare Nutzbarkeit für den Einzelnen. Zum anderen öffnen frei zugängliche Daten die Tür zur weiteren Nutzung dieser Daten und fungieren so als Innovationstreiber.

II. Europäische Regelungsansätze

So erstrebenswert die freie Zugänglichmachung von Daten und insbesondere staatlicher Daten ist, so bedarf es dennoch eines rechtlichen Rahmens für ein solches Vorgehen.

Zu regeln gilt es vor allem, welche Daten in welcher Form zur Verfügung stehen müssen. Ferner stellt sich die Frage, wie mit Daten umzugehen ist, welche einen Personenbezug aufweisen oder anderweitige Rechte (Urheberrechte, Geheimnisschutzrechte etc.) tangieren.

Bereits 2003 kam der europäische Gesetzgeber dem Regelungsbedürfnis mit der „Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors“ (Public Sector Information Richtlinie oder PSI-RL)[2] in Teilen nach. Geregelt wurde hier der Umgang mit Daten, die bereits aufgrund anderer Verpflichtungen, zum Beispiel eines nationalen Gesetzes, zur Verfügung standen. Die Weiterverwendung solcher Daten sollte ohne wettbewerbsverzerrende Störungen gefördert werden. Eine eigene Pflicht zur Bereitstellung von staatlichen Daten ergab sich hieraus aber nicht.

Im Jahr 2019 wurde die PSI-RL neugefasst als „Richtlinie über offene Daten und die Weiterverwendung von Informationen

1 Siehe hierzu bspw.: https://www.horizont-europa.de/de/Open-Science-und-Open-Data-1767.html und https://eosc.eu/ (zuletzt abgerufen am 21.10.2022).

2 RL 2003/98/EG.

des öffentlichen Sektors“ (Open Data Richtlinie oder OD-RL).[3] Hierin wurde nunmehr festgelegt, dass bereitgestellte Daten zur besseren Weiterverwendbarkeit in maschinenlesbarer Form zur Verfügung stehen müssen. Eine aktive Pflicht zur Bereitstellung ergab sich allerdings auch nicht aus der OD-RL. Es bleibt bei der „Förderung der Weiterverwendung“. Festgelegt wird auch, wie mit Daten, die Personenbezug aufweisen oder an denen Rechte des geistigen Eigentums bestehen, umzugehen ist.

Weiterhin legt die Richtlinie fest, was unter „dynamischen Daten“, „Forschungsdaten“ und „hochwertigen Datensätzen“ zu verstehen ist und wie diese im Bereich der Open Data zu handhaben sind.

Dynamische Daten sind nach Art. 2 Nr. 8 OD-RL „Dokumente in digitaler Form, die häufig oder in Echtzeit aktualisiert werden, insbesondere aufgrund ihrer Volatilität oder ihres raschen Veraltens; von Sensoren generierte Daten werden in der Regel als dynamische Daten angesehen“. Diese sollen, insofern sie denn zur Verfügung gestellt werden, unmittelbar nach der Erfassung über eine entsprechende Schnittstelle zugänglich sein (Art. 5 Abs. 5 OD-RL).

Forschungsdaten definiert Art. 2 Nr. 9 OD-RL als „Dokumente in digitaler Form, bei denen es sich nicht um wissenschaftliche Veröffentlichungen handelt und die im Laufe von wissenschaftlichen Forschungstätigkeiten erfasst oder erzeugt und als Nachweise im Rahmen des Forschungsprozesses verwendet werden oder die in der Forschungsgemeinschaft allgemein für die Validierung von Forschungsfeststellungen und -ergebnissen als notwendig erachtet werden“. Öffentlich finanzierte Forschungsdaten sollen nach Art. 10 Abs. 1 OD-RL, ohne dass eine konkrete Verpflichtung hierzu besteht, „nach dem Grundsatz der „standardmäßig offenen Daten“ und im Einklang mit den FAIR-Grundsätzen offen zugänglich“ gemacht werden. Die FAIR-Grundsätze beschreiben die idealen Eigenschaften von Daten, die einer Weiterbildung eines gemeinsamen Wissensapparates dienen. Übersetzt sind das die folgenden Eigenschaften: Auffindbarkeit (findable), Zugänglichkeit (accessible), Interoperabilität (interoperable), Wiederverwendbarkeit (reusable).

Unter hochwertigen Datensätzen versteht die Richtlinie nach Art. 2 Nr. 10 OD-RL „Dokumente, deren Weiterverwendung mit wichtigen Vorteilen für die Gesellschaft, die Umwelt und die Wirtschaft verbunden ist, insbesondere aufgrund ihrer Eignung für die Schaffung von Mehrwertdiensten, Anwendungen und neuer, hochwertiger und menschenwürdiger Arbeitsplätze sowie aufgrund der Zahl der potenziellen Nutznießer der Mehrwertdienste und –anwendungen auf der Grundlage dieser Datensätze“. Zur Einordnung hängt der Richtlinie eine Liste von thematischen Kategorien von hochwertigen Datensätzen an. Zu diesen zählen beispielsweise Georaum- und Mobilitätsdaten. Der Kommission steht es nach nach Art. 13 Abs. 2 i.V.m. Art. 15 OD-RL zu, diese Liste zu ergänzen. Darüber hinaus kann die Kommission nach Art. 14 OD-RL mittels Durchführungsverordnung die Daten und die Modalität ihrer Bereitstellung konkretisieren.

Von dieser Befugnis hat die EU-Kommission Gebrauch gemacht und in diesem Jahr den Entwurf einer entsprechenden Durchführungsverordnung vorgelegt. Zu diesem Entwurf konnte im Sommer Stellung[4] genommen werden und eine finale Version wird im kommenden Jahr erwartet. Die nach dem Verordnungsentwurf offenzulegenden Daten entsprechen der nach der OD-RL festgelegten Liste von thematischen Kategorien von hochwertigen Datensätzen. Die Liste hochwertiger Datensätze als solche und die Modalitäten ihrer Veröffentlichung sind in der Durchführungsverordnung und ihrem Anhang konkretisiert. Beispielsweise wird festgelegt, in welcher Tiefe Datensätze aus den Bereichen Georaum, Erdbeobachtung, Meteorologie, Statistik, Unternehmen und Eigentümerschaft an Unternehmen sowie Mobilität bereitgestellt werden müssen.

Neben der OD-RL und der begleitenden Durchführungsverordnung hat die EU in diesem Jahr als Teil der europäischen Datenstrategie noch den Data-Governance-Act (DGA)[5] verabschiedet. Diese Verordnung hat ebenfalls das Ziel, Daten der öffentlichen Hand leichter und sicherer zugänglich zu machen. Vor allem soll der Austausch von Daten zwischen Mitgliedsstaaten und verschiedenen Sektoren erleichtert werden. Insofern ergänzt sie die Regelungen der OD-RL. Allerdings ergibt sich auch aus dem DGA keine Bereitstellungspflicht für staatliche Daten.

3 RL 2019/1024/EU.

4 Zu dem Verordnungsverfahren: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12111-Offene-Daten-Verfugbarkeit-offentlicher-Datensatze_de (zuletzt abgerufen am 21.10.2022).

5 VO (EU) 2022/868.

III. Nationale Regelungen

Auf nationaler Ebene wurden die Richtlinien der EU durch mehrere Gesetze umgesetzt. Zentral ist hierbei auf Bundesebene der § 12a E-Government-Gesetz (EGovG). Dieser verpflichtete die Behörden der unmittelbaren Bundesverwaltung grundsätzlich dazu, „unbearbeitete maschinenlesbare Daten, die sie zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen, zum Datenabruf über öffentlich zugängliche Netze bereit[zustellen]“. Das Zweite Open-Data-Gesetz erweitert die Anwendung Vorschrift auf die Behörden der mittelbaren Bundesverwaltung. Explizit ausgenommen sind Selbstverwaltungskörperschaften und damit auch Universitäten. Ähnlich einem Datenschutzbeauftragten verpflichtet § 12a Abs. 9 EGovG die betroffenen Behörden dazu, einen Open-Data-Koordinator zu benennen, der als Ansprechpartner in Sachen Open Data gilt.

Auch auf landesrechtlicher Ebene wurden einige Regelungen zur Bereitstellung von Open Data getroffen. Teilweise wird bei diesen nicht der gleiche „offene“ Ansatz wie auf Bundesebene verfolgt, sondern es wird abschließend geregelt, welche Daten offengelegt werden müssen.[6] § 12a EGovG hingegen stellt auf erster Ebene den Grundsatz auf, alle Daten, die der genannten Gruppe unterfallen, zu veröffentlichen. Auf zweiter Ebene werden dann Ausnahmen von dieser Regel getroffen.
Die Modalitäten der Bereitstellung (also das „wie“) von Open Data auf nationaler Ebene regelt derzeit das Datennutzungsgesetz. Dieses übernimmt die oben dargelegten Vorgaben der OD-RL.

IV. Problemfelder

Die existierenden Regelungen hinterlassen einige allgemeine Problemfelder. So ist den dargestellten Definitionen nicht immer klar zu entnehmen, ob ein bestimmtes Datum eine der einschlägigen Kategorien erfüllt. Ohne eine klare Einordnung besteht die Gefahr, einer Bereitstellungspflicht nicht nachzukommen oder Daten „falsch“, also beispielsweise nicht im richtigen Format, zur Verfügung zu stellen. Zumal schon die Feststellung der Bereitstellungspflicht einen nicht zu unterschätzenden Verwaltungsaufwand bedeutet. Hinzu kommt die grundsätzliche Schwierigkeit, den Weg durch den nicht unerheblichen Regelungsdschungel der Open Data zu finden.

Weiterhin kann kritisiert werden, dass nur für eine sehr geringe Zahl von Daten bisher eine Bereitstellungspflicht besteht. Selbst der recht weitreichende § 12a EGovG hat zahlreiche Ausnahmen. So ist zwar umfassend geregelt, wie mit Daten zu verfahren ist, die bereits öffentlich zur Verfügung gestellt werden. Dass und welche Daten jedoch zur Verfügung gestellt werden müssen, besagen nur wenige Rechtsakte.

V. Fazit und Bedeutung für wissenschaftliche Einrichtungen

Die Regelungen zu offenen Verwaltungsdaten scheinen noch nicht vollständig ausgereift zu sein. Zur rechtssicheren Handhabung sind klare, verbindliche und einheitliche Regelungen notwendig. Dennoch verspricht der gesamte Open Data Bereich ein großes Potenzial, insbesondere auch für Hochschulen. Diese können von frei und einfach zugänglichen Datensätzen sowohl in Forschungsbereich, als auch im Rahmen der Ausbildung profitieren. Hochschulen selbst und andere wissenschaftliche Einrichtungen wie Archive, Museen und Bibliotheken sind bisher von einer Bereitstellungspflicht ausgenommen. In der Regel würden hier allerdings auch das Datenschutzrecht und Rechte des geistigen Eigentums im Weg stehen.

6 S. hierzu bspw.: Hamburgisches Transparenzgesetz (HmbTG).

Hamstern verboten

Die aktuelle Regelung zur Vorratsdatenspeicherung in Deutschland ist unzulässig

von Klaus Palenberg

Der Gerichtshof der Europäischen Union (EuGH, Urteil vom 20. September 2022 – C-793/19 und C-794/19 [verbundene Rechtssachen]) hat erneut ein Urteil zur Vorratsdatenspeicherung gefällt. Auch die derzeitige deutsche Regelung einer Pflicht zur anlasslosen Speicherung von Verkehrs-daten für Telekommunikationsanbieter ist unionsrechtswidrig. Nach diesem Urteil geht die grundsätzliche Diskussion um die Abwägung von Sicherheit und Datenschutz in eine neue Run-de. Die Bundespolitik ringt bereits seit Jahrzehnten um eine europa- und verfassungsrechtlich zulässige Lösung.

I. Der Hintergrund des Verfahrens

Die aktuelle Entscheidung ist nicht das erste Urteil zu einer deutschen Vorratsdatenspeicherung. Bereits 2010 erklärte das Bundesverfassungsgericht (BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08) eine erste Einführung einer Vorratsdatenspeicherung in den §§ 113a, 113b Telekommunikationsgesetz (TKG) i.V.m. § 100g Abs. 1 S. 1 Strafprozessordnung (StPO) für nichtig. Die Neuregelung des TKG aus dem Jahre 2015 (seit dem 01.12.2021 sind die Regelungen in den §§ 175 ff. TKG zu finden) hingegen beanstandete das Gericht zunächst sowohl 2016 (Beschlüsse vom 08.07.2016 – 1BvR 229/16 und 1 BvQ 42/15) als auch 2017 (Beschlüsse vom 26.03.2017 – 1 BvR 114/16 und 1 BvR 3156/15) nicht. Das BVerfG sah allein durch die Speicherung der Verkehrsdaten zur Bevorratung noch keine derart schwerwiegenden Nachteile für die Antragsteller und befand deshalb, dass eine Außervollzugsetzung des Gesetzes im Eilverfahren nicht erforderlich sei. Im Hauptverfahren liegt dahingegen noch keine Entscheidung vor, so dass die aktuellen Regelungen weiterhin Geltung besitzen, aber unklar ist, wie sie verfassungsrechtlich zu bewerten sind.

Im Jahr 2014 musste der EuGH (Urteil vom 08. April 2014 – C-293/12 und C-594/12)[1] zunächst über die Gültigkeit der EU-Richtlinie, die Mitgliedsstaaten zur Vorratsdatenspeicherung verpflichtete (RL 2006/24/EG), entscheiden. In der Folgezeit hatte er dann mehrere nationale Regelungen einer Vorratsdatenspeicherung zu beurteilen. Einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung erteilte der Gerichtshof dabei eine Absage. Auf dieser Grundlage setzte 2017 das Oberverwaltungsgericht Münster (Beschluss vom 22.06.2017 – 13 B 238/17)[2] die Verpflichtung zur Speicherung von Verkehrsdaten gegenüber einem der klagenden Provider aus. Die Bundesnetzagentur erklärte daraufhin, auch gegenüber anderen Providern, keine Maßnahmen zur Durchsetzung der Speicherverpflichtung zu treffen. Seitdem findet die Vorratsdatenspeicherung faktisch kaum noch statt. Da die Regelung dennoch weiterhin besteht, mussten sich auch in jüngerer Vergangenheit Verwaltungsgerichte damit befassen. Am 25.09.2019 legte schließlich das Bundesverwaltungsgericht (BVerwG, Beschlüsse vom 25.09.2019 – 6 C 12.18 und 6 C 13.18) die Regelungen der Vorratsdatenspeicherung dem EuGH vor.

II. Die Vorlagefrage

Die deutsche Regelung, in der für das Ausgangsverfahren anwendbaren Fassung, sieht in den § 113a ff. TKG (nun §§ 175 ff. TKG) vor, dass Erbringer öffentlich zugänglicher Telekommunikationsdienste verpflichtet sind, Verkehrsdaten für zehn Wochen und Standortdaten für vier Wochen zu speichern (§ 113b Abs. 1 TKG). Daten über aufgerufene Internetseiten und

1 Siehe hierzu auch Klein, DFN-Infobrief Recht 05/2014.

2 Siehe hierzu auch Baur, DFN-Infobrief Recht 10/2017.

Daten von E-Mail-Diensten dürfen jedoch nicht gespeichert werden (§ 113b Abs. 5 TKG). Auch können sich soziale oder kirchliche Telefonseelsorger in eine Liste bei der Bundesnetzagentur eintragen lassen, so dass deren Verbindungsdaten ebenfalls nicht gespeichert werden dürfen (§ 113b Abs. 6 TKG). Die gespeicherten Daten sind umfassend durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen (§ 113d Abs. 1 TKG) und auch der Zugang zu ihnen ist allein bei besonders schweren Straftaten möglich (§ 113c Abs. 1, 2 TKG i.V.m. §§ 100g, 101a StPO).[3]

Das BVerwG hatte Zweifel an der Vereinbarkeit der deutschen Regelung mit europäischem Recht, insbesondere auf Grund der bisherigen Rechtsprechung des EuGH. Das BVerwG legte deshalb dem EuGH die deutsche Regelung zur Vorabentscheidung vor. In einem Vorabentscheidungsverfahren stellt der EuGH die Vereinbarkeit oder Unvereinbarkeit nationaler Regeln mit europäischem Recht fest. Das vorlegende Gericht ist dann an die Entscheidung des EuGH gebunden und darf im Falle einer Unvereinbarkeit die nationale Regel nicht mehr anwenden.

III. Die Entscheidung

Der EuGH erteilt in seiner Entscheidung einer anlasslosen Vorratsdatenspeicherung erneut eine Absage. Dabei sieht er die vom BVerwG gesehenen Unterschiede der nationalen Regelungen als nicht bedeutend an, so dass die Argumentation bereits aus den vorangegangenen Entscheidungen bekannt ist. Der Grundsatz, nach dem Nutzer:innen elektronischer Kommunikationsmittel erwarten dürfen, dass ihre Nachrichten und die damit verbundenen Verkehrsdaten anonym bleiben und nicht gespeichert werden dürfe - es sei denn, sie haben in die Speicherung eingewilligt - bleibt bestehen. In wenigen Ausnahmefällen soll eine Vorratsdatenspeicherung hingegen zulässig sein. Diese Ausnahmen seien dann wiederum eng auszulegen. Der EuGH erkennt also an, dass es Zwecke gibt, zu deren Erfüllung eine Vorratsdatenspeicherung zulässig ist. Diese Zwecke listet der EuGH in seiner Entscheidung abschließend auf. Da mit der Speicherung somit konkrete Zwecke verfolgt werden, liegt dann eine gezielte Vorratsdatenspeicherung vor und eben keine anlasslose. Es werden nicht wahllos sämtliche Daten sämtlicher Nutzer:innen gespeichert, sondern jeweils immer auf Grund einer besonderen Lage, einer besonderen geografischen oder personellen Konstellation oder nur bestimmte Daten gespeichert. Auch das nachträgliche Speichern wegen konkreter Verdachtsmomente kann zulässig sein. Darüber hinaus soll eine Vorratsdatenspeicherung nicht möglich sein. In diesem Zusammenhang weist der EuGH auch nochmals daraufhin, dass die Verkehrs- und Standortdaten Informationen über eine Vielzahl von Aspekten des Privatlebens enthalten können, wodurch eine umfassende Profilbildung der Betroffenen möglich ist. Dieses Profil enthält dann ebenso sensible Informationen wie der Inhalt der Kommunikation selbst.

Auf der anderen Seite erkennt der EuGH aber auch die Verpflichtungen der Mitgliedstaaten an, ihre nationale Sicherheit zu bewahren und schwere Kriminalität zu bekämpfen. Dies gelte insbesondere für Straftaten gegen Minderjährige und andere schutzbedürftige Personen, die auch Maßnahmen zum Schutz des Privat- und Familienlebens erforderten.

Um zwischen diesen Interessen einen Ausgleich zu schaffen, dürfen die Mitgliedstaaten Regelungen zur Vorratsdatenspeicherung treffen, soweit diese sich u. a. auf das absolut Notwendige beschränken.

Eine allgemeine und unterschiedslose Speicherung der Daten auf Vorrat sei deshalb nur zum Schutz der nationalen Sicherheit möglich. Hierzu muss aber eine Lage einer realen und aktuellen oder vorhersehbaren Bedrohung für die nationale Sicherheit vorliegen. Dann, aber auch nur dann, darf eine zeitlich begrenzte Speicherung von Verkehrs- und Standortdaten erfolgen. Diese Daten dürfen, auch wenn sie zuvor rechtmäßig erhoben wurden, nicht zur Bekämpfung auch schwerer Kriminalität oder Verhütung ernster Bedrohungen verwendet werden, sondern allein, um die nationale Sicherheit zu bewahren.

Weitere Möglichkeiten einer Vorratsdatenspeicherung sieht der EuGH beispielsweise bei einer Unterscheidung nach personalen oder geografischen Kriterien, bei der Speicherung von IP-Adressen der Verbindungsquelle und Daten, die zur Identifikation der Nutzer:innen dienen. Schließlich lässt der EuGH auch das sogenannte quick freeze-Verfahren zu, bei dem bestimmte, bereits vorliegende Verkehrs- und Standortdaten nachträglich auf behördliche Anordnung länger als ursprünglich erlaubt gespeichert werden. Aber auch diese Verfahren erfordern materielle und prozedurale Voraussetzungen und wirksame Garantien zum Schutz vor Missbrauch.

3 Siehe hierzu auch Rennert, DFN-Infobrief Recht 03/2022.

Dies bedeutet für die deutsche Regelung, dass die derzeitige allgemeine und unterschiedslose Vorratsspeicherung nicht deshalb zulässig ist, weil sie bestimmte Daten ausspart und zeitlich beschränkt ist. Dadurch werde sie nämlich nicht zu einer gezielten Vorratsdatenspeicherung.

Zwar schließt sie die Speicherung des Inhalts der Kommunikation und Daten über aufgerufene Websites und E-Mails aus, aber diese Daten stellten nur einen Bruchteil der insgesamt verfügbaren Daten dar. Ebenfalls falle die Ausnahme für Telefonseelsorge angesichts gerade einmal 1.300 gelisteter Stellen nicht ins Gewicht. Vielmehr genügten auch die sonstigen zu speichernden Daten für eine umfassende Profilbildung aus.

Zwar fielen die Speicherfristen der deutschen Regelung deutlich kürzer aus als bei den bisher bewerteten nationalen Regelungen. Aber weder die Dauer der Speicherung noch die Art oder Menge der gespeicherten Daten spiele eine entscheidende Rolle, da dennoch sehr genaue Schlüsse auf das Privatleben möglich seien. Die Speicherung, für sich gesehen, ermögliche nämlich diese Schlüsse bereits.

Dahingegen sind Speicherungen der IP-Adresse der Quelle einer Verbindung unter gewissen Umständen zulässig. Diese sei nämlich teilweise der einzige Anhaltspunkt um schwere Straftaten, die im Internet begangen werden, aufklären zu können. Dabei geht es insbesondere um Fälle von Kinderpornografie, die größtenteils über das Internet verbreitet wird. In diesen Fällen überwiegt das Interesse an einer effektiven Strafverfolgung das Interesse der Betroffenen, anonym im Internet unterwegs zu sein. Dementsprechend sei es zum Beispiel auch zulässig, beim Kauf von SIM-Karten eine Identitätsprüfung zu verlangen. Wohingegen auch andere Ermittlungsinstrumente zur Verfügung stehen, seien diese vorrangig zu nutzen.

Auch zulässig können gezielte Vorratsspeicherungen sein, wenn sie den Kreis der betroffenen Personen personell oder geografisch beschränken. Auf Grundlage objektiver und nichtdiskriminierender Kriterien sei es möglich, Standort- und Verkehrsdaten bestimmter Personen, die in einem unmittelbaren Zusammenhang mit schweren Straftaten stehen oder standen, zu speichern. Ebenso sei dies für Orte möglich, an denen eine erhöhte Zahl schwerer Straftaten begangen wurde, wo sich viele Menschen aufhalten oder die strategisch von Bedeutung sind. Dies gilt beispielsweise für Flughäfen oder Bahnhöfe. Ob es auch weitere Kriterien für eine gezielte Vorratsspeicherung geben kann, lässt der EuGH an dieser Stelle bewusst offen, da er der Einschätzung des Gesetzgebers nicht vorgreifen möchte.

Zudem sei weiterhin eine umgehende Speicherungsanordnung (quick freeze) zulässig. Betreiber elektronischer Kommunikationsdienste dürfen gewisse Daten für eine gewisse Dauer speichern. Darunter fallen beispielsweise Daten, die zur Rechnungsstellung erforderlich sind. Auf diese Daten dürfen die Behörden wiederum unter bestimmten Umständen zugreifen. Damit diese Daten nicht gelöscht werden, bevor sie tatsächlich gebraucht werden, können die Behörden zur Aufklärung von schweren Straftaten oder zur Abwendung einer Gefahr für die nationale Sicherheit anordnen, sie über den ursprünglich zulässigen Zeitraum hinweg zu speichern. Diese Anordnungen können sich dann auch auf Daten anderer Personen als den Tatverdächtigen erstrecken, auch beispielsweise auf Daten der Opfer.

Konsequenterweise schließt der EuGH einen Zugang zu den Daten, die zur Bewahrung der nationalen Sicherheit allgemein und unterschiedslos gespeichert wurden, für Zwecke der Strafverfolgung aus. Wenn die Daten zu diesem Zweck nicht gespeichert werden durften, sie am Ende dann aber doch dazu genutzt werden dürften, unterliefe dies die Wirksamkeit des Speicherverbots. In diesem Zusammenhang betont der EuGH erneut, dass die nationale Sicherheit höherrangig im Vergleich zur Bekämpfung auch schwerer Kriminalität sei. Deshalb verbiete sich ein Zugriff auf diese Daten durch die Strafverfolgungsbehörden.

IV. Folgen der Entscheidung

Die Entscheidung kommt weder besonders überraschend noch liefert sie spektakuläre neue Hinweise zur Ausgestaltung einer Vorratsdatenspeicherung. Sie hat dennoch erhebliche Auswirkungen für die Bundespolitik. Sie muss sich erstens einigen, ob sie einen weiteren Versuch unternehmen möchte, eine Vorratsdatenspeicherung einzuführen und falls ja, muss sie darüber entscheiden, wie sie diese ausgestalten möchte. Von dieser Ausgestaltung hängt dann wiederum ab, ob eine Speicherverpflichtung auch Hochschulen betreffen wird. Es sind auch bereits erste Vorschläge aus dem Bundesjustiz- und –innenministerium gemacht worden. Bundesjustizminister Marco Buschmann spricht sich dabei für das quick freeze-Verfahren aus, wohingegen Bundesinnenministerin Nancy Faeser die Möglichkeit der Speicherung von IP-Adressen nutzen möchte.

Deshalb bleibt der altbekannte Zielkonflikt weiterhin bestehen: Wieweit darf eine Überwachung durch den Staat zur Aufklärung von Straftaten gehen? Diese Diskussion wird nicht nur im Bereich des Datenschutzes geführt, sondern auch an anderer Stelle, wie beispielsweise in Hinblick auf die körperliche Unversehrtheit bei Blutuntersuchungen.

Vor diesem Hintergrund verwundert es nicht, dass die Politik seit Jahren damit ringt, diesen Konflikt sowohl europa- als auch verfassungsrechtlich zulässig aufzulösen. Ein weiterer Versuch ist mit diesem Urteil gescheitert. Positiv hervorheben lässt sich, dass mit jedem neuen Urteil zu diesem Thema die Rahmenbedingungen klarer werden. So hat der EuGH verhältnismäßig deutlich benannt, welche Bedingungen eine zulässige Vorratsdatenspeicherung erfüllen muss und wo ihre Grenzen sind.

Selbst ist (nicht) die Kontrolle

Bußgeld gegen Berliner Unternehmen wegen fehlender Unabhängigkeit des Datenschutzbeauftragten

von Johannes Müller

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat ein Bußgeld in Höhe von 525.000 Euro gegen die Tochtergesellschaft eines Berliner Handelskonzerns verhängt.[1] Dieses wird mit einem bestehenden Interessenskonflikt des Datenschutzbeauftragten des Unternehmens begründet, da dieser selbst im Rahmen von Dienstleistungsgesellschaften maßgebliche Entscheidungen über die Verarbeitung personenbezogener Daten treffen würde.

I. Die Rolle des Datenschutzbeauftragten

Artikel 37 der Datenschutzgrundverordnung (DSGVO) begründet für unterschiedliche Einrichtungen, wie etwa auch öffentliche Stellen, die Pflicht einen Datenschutzbeauftragten zu benennen. Gemäß Art. 39 Abs. 1 DSGVO hat dieser unter anderem die Aufgabe, die Einrichtungen hinsichtlich ihrer datenschutzrechtlichen Pflichten zu beraten und die Einhaltung der Vorschriften der DSGVO zu überwachen. Art. 38 Abs. 3 DSGVO normiert die Unabhängigkeit des Datenschutzbeauftragten. Hiernach darf dieser keine Weisungen im Rahmen der Ausübung seiner Aufgaben erhalten. Darüber hinaus verpflichtet Art. 38 Abs. 6 S. 2 DSGVO die Einrichtungen dazu sicherzustellen, dass keine Interessenskonflikte zwischen der Tätigkeit einer Person als Datenschutzbeauftragter und anderen Aufgaben bestehen, die die Person neben der Tätigkeit als Datenschutzbeauftragter ausführt. Ein solcher Konflikt liegt insbesondere dann vor, wenn der Datenschutzbeauftragte seine eigene Arbeit überwacht. Dies kann passieren, wenn dieselbe Person in einer anderen Rolle relevante Entscheidungen zu datenverarbeitenden Tätigkeiten trifft und daher auch die Überwachung dieser Tätigkeit in den Aufgabenbereich derselben Person als Datenschutzbeauftragter fällt.

II. Bußgeldverhängung durch Berliner Datenschutzbeauftragte

In ihrer Begründung für die Bußgeldverhängung hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit das Bestehen eines solchen Interessenkonfliktes geahndet. Bei der Tochtergesellschaft eines Berliner E-Commerce-Konzerns wurde eine Person als Datenschutzbeauftragter beschäftigt, die selbst Geschäftsführer bei zwei Dienstleistungsgesellschaften war. Diese Gesellschaften haben im Auftrag desjenigen Unternehmens Daten verarbeitet, bei dem die Person als Datenschutzbeauftragter gearbeitet hat. So hat dieselbe Person einerseits Dienstleistungsgesellschaften, die Datenverarbeitungen vornehmen, geleitet und andererseits die Tätigkeiten dieser Gesellschaften überwacht. Hierin wurde eine Selbstkontrolle und damit ein Interessenskonflikt im Sinne des Art. 38 Abs. 6 S. 2 DSGVO gesehen. Nachdem die Berliner Aufsichtsbehörde im Jahr 2021 dem Unternehmen bereits eine Verwarnung erteilt hat und diese dennoch dem Datenschutzverstoß nicht abgeholfen hat, wurde ein Bußgeld in Höhe von 525.000 Euro verhängt. Bei der Bestimmung der Bußgeldhöhe wurde der dreistellige Millionenumsatz des E-Commerce-Konzerns, die bedeutende Rolle des Datenschutzbeauftragten sowie die Weiterbenennung trotz vorheriger Verwarnung berücksichtigt.

1 Pressemitteilung des Berliner Beauftragten für Datenschutz und Informationsfreiheit abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2022/20220920-BlnBDI-PM-Bussgeld-DSB.pdf (zuletzt abgerufen am 06.10.2022).

III. Relevanz für Forschungs- und Wissenschaftseinrichtungen

Auch wenn lediglich private Hochschulen und Forschungsstellen, die nicht öffentlich-rechtliche Einrichtungen sind, Adressaten von Bußgeldern sein können,[2] haben die Ausführungen zur Unabhängigkeit des Datenschutzbeauftragten allgemeine Relevanz. Gemäß Art. 37 Abs. 1 lit. a DSGVO trifft öffentliche Stellen, also auch öffentliche Universitäten, die Datenverarbeitungen ausführen, die Pflicht einen Datenschutzbeauftragten zu benennen. Dieser ist verpflichtet, die erforderliche Unabhängigkeit zu wahren. Universitäten haben ein Augenmerk darauf zu legen, dass dieser selbst keine relevanten datenschutzrechtlichen Entscheidungen trifft, zu deren Überwachung er als Datenschutzbeauftragter verpflichtet ist.

2 Uphues, Kuschelkurs hat ausgedient, DFN-Infobrief Recht 04/2019; John, Unus pro omnibus, omnes pro uno, DFN-Infobrief Recht 05/2022; Müller, Bußgeldberechnung für Dummies, DFN-Infobrief Recht 10/2022.

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