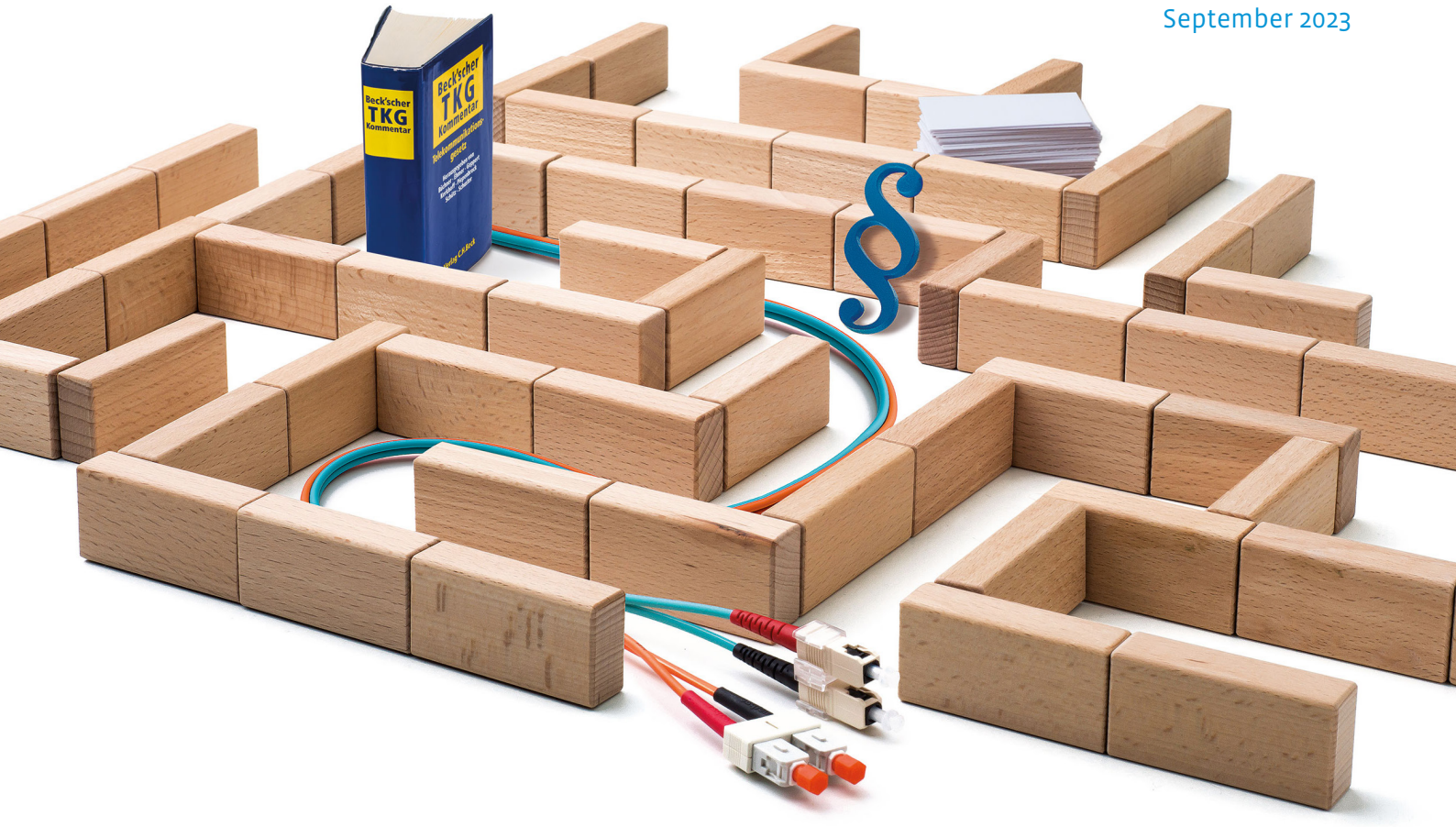
„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

9/2023
September 2023



Cyber Angriff ade mit dem CRA-E?

Die EU-Kommission schlägt zur Verbesserung der IT-Sicherheit den Cyber Resilience Act vor

von Klaus Palenberg

Im Zuge ihrer Digitalstrategie veröffentlichte die Europäische Kommission im Herbst 2022 einen Entwurf für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen oder kurz Cyberresilienzverordnung (Cyber Resilience Act [CRA]).[1] Im Juni 2023 haben das Europäische Parlament und der Rat der Europäischen Union eine vorläufige Einigung über den Entwurf erzielt. Der CRA soll die Cybersicherheit von in der EU vertriebenen digitalen Produkten durch eine sektorübergreifende Regulierung verbessern. Wie dies gelingen soll, welche Ansätze verfolgt werden und inwieweit Hochschulen betroffen sein werden, wird im Folgenden erörtert.

I. Ziel des Gesetzgebungsverfahrens

Es wird mittlerweile[1] gebetsmühlenartig wiederholt, jedoch mindert dies nicht den Wahrheitsgehalt der Aussage: Die Gefahr von Cyberangriffen ist erheblich. Sowohl Hardware- als auch Softwareprodukte sind zunehmend Gegenstand erfolgreicher Cyberangriffe. Jährlich entstehen so weltweit durch Cyberkriminalität geschätzt Kosten von 5,5 Billionen Euro.[2] Einfallstor für die Angreifer sind dabei meist Produkte mit digitalen Elementen. Diese weisen häufig zu wenige oder unzureichende Maßnahmen der Cybersicherheit auf. Fatalerweise werden regelmäßige Sicherheitsupdates entweder gar nicht angeboten oder nicht durchgeführt oder die technischen Komponenten sind schlicht von vorneherein nicht ausreichend gegen Angriffe abgesichert. Digitale Produkte bergen somit erhebliche Gefahren für die IT-Sicherheit und verursachen sowohl für Unternehmen als auch für Verbrauchende einen immensen (wirtschaftlichen) Schaden.

Als Reaktion auf diese Problematik veröffentlichte die Europäische Kommission im Herbst 2022 einen, bereits im Jahr 2021 angekündigten, Verordnungsentwurf für einen Cyber Resilience Act. Durch diesen soll die Cybersicherheit von in der EU vertriebenen digitalen Produkten einheitlich und horizontal reguliert werden. Konkret sollen sektorübergreifend alle Produkte mit digitalen Elementen erfasst werden. Das heißt, sämtliche Produkte, die bestimmungsgemäß oder vernünftigerweise vorhersehbar dazu benutzt werden können, eine Datenverbindung zu einem Gerät oder einem Netzwerk aufzubauen (Art. 2 I CRA-E). Insofern weist die Verordnung einen sehr weiten Anwendungsbereich auf. Es dürften somit jede Software, jedes Smartphone, jeder PC, aber auch smarte Geräte wie Kühlschränke oder Waschmaschinen, kurz jedes erdenkliche vernetzte digitale Produkt von den Regelungen des Cyber Resilience Act in unterschiedlicher Ausprägung betroffen sein.[3]

---

1 Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (zuletzt abgerufen am 01.08.2023).

2 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (zuletzt abgerufen am 01.08.2023).

3 Rennert, Mehr Cybersicherheit für vernetzte Produkte: Der Vorschlag der EU-Kommission für einen „Cyber Resilience Act“, ZfDR 2023, 206 (209).

II. Cyber Resilience Act

1. Bisherige Cybersicherheitsregulierung in der EU

Der Cyber Resilience Act reiht sich dabei in eine ganze Reihe europäischer Gesetzgebungsverfahren ein, die zu einer Stärkung der Cybersicherheit führen sollen. Bislang kamen hier hauptsächlich die NIS-RL[4] zum Schutz für elektronische Kommunikationsnetze und ihre Nachfolgerin, die NIS2-RL[5] zum Tragen.[6] EU-weit wird die Cybersicherheit darüber hinaus durch den Rechtsakt zur Cybersicherheit[7] und die EU-Infrastrukturschutz-RL[8] geregelt. Zwar wurden somit auf europäischer Ebene bereits eine Reihe von harmonisierenden Rechtsakten geschaffen, die das Sicherheitsniveau für digitale Produkte und digitale Kommunikation teilweise erhöhen sollen. Die große Schwäche der vielen verschiedenen Teilregelungen ist jedoch, dass sie ausschließlich punktuell schützen. So schützen die NIS-Richtlinien oder die EU-Infrastrukturschutz-RL beispielsweise ausschließlich den Bereich der kritischen Infrastrukturen. Eine effektive sektorübergreifende Regulierung fehlt aber bislang. Diesen Missstand soll nun der Cyber Resilience Act beseitigen.

2. Anwendungsbereich des Cyber Resilience Act

Durch den Cyber Resilience Act werden deshalb alle vernetzten Produkte mit digitalen Elementen erfasst. Vom Anwendungsbereich der Richtlinie umfasst sind alle Software- oder Hardwarekomponenten, die separat auf den Markt gebracht werden und mit einem Netzwerk oder anderen Geräten verbunden sind. Ausgenommen wird lediglich „freie und quellenoffene Software, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt wird“ (Erwägungsgrund 10), meist also wohl sog. „Open-Source-Software“. Ebenfalls sollen für solche Produkte keine weiteren Verpflichtungen entstehen, für die bereits spezifische Regelungen auf Grundlage anderer Rechtsakte, wie beispielsweise den oben genannten, vorhanden sind. Dies gilt insbesondere im medizinischen und verkehrstechnischen Sektor.

Doch sollen nicht für alle von der Verordnung erfassten digitalen Produkte dieselben Sicherheitsanforderungen gelten. Vielmehr werden verschiedene Sicherheitsstufen, namentlich kritische Produkte mit digitalen Elementen und hochkritische Produkte mit digitalen Elementen, eingeführt. Für sie gelten zusätzlich erhöhte Sicherheitsanforderungen. Für kritische Produkte mit digitalen Elementen findet sich im Anhang der Verordnung eine Festlegung von typischen, von der Definition erfassten, Produktkategorien aufgeteilt in zwei Klassen. Umfasst sind beispielsweise Passwort-Manager, Produkte mit der Funktion eines virtuellen privaten Netzes (VPN), industrielles Internet der Dinge-Geräte (IIoT), aber auch (virtuelle) Betriebssysteme für Desktop-Computer und mobile Endgeräte. Für sie gelten besondere Konformitätsbewertungsverfahren.

Für hochkritische Produkt mit digitalen Elementen fehlt eine solche Auflistung hingegen. Diese sollen, wenn sie ein bestimmtes Cybersicherheitsrisiko bergen, von der Kommission gesondert festgelegt werden. Erfasst werden sollen hier z. B. Produkte, die von wesentlichen Einrichtungen, die in der NIS2-RL aufgezählt sind, genutzt werden oder für die Widerstandsfähigkeit der gesamten Lieferkette von Produkten mit digitalen Elementen gegen Störungen von Bedeutung sind. Bei dieser Kategorie von Produkten wird dann ein Cybersicherheitszertifikat notwendig sein.

Konkret verpflichtet der Cyber Resilience Act auch Importeure und Vertreiber, aber vor allem natürlich Hersteller solcher

4 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

5 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.

6 Hierzu bereits ausführlich: John, „CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?“ in DFN-Infobrief Recht 04/2023.

7 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013.

8 Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

Produkte. So werden konkrete Sicherheitsanforderungen für digitale Produkte insbesondere im Anhang I festgelegt, die die Hersteller zwingend zu berücksichtigen haben. Außerdem müssen Risikoanalysen durchgeführt werden, um die Cybersicherheit des Produktes sicherzustellen. Ebenso werden die Hersteller verpflichtet, Sicherheitslücken effektiv zu beheben. Konkret wird ihnen beispielsweise hierfür aufgegeben, für die Lebensdauer des Produktes, mindestens aber für fünf Jahre, Sicherheitsupdates für das digitale Produkt bereitzustellen. Außerdem müssen sogenannte Konformitätsbewertungsverfahren (Art. 24 CRA-E) durchgeführt werden, es werden Informationspflichten (Anhang II) eingeführt und bei entdeckten Sicherheitslücken bestehen Berichtspflichten an die jeweils zuständigen Stellen.

Sollte den Verpflichtungen durch den Hersteller, Importeur oder Vertreiber nicht nachgekommen werden, drohen laut Art. 53 CRA-E Bußgelder in Höhe von 15 Mio. Euro oder alternativ 2,5 Prozent des weltweiten Vorjahresumsatzes. Außerdem besteht eine Rückrufbefugnis der Aufsichtsbehörden für Produkte, die nicht im Einklang mit den Vorschriften des Cyber Resilience Act stehen und daher ein erhebliches Cybersicherheits-Risiko oder eine Gefahr für die Gesundheit oder Sicherheit von Personen darstellen (Art. 45 CRA-E i.V.m. Erwägungsgrund 59).

Wer Hersteller ist, ergibt sich nach Art. 3 Nr. 18 CRA-E. Demnach wird ein Hersteller definiert als eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter eigenem Namen oder eigener Marke vermarktet, sei es entgeltlich oder unentgeltlich. Somit tritt neben die eigentliche Herstellung noch eine zweite Variante, nämlich die Vermarktung. Damit sind auch solche Akteure gemeint, die fremde Produkte unter eigenem Namen anbieten.

Bei Herstellern ergeben sich die obengenannten Pflichten, wenn sie das jeweilige Produkt „in Verkehr bringen". Das ist nach Art.3 Nr. 22 CRA-E bei der erstmaligen Bereitstellung eines Produkts mit digitalen Elementen auf dem EU-Binnenmarkt der Fall. Dies wiederum liegt vor, wenn ein Produkt zum ersten Mal an einen Händler oder einen Endverbraucher geliefert wird. [9]

Bei den weiteren Akteuren kann auch eine „Bereitstellung auf dem Markt" ausreichen, was nach Art. 3 Nr. 23 CRA-E jede entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit sein kann.

3. Weiterer Gang des Gesetzgebungsverfahrens

Der Entwurf der Kommission ist zwischenzeitlich vom Europäischen Parlament und dem Rat der Europäischen Union geprüft worden. Am 26. Juni 2023 wurde auch eine vorläufige Einigung[10] zwischen diesen beiden Institutionen erzielt und am 19. Juli 2023 ein gemeinsamer Standpunkt der Mitgliedstaaten[11] veröffentlicht. Hierin finden sich einige Änderungen in den Details, wie eine im Vergleich zum Kommissionsentwurf vereinfachte Konformitätserklärung. Auf Basis dieser Entscheidungen beginnt nun das Trilog-Verfahren über die endgültige Fassung der Verordnung. Nach Inkrafttreten besteht voraussichtlich eine ein- bis zweijährige Übergangsfrist für die betroffenen Akteure.

III. Auswirkungen für Hochschulen

Auch Hochschulen dürften von den Regelungen des Cyber Resilience Act unmittelbar betroffen sein. Dabei kann der Hochschule sogar eine Doppelnatur zukommen, indem sie zugleich als Herstellerin digitaler Produkte als auch Nutzerin digitaler Produkte fungiert.

Soweit die Hochschulen selbst Produkte mit digitalen Elementen im Rahmen des Hochschulbetriebes oder auch zu Forschungszwecken herstellen bzw. entwickeln ist zudem noch ein „Inverkehrbringen" erforderlich. Grundsätzlich können somit auch

9 So der Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide") – 2022/C 247/01, S. 19 (verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022XC0629(04)&from=EN, zuletzt abgerufen am 01.08.2023).

10 Siehe die Pressemitteilung vom selben Tag, abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2023/06/26/cybersecurity-at-the-eu-institutions-bodies-offices-and-agencies-council-and-parliament-reach-provisional-agreement/ (zuletzt abgerufen am 01.08.2023).

11 Abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/ (zuletzt abgerufen am 01.08.2023).

digitale Produkte aus Hochschulhand unter den Anwendungsbereich des CRA fallen. Im Hinblick auf drohende Bußgelder ist dabei allerdings zu beachten, dass Art. 53 VIII CRA-E festlegt, dass jeder Mitgliedstaat Vorschriften darüber erlässt, ob und in welchem Umfang gegen Behörden und öffentliche Stellen Geldbußen verhängt werden können.

Vom Sinn und Zweck des Regelungsinhalts der Verordnung erscheint es grundsätzlich richtig, dass auch Hochschulen von den Regelungen des Cyber Resilience Act erfasst werden. Neben Bußgeldern besteht als weitere Sanktionsmöglichkeit nämlich die Befugnis der Aufsichtsbehörden einen Rückruf anzuordnen. Dieser sollte auch gegenüber Hochschulen durchgesetzt werden können, da sein Schutzzweck auf eine höhere Cybersicherheit abzielt. Die IT-Sicherheit kann auch durch digitale Produkte von Hochschulen gefährdet werden. Es ist daher davon auszugehen, dass auch Hochschulen als Hersteller von digitalen Produkten von den Regelungen des Cyber Resilience Act umfasst sein werden.

Besonders im Rahmen hochschulischer Tätigkeit ist die, bereits angesprochene, Bereichsausnahme für Open-Source-Software zu beachten. In jedem Fall nicht von dem Entwurf erfasst werden „offen geteilte und frei zugängliche, nutzbare, veränderbare und weiterverteilbare Software, einschließlich ihres Quellcodes und ihrer veränderten Versionen“ (Erwägungsgrund 10). Wie weit diese Ausnahme allerdings genau reicht und ob auch von Unternehmen unterstützte Projekte erfasst sind oder ob Open-Source-Software als fester Bestandteil eines weiteren digitalen Produkts unter die strengen Regelungen des CRA fallen soll, ist derzeit noch unklar.

Betriebsratsmitglieder als Datenschutzbeauftragte? „Nein!? Doch! Ohh!“

Dürfen Betriebsratsmitglieder zugleich betriebliche Datenschutzbeauftragte sein, oder handelt es sich hierbei um einen Interessenkonflikt?

von Ole-Christian Tech

Bereits 2011, also deutlich vor Inkrafttreten der Datenschutzgrundverordnung (DSGVO), war eine Frage unter Arbeitsrechtlern heftig umstritten: Dürfen betriebliche Datenschutzbeauftragte (DSB) zugleich dem Betriebsrat angehören? Der Gerichtshof der Europäischen Union (EuGH) gibt (keine) Antworten im EuGH (6. Kammer) Urteil vom 9. Februar 2023 - C-453/21 (X-FAB). Gleichwohl sieht das Bundesarbeitsgericht (BAG) in seiner jüngsten Entscheidung (BAG 6.6.2023 - 9 AZR 383/19) die Frage nun eindeutig beantwortet. Unter der Rechtslage des bis zur DSGVO geltenden Bundesdatenschutzgesetzes (BDSG alt) wurde diese Frage zunächst durch das BAG im Urteil vom 23. März 2011 - 10 AZR 562/09 bejaht. Keine sieben Jahre später stellte sich die gleiche Frage – nun unter Geltung der DSGVO – erneut in einem Verfahren vor dem Arbeitsgericht Dresden (ArbG Dresden, 27.6.2018 - 10 Ca 234/18), das schließlich nach der Durchführung eines Vorlageverfahrens durch das BAG dazu führte, dass in der Doppelbesetzung ein Interessenkonflikt erkannt wurde.

I. Was ist das Problem?

Im Kern geht es um die Frage, ob die Interessen des Datenschutzbeauftragten grundsätzlich derart inkompatibel mit denen des Betriebsrats als Vertreter der Arbeitnehmer sind, dass dieser Konflikt einen „wichtigen Grund“ i.S.d. Bundesdatenschutzgesetzes BDSG (neu) darstellt und somit eine Abberufung nach § 6 Abs. 4 BDSG i.V.m § 626 Bürgerliches Gesetzbuch (BGB) rechtfertigt (so in dem Verfahren vor dem Arbeitsgericht Dresden) bzw. bereits einer erstmaligen Benennung nach § 5 Abs. 1 BDSG (für öffentliche Stellen wie etwa staatliche Hochschulen) bzw. § 38 Abs. 1 BDSG (für nicht-öffentliche Stellen) als Datenschutzbeauftragten im Wege steht.[1]

§ 626 BGB stellt einen allgemeinen Rechtsgrundsatz dar, der es erlaubt jedes Dauerschuldverhältnis- also auch Arbeitsverträge- aus einem wichtigen Grund auch vor Ablauf etwaiger Fristen zu kündigen.[2] Im Arbeitsrecht bietet § 626 BGB die Grundlage für die sog. außerordentliche Kündigung und wird in der Praxis eng ausgelegt, sodass an den „wichtigen Grund“ hohe Anforderungen zu stellen sind.

1 Vertiefend hierzu Müller, Selbst ist (nicht) die Kontrolle, DFN-Infobrief Recht 11/2022;
Auf europäischer Ebene läuft dazu derzeit eine Prüfaktion des Europäischen Datenschutzausschusses (EDSA), der europaweit die Stellung und Aufgaben der Datenschutzbeauftragten begutachtet und vergleicht https://edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en.

2 Vossen in: Ascheid/Preis/Schmidt, Kündigungsrecht 6. Auflage 2021, § 626 Rn. 6.

§ 6 Abs. 4 BDSG regelt die zulässige Abberufung des Datenschutzbeauftragten und verweist hierfür auf den § 626 BGB als allgemeinen Rechtsgrundsatz. Somit ist auch für die Abberufung des obligatorischen Datenschutzbeauftragten ein wichtiger Grund erforderlich. Bei freiwillig berufenen Datenschutzbeauftragten ist § 6 Abs. 4 BDSG laut § 38 Abs. 2 BDSG nicht anwendbar, sodass hier für die Abberufung auch kein wichtiger Grund erforderlich ist.

In dem bereits beschriebenen Verfahren vor dem ArbG Dresden waren der Beklagte (der Arbeitgeber) und pikanterweise der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit der Auffassung, dass ein solcher Interessenkonflikt bestehe. Der Kläger wäre somit gar nicht erst wirksam als Datenschutzbeauftragter benannt worden, jedenfalls aber rechtgemäß abberufen worden.

Der Kläger hingegen, Betriebsratsvorsitzender bei der Beklagten und zugleich betrieblicher Datenschutzbeauftragter, wehrte sich gegen seine Abberufung und gewann in erster Instanz vor dem ArbG Dresden und sodann in zweiter Instanz die Revision vor dem Sächsischen Landesarbeitsgericht (LAG).
Hieraufhin legte der Arbeitgeber nun wieder Revision vor dem BAG in Erfurt ein, welches das Verfahren aussetzte und dem EuGH zur Vorabentscheidung vorlegte.

Ein Vorlageverfahren nach Art. 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ermöglicht es nationalen Gerichten, Fragen über die Auslegung von Unionsrecht und die Vereinbarkeit von nationalem Recht mit Unionsrecht an den EuGH zur Vorabentscheidung zu stellen. Ziel ist es, eine einheitliche Anwendung des Unionsrechts sicherzustellen und Rechtssicherheit für alle Beteiligten zu schaffen.

II. (Keine) Antwort vom EuGH

Die lang ersehnte Antwort des EuGHs (EuGH, 09.02.2023 - C-453/21) löste aber eher Ernüchterung aus: „Ob ein Interessenkonflikt (...) vorliegt, ist im Einzelfall auf der Grundlage einer Würdigung aller relevanten Umstände, insbesondere der Organisationsstruktur des Verantwortlichen oder seines Auftragsverarbeiters und im Licht aller anwendbaren Rechtsvorschriften, einschließlich etwaiger interner Vorschriften des Verantwortlichen oder des Auftragsverarbeiters, festzustellen."
Mit anderen Worten also: Es ist Aufgabe der nationalen Gerichte im Einzelfall zu entscheiden, ob ein Interessenkonflikt besteht oder nicht. Ein solcher kann aus der Personalunion aus Betriebsratsmitglied und Datenschutzbeauftragtem bestehen, muss es aber nicht.

III. Argumente für und wider

Nach welchen Vorgaben sollen sich verantwortliche Stellen bei der Benennung ihrer Datenschutzbeauftragten also nun richten? Hier eine kurze Erörterung:

1. Nach § 80 Abs. 1 Betriebsverfassungsgesetz (BetrVG) gehört die Überwachung des Arbeitnehmerdatenschutzes zu den allgemeinen Kontrollfunktionen des Betriebsrats. Eine dreigliedrige Kontrolle, bestehend aus Aufsichtsbehörde, Datenschutzbeauftragten und Betriebsrat, ist somit nicht gewährleistet, wenn der Datenschutzbeauftragte seine Beaufsichtigungs- und Kontrollbefugnisse auch gegenüber dem Betriebsrat auszuüben hat. Mangels dieser Trennung führen solche Doppelmandate also im Einzelfall womöglich dazu, dass es sich bei Datenschutzbeauftragten um „Richter in eigener Sache" handelt.

2. Die Einsichtsrechte des Datenschutzbeauftragten reichen in der Regel weiter als solche des Betriebsrats. Hier ist ein Betriebsratsmitglied, welches gleichzeitig Datenschutzbeauftragter ist, erheblich besser gestellt als ein „einfaches" Betriebsratsmitglied.

3. Generelle Interessenskonflikte bestehen anderorts durchaus und sind auch in der Rechtsprechung anerkannt. So ist etwa die Benennung des Leiters der IT, des Personalleiters oder des Vertriebsleiters generell unzulässig, da hier Interessenkonflikte als vorprogrammiert gelten.

4. Auch im Arbeitsrecht gibt es Beispiele für Interessenkonflikte, wie zum Beispiel bei einem Betriebsratsmitglied, das gleichzeitig Mitglied in der Jugend- und Auszubildendenvertretung ist. Deshalb ist ein solches Doppelmandat dort nicht möglich.

5. Es haben sich jedoch keine nennenswerten Unterschiede zu den Verfahren in der Vergangenheit hinsichtlich der Rollen des Betriebsrats und des Datenschutzbeauftragten ergeben. Das BAG stellte in einem Urteil vom 23.03.2011 fest, dass kein Interessenkonflikt besteht: „Ob

dem Datenschutzbeauftragten im Einzelfall mögliche Beaufsichtigungs- und Kontrollbefugnisse gegenüber dem Betriebsrat zukommen, kann dahingestellt bleiben. Auch als Mitglied des Betriebsrats kann ein Datenschutzbeauftragter diese Rechte ordnungsgemäß wahrnehmen, ebenso wie er sie als Arbeitnehmer gegenüber seinem Arbeitgeber wahrzunehmen hat. Eine generelle Unvereinbarkeit ist nicht anzunehmen."

6. Außerdem sind Abwägungen zur Feststellung von Interessenkonflikten die Regel, während generelle Interessenkonflikte die Ausnahme sind. In anderen Konstellationen ist dies möglich und üblich, zum Beispiel wenn ein Betriebsratsmitglied gleichzeitig Vertrauensperson für schwerbehinderte Menschen ist. Ein solches Doppelmandat ist also nicht grundsätzlich auszuschließen.

7. Der deutsche Gesetzgeber ist im BDSG und dem Verweis auf § 626 BGB deutlich über das von der DSGVO gesetzte Schutzniveau hinausgegangen. Eine vage und abstrakte Vermutung, dass ein Interessenkonflikt vorliegen könnte und dies einen wichtigen Grund im Sinne von § 626 BGB darstellt, widerspricht der üblichen Auslegung des § 626 BGB im Arbeitsrecht und würde den Zweck der gesetzgeberischen Entscheidung, den Datenschutzbeauftragten als besonders unabhängige Stelle im Unternehmen zu etablieren, untergraben.

8. Auch logisch betrachtet liegt diese Auslegung nahe: Der Datenschutzbeauftragte darf keine Aufgaben oder Pflichten übernehmen, die ihn dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten beim Verantwortlichen oder seinem Auftragsverarbeiter festzulegen, da er dann nicht mehr unabhängig überwachen könnte. Ob der Datenschutzbeauftragte als Betriebsrat diese Zwecke und Mittel der Verarbeitung festlegt, hängt von der jeweiligen Organisationsstruktur und der Realität im Betrieb ab und kann nicht generell festgestellt werden.

IV. Entscheidung des BAG

Das Bundesarbeitsgericht (BAG) hat sich nun mit der Entscheidung des EuGHs befasst und in einem aktuellen Urteil (BAG 6.6.2023 – 9 AZR 383/19) festgestellt, dass der Vorsitz im Betriebsrat typischerweise mit der Wahrnehmung der Aufgaben des Datenschutzbeauftragten unvereinbar ist, da diese Aufgaben typischerweise nicht von derselben Person ohne Interessenkonflikt ausgeübt werden können. Dies gilt zumindest für die herausgehobene Funktion des Betriebsratsvorsitzenden, während die Richter offenließen, ob dies auch für die übrigen Mitglieder des Betriebsrats gilt. Die Entscheidung steht somit im Widerspruch zur Entscheidung des EuGHs, der keine typische Unvereinbarkeit postulierte, sondern eine Einzelfallbetrachtung forderte, und weicht auch von der bisherigen Rechtsprechung des BAG (BAG 23.3.2011 - 10 AZR 562/09) ab.

Für die Praxis ist somit das Urteil des BAG maßgeblich, dass von einer typischen Unvereinbarkeit ausgeht. Dies gilt umso mehr, da das Arbeitsrecht noch stärker von höchstrichterlicher Rechtsprechung geprägt ist als andere Bereiche des Zivilrechts.

V. Personalrat = Betriebsrat?

Für Beschäftigte in öffentlichen Verwaltungen, einschließlich Anstalten und Körperschaften, entspricht der Personalrat dem Betriebsrat. Im Gegensatz zum Betriebsrat, der seine Aufgaben im BetrVG findet, ist das Personalvertretungsrecht in der Verwaltung Sache der einzelnen Bundesländer. Mit anderen Worten: Jedes Bundesland und auch der Bund selbst hat ein eigenes Personalvertretungsgesetz, das sich substanziell von den Gesetzen der anderen Länder unterscheidet.

Und genau hier liegt auch ein Problem für die Vergleichbarkeit von Betriebsrat und Personalrat: In Nordrhein-Westfalen hat die Personalvertretung eine sehr starke Stellung. Gemäß § 65 Abs. 4 des Personalvertretungsgesetzes NRW obliegt die Einhaltung des Datenschutzes dem Personalrat, und die getroffenen Maßnahmen müssen der Dienststelle mitgeteilt werden. Es gibt keine Beschränkung auf den reinen Beschäftigtendatenschutz. Daraus kann man schließen, dass der nordrhein-westfälische Gesetzgeber keinen Interessenkonflikt sieht. Ähnliches lässt sich aus § 72 Abs. 4 Nr. 6 des Personalvertretungsgesetzes NRW ableiten, wonach der Personalrat bei der Bestellung und Abberufung des Datenschutzbeauftragten mitbestimmt.
Im Gegensatz dazu steht Sachsen, in dessen Personalvertretungsgesetz (SächsPersVG) der Begriff Datenschutz nicht einmal auftaucht.

Auch der Bund regelt diese Frage in seinem Bundespersonalvertretungsgesetz (BPersVG) in § 69 BPersVG nicht eindeutig und

verlangt lediglich, dass die Dienststelle und der Personalrat sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften unterstützen, ohne dem Personalrat eine konkrete Aufgabe oder Kompetenz zuzuweisen.

Thüringen geht mit dem Thüringer Personalvertretungsgesetz (ThürPersVG) noch einen Schritt weiter. Während § 73 Abs.3 Nr. 1 in Verbindung mit § 72 Abs. 5 Satz 2 und 3 ThürPersVG ein ausdrückliches Mitbestimmungsrecht bei Fragen des Beschäftigtendatenschutzes einräumt, erteilt § 80 Abs. 1 Satz 1 ThürPersVG der Personalvertretung die Aufgabe, sich für die Wahrung des Datenschutzes in der Dienststelle einzusetzen und hierfür einen Datenschutzbeauftragten zu bestellen. Es gibt keine Beschränkung auf den Beschäftigtendatenschutz, im Gegensatz zu § 73 ThürPersVG. Dies lässt den Schluss zu, dass der Gesetzgeber auch hier keinen Interessenkonflikt sieht und dem Personalrat das umfassende datenschutzrechtliche Mandat des Datenschutzbeauftragten einräumt.

Kurz gesagt: Die Rechtslage zur Vereinbarkeit von Personalvertretung und Datenschutzbeauftragtem in Personalunion ist für Beschäftigte der Landes- und Bundesverwaltung deutlich komplexer, und das Urteil des BAG ist kaum übertragbar.[3]

VI. Relevanz für Hochschulen und praktische Empfehlung

Hochschulen und Forschungseinrichtungen, sowohl öffentliche als auch private, müssen einen Datenschutzbeauftragten benennen, und dies haben sie in der Regel bereits getan. Einige von ihnen können aufgrund ihrer privaten Rechtsform zusätzlich vor dem zuvor beschriebenen Problem stehen, dass der Datenschutzbeauftragte ein Mitglied des Betriebsrats ist. In diesem Fall sollte das Urteil des BAG nun berücksichtigt werden.

3 Hierzu auch der Bayerische Landesbeauftragte für den Datenschutz (BayLfD), der den Interessenkonflikt sieht und sich für eine Einzelfallbetrachtung ausspricht https://www.datenschutz-bayern.de/datenschutzreform2018/aki14.html.

Match David vs. Goliath: Underdog for the win!

Triumph des Bundeskartellamts über den Meta-Konzern vor dem EuGH

Von Johanna Voget

Bereits im September 2022 berichtete die Forschungsstelle Recht über den Rechtsstreit zwischen dem Bundeskartellamt und dem Meta-Konzern, über das der Europäische Gerichtshof (EuGH) in einem Vorlageverfahren zu entscheiden hatte.[1] Nun haben die Richter in Luxemburg Recht gesprochen: Der Digitalgigant wird in die Schranken gewiesen, während das Bundeskartellamt das Urteil stolz als „bahnbrechendes Signal für die Kartellrechtsdurchsetzung in der digitalen Wirtschaft" verbucht.[2] Dieser Beitrag widmet sich nun im Einzelnen der Entscheidung, ihrer Begründung und ihrer Auswirkungen auf das Geschäftsmodell von Meta.

I. Hintergrund und Verfahrensgeschichte

Vorab ein kurzer Rückblick auf den Streitgegenstand und den Verfahrensgang:
Im Jahr 2019 ging das Bundeskartellamt gegen Meta, im Wege der Untersagung der Zusammenführung von Nutzerdaten aus verschiedenen Quellen vor.[3] Die Nutzungsbedingungen von Facebook sehen nämlich vor, dass Meta alle Daten eines Nutzers, die über die konzerneigenen Dienste und Drittwebseiten generiert werden konnten, mit dem Facebook-Nutzerkonto zu einem einheitlichen Profil zusammenführen durfte. In der Praxis bedeutet das, dass die Daten die von Facebook-Nutzern generiert werden, wenn sie zum Beispiel auf anderen Websites surfen oder Instagram und WhatsApp verwenden, von Meta dazu benutzt werden, um Werbung, die die Nutzer auf Facebook angezeigt bekommen, auf deren Präferenzen zuzuschneiden. Das Bundeskartellamt, der nationale Hüter des Wettbewerbs, erkannte hierin einen Verstoß gegen die europäischen Datenschutzvorschriften. Für die Datenverarbeitung liege keine Rechtfertigung nach der Datenschutz-Grundverordnung (DSGVO) vor. Eine solche Zuordnung von Daten aus Drittquellen dürfe nach der Anordnung des Bundeskartellamts vielmehr nur nach einer freiwilligen Einwilligung des Nutzers erfolgen. Durch die bisherige Praxis, die umfangreiche Sammlung und Verknüpfung personenbezogener Daten ohne Zustimmung der Nutzer, habe Facebook jedoch gegen § 19 Abs. 1 Gesetz gegen Wettbewerbsbeschränkungen (GWB) verstoßen, und seine marktbeherrschende Stellung missbraucht. Aus diesem Verstoß leitete das Bundeskartellamt wiederum seine Zuständigkeit für ein Vorgehen gegen Meta ab.
Es folgte ein prozessuales Hin und Her auf verschiedenen Ebenen. Das Oberlandesgericht (OLG) Düsseldorf gab dem Meta-Konzern im Eilverfahren gegen die Anordnung des Bundeskartellamts zunächst Recht.[4] Das Bundeskartellamt legte gegen diese Entscheidung wiederum Beschwerde vor dem Bundesgerichtshof (BGH) ein, der den Beschluss des OLG im Sommer 2020 verwarf und den Eilantrag Metas zurückwies.[5]

---

1 Schaller, Bundeskartellamt vs. Meta: David gegen Goliath, DFN Infobrief-Recht 09/2022.

2 https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2023/04-07_2023_EuGH.html.

3 https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5.

4 OLG Düsseldorf - Beschluss vom 26. August 2019 - VI-Kart 1/19 (V), WRP 2019, 1333, S. 7 ff.

5 BGH – Beschluss vom 23. Juni 2020 – KVR 69/19; https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html Pressemitteilung.

Im Zuge des sich anschließenden Hauptverfahrens in der Sache vor dem OLG Düsseldorf legte dieses sodann dem EuGH einige streitentscheidende Fragen zur Auslegung vor.[6]
Unter anderem handelte es dabei um folgende Fragestellungen: Darf das Bundeskartellamt als Wettbewerbsbehörde Entscheidungen aufgrund von Verstößen gegen Datenschutzrecht treffen, obwohl nach der DSGVO die irische Datenschutzbehörde für die Ahndung von Verstößen von Meta gegen die Vorschriften der DSGVO zuständig wäre?
Kann sich der Datenverarbeiter bei der Datensammlung aus Drittquellen auf die Rechtfertigungstatbestände der Vertragserfüllung (Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO) oder der Erforderlichkeit zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO) berufen?
Und kann gegenüber einem marktbeherrschenden Unternehmen wie Meta eine wirksame (und freiwillige) Einwilligung erklärt werden?
Nun hat der EuGH am 04. Juli 2023 das mit Spannung erwartete Urteil gesprochen und die Fragen für den weiteren Verfahrensgang vor dem OLG Düsseldorf beantwortet.[7]

II. Die Entscheidung im Einzelnen

1. Zuständigkeit des Bundeskartellamts

In den Entscheidungsgründen wird einleitend klargestellt, dass jede Aufsichtsbehörde zur Erfüllung der ihr obliegenden Aufgaben im eigenen Mitgliedsstaat zuständig ist. Ausdrückliche Regelungen zum Verhältnis zwischen den nationalen Wettbewerbsbehörden und den Datenschutzaufsichtsbehörden gebe es nicht. Die Richter in Luxemburg betonen daher zunächst den allgemeinen Grundsatz, dass die Aufsichtsbehörden, die durch die DSGVO legitimiert werden, damit betraut sind, die Anwendung der DSGVO zu überwachen und zu harmonisieren sowie die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, während die Wettbewerbsbehörden Entscheidungen zu marktbeherrschenden Stellungen von Unternehmen treffen und dadurch sicherstellen sollen, dass der Markt und im Ergebnis auch die Verbraucher vor Verfälschungen geschützt werden.

Sodann stellt der EuGH jedoch fest, dass die Wettbewerbsbehörde in die Wertung der für die kartellrechtliche Prüfung maßgeblichen Gesamtumstände auch als Indiz mit einbeziehen könne, ob ein Verstoß gegen die DSGVO vorliegt. Dies könne sich nämlich maßgebend auf die Entscheidung auswirken, ob das Verhalten ein Mittel des normalen Wettbewerbs darstelle oder ein Missbrauch der marktbeherrschenden Stellung nach Art. 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) vorliege. Daher könne die Wettbewerbsbehörde, trotz ihrer anderen Zielrichtung, in solchen Fällen neben den Datenschutzbehörden tätig werden. Dabei seien wiederum Maßnahmen zu unterlassen, die der Verwirklichung des EU-Rechts entgegenstehen können (Art. 4 Abs. 3 des Vertrags über die Europäische Union (EUV), sog. „effet utile“). Damit bestätigt der EuGH die Zuständigkeit des Bundeskartellamts zur Prüfung der datenschutzrechtlichen Verstöße im Rahmen der Bewertung der marktbeherrschenden Stellung und das damit verbundene Vorgehen gegen Meta.

Der EuGH verweist indes jedoch auch ausdrücklich auf das potenzielle Erfordernis einer Kooperation: im Zweifelsfall müssen sich die Behörden also miteinander abstimmen und nur soweit die zuständigen Datenschutzaufsichtsbehörden nicht innerhalb einer angemessenen Frist antworten oder sich mit der Prüfung durch die Kartellbehörde einverstanden erklären, dürfe diese den Sachverhalt eigenständig bewerten. Habe eine Datenschutzbehörde bereits eine bestimmte Praxis auf DSGVO-Konformität geprüft, dürfe sich das Kartellamt über diese Entscheidung nicht hinwegsetzen, sondern müsse die getroffene Beurteilungen im Rahmen der kartellrechtlichen Prüfung und Entscheidung übernehmen. Im Ergebnis stärkt die Entscheidung also die Befugnis zur Prüfung datenschutzrechtlicher Verstöße durch Kartellbehörden, und zeigt dieser Kompetenz zugleich aber auch klare Grenzen auf.

2. Rechtfertigung der Datenverarbeitung

Sodann widmet sich der EuGH dem Datenverarbeitungsmodell des Meta-Konzerns und der inhaltlichen Entscheidung des Bundeskartellamts. Eine abschließende Entscheidung über den

6 Vorabentscheidungsersuchen des OLG Düsseldorf vom 22.04.2021, Rechtssache C-252/21 = BeckEuRS 2021, 738390.

7 https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=E3DD7AE8CDB8FA70A6691927B4DFCDA8?mode=DOC&pageIndex=0&docid=275125&part=1&doclang=DE&text=&dir=&occ=first&cid=2657915https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=E3DD7AE8CDB8FA70A6691927B4DFCDA8?mode=DOC&pageIndex=0&docid=275125&part=1&doclang=DE&text=&dir=&occ=first&cid=2657915.

Streitgegenstand beinhaltet das Urteil nicht, den Antworten auf die Vorlagefragen lassen sich jedoch Zweifel der Rechtmäßigkeit entnehmen.
Zu der Frage, ob sich Meta für die Datensammlung aus Drittquellen auf einen Rechtfertigungstatbestand berufen kann, weisen die Richter vorab darauf hin, dass die Erlaubnistatbestände zur Datenverarbeitung aus Art. 6 DSGVO grundsätzlich eng auszulegen sind.

a) Vertragserfüllung

Hinsichtlich einer möglichen Rechtfertigung der Datenverarbeitung durch den Zweck der Vertragserfüllung gem. Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO, stellt die Entscheidung zunächst deklaratorisch klar, dass die Datenverarbeitung für die Erfüllung des Hauptgegenstandes des Vertrags unerlässlich sein muss. Dabei müsse zwischen den verschiedenen Dienstleistungen, die der Vertrag zwischen Meta und dem einzelnen Nutzer beinhaltet, differenziert und für die jeweiligen Zwecke die Erforderlichkeit der Datenverarbeitung konkret geprüft werden. Der EuGH stellt hier fest, dass die Datenverarbeitung zum Zweck der Personalisierung im Rahmen der vertraglichen Dienstleistung des Anbietens eines sozialen Netzwerks nicht zwingend erforderlich oder unerlässlich ist. Auch der Einwand Metas, die Datenverarbeitung sei erforderlich, um eine durchgängige und nahtlose Nutzung aller Meta-Dienste (Instagram, WhatsApp, Facebook) zu gewährleisten, greife nicht durch. Praktisch sei es gar nicht erforderlich bei allen Diensten ein Konto zu unterhalten, die Dienste könnten auch einzeln und unabhängig voneinander genutzt werden, und jedes Produkt beruhe auf einem eigenen Vertrag. Im Ergebnis zeigt sich der EuGH mithin abgeneigt, eine Rechtfertigung aufgrund eines Erfordernisses zur Vertragserfüllung zu bejahen.

b) Wahrnehmung berechtigter Interessen

Sodann widmet sich der EuGH dem Rechtfertigungsgrund der Wahrung berechtigter Interessen des Verarbeiters oder eines Dritten (Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO). Entscheidend ist hierbei, ob die Datenverarbeitung hierzu erforderlich ist und die entgegenstehenden Interessen der Person, deren Daten geschützt werden, demgegenüber nicht überwiegen.

Derjenige, der sich auf berechtigte Interessen beruft, müsse der betroffenen Person bei der Erhebung der personenbezogenen Daten diese berechtigten Interessen mitteilen. Darüber hinaus könne dieser Rechtfertigungsgrund nur zum Tragen kommen, sofern keine anderen Mittel zur Wahrung der Interessen in Betracht kommen, die weniger stark in die Rechte der betroffenen Person eingreift. In diesem Zusammenhang sei auch der Grundsatz der Datenminimierung zu berücksichtigen.

Meta berief sich konkret auf drei berechtigte Interessen: Personalisierung, Netzsicherheit und Produktverbesserung.
Des Weiteren hatte das OLG Düsseldorf im Rahmen der Vorlage auch eine Einschätzung des EuGH zum berechtigten Interesse an der Information der Strafverfolgungs- und –vollstreckungsbehörden erfragt.

Für das Überwiegen der Interessen der betroffenen Person gegenüber dem erstgenannten Interesse der Personalisierung spreche nach Ansicht des EuGH, dass Nutzer sozialer Netzwerke trotz der Unentgeltlichkeit der Nutzung nicht damit rechnen müssen, dass ihre Daten auch ohne Einwilligung genutzt werden, um personalisierte Werbung zu schalten. Diese Feststellung werde zusätzlich durch den nahezu unbegrenzten Umfang der Datenerhebung und das Potential, beim Nutzer ein Gefühl des „Überwachtwerdens“ auszulösen, gestützt.

Bezüglich des zweitgenannten Grundes, der Netzsicherheit, erklärt die Entscheidung, dass dieser zwar grundsätzlich ein berechtigtes Interesse darstellt. Sodann stellen die Richter jedoch in Frage, ob nicht mildere Mittel als die konkrete umfangreiche Datenverarbeitung in Betracht kommen, was darauf hindeutet, dass auch die Netzsicherheit als berechtigtes Interesse nicht zur Rechtmäßigkeit der Datenverarbeitung gereichen kann.
Auch hinsichtlich des dritten Rechtfertigungsversuchs, mit dem Zweck der Produktverbesserung, meldet der EuGH erhebliche Zweifel an. Vielmehr klingt an, dass angesichts des erheblichen Umfangs der Datenverarbeitung die Interessen des betroffenen Nutzers gegenüber dem kommerziellen Ziel Metas zur Produktverbesserung überwiegen.

Zuletzt erteilt der EuGH dem berechtigten Interesse der Information der Strafverfolgungs- und –vollstreckungsbehörden eine Absage, da ein privates Unternehmen wie Meta, dessen kommerzielle Tätigkeit nicht mit der Erhebung solcher Daten zu solchen Zwecken zusammenhängt, sich nicht auf dieses Interesse berufen könne.

c) Wirksamkeit der Einwilligung gegenüber einem marktbeherrschenden Unternehmen

Zuletzt befasst sich der EuGH mit der Frage nach der Wirksamkeit der Einwilligung des Nutzers in die Datenverarbeitung. Sofern nämlich eine solche wirksame Einwilligung vorliegt, wäre eine Rechtfertigung nach den zuvor dargestellten und in ihrem Vorliegen bezweifelten Rechtfertigungstatbeständen gar nicht mehr erforderlich.

Dabei bildet die Prüfung der Freiwilligkeit der Einwilligung, die gemäß Art. 4 Nr. 11 DSGVO für die Wirksamkeit erforderlich ist, gegenüber einem marktbeherrschenden Unternehmen, wie Meta, den Kern der Feststellungen. Maßstab für die Beurteilung der Freiwilligkeit ist dabei zunächst, ob der Einwilligende eine Wahlfreiheit hat oder nicht in der Lage ist, ohne Nachteile die Einwilligung zu Verweigern oder zu widerrufen.

Der EuGH stellt hierzu fest, dass alleine das Vorliegen einer marktbeherrschenden Stellung nicht die Freiwilligkeit entfallen lässt. Es sei aber zu berücksichtigen, dass es in einem solchen Fall leichter ist, Bedingungen und Datenverarbeitungen festzusetzen, die zur Erfüllung des Vertrages nicht zwingend erforderlich seien und dadurch im Ergebnis die Wahlfreiheit des Nutzers beeinträchtigt werden könne. Den Nutzenden müsse daher für einzelne Datenverarbeitungsvorgänge konkret die Möglichkeit der Zustimmungsverweigerung eröffnet sein. In diesem Zusammenhang fordert der EuGH auch eine Trennung zwischen den innerhalb des konkreten sozialen Netzwerks erzeugten Daten und den außerhalb „Off-Facebook“ generierten und erhobenen Daten im Rahmen der Einwilligung.
Abschließend weist der EuGH noch einmal darauf hin, dass der Datenverarbeiter die Beweislast für die Wirksamkeit der Einwilligung (Art. 7 Abs. 1 DSGVO) und daher auch für die Freiwilligkeit trage.

III. Auswirkungen der Entscheidung

Nun hat das OLG Düsseldorf unter Berücksichtigung der Entscheidung des EuGH in dem laufenden Hauptsacheverfahren über den Sachverhalt zu entscheiden.
Dieses Urteil sowie bereits die der EuGH Entscheidung zu entnehmenden Feststellungen könnten sich sodann erheblich auf das Geschäftsmodell von Meta auswirken. Der umfangreichen Verarbeitung, insbesondere von außerhalb des sozialen Netzwerks Facebook generierten Daten, sowie der damit verbundenen Möglichkeit der Zusammenführung der Informationen und Erstellung eines umfassenden Nutzerprofils könnte damit ein Ende gesetzt werden. Meta dürfte gezwungen sein, seine Nutzungsbedingungen zu aktualisieren und der Einwilligung der Nutzenden mehr Bedeutung zu verleihen. Im Ergebnis stärkt die Entscheidung die Kompetenz der Kartellbehörden, weitet damit einhergehend auch die Relevanz der Prüfung der Vorschriften der DSGVO aus und kommt letztlich den einzelnen Nutzenden und Verbrauchern zugute, deren Daten bislang umfangreich gesammelt und zusammengeführt wurden.

IV. Bedeutung für Hochschulen und wissenschaftliche Einrichtungen

Das Verfahren und die daraus resultierenden rechtlichen Grundsätze zeitigen zwar keine unmittelbare Wirkung für Hochschulen und wissenschaftliche Einrichtungen. Dennoch ist der Datenschutz und die Begrenzung der Marktmacht von sog. Gatekeepern wie Meta, Google, Amazon und Co. für die Gesellschaft und jeden einzelnen von Relevanz. Die Auswirkungen der Entscheidung auf das Geschäftsmodell von Meta und anderen Digitalgiganten sind nun mit Spannung abzuwarten.

Kurzbeitrag: Zuerst ein Like des Personalrats

BVerwG zum Mitbestimmungsrecht des Personalrats bei der Einrichtung von Seiten auf sozialen Medien

von Johannes Müller

Das Bundesverwaltungsgericht (BVerwG) musste sich mit der Frage beschäftigen, ob dem Personalrat der Körperschaft Deutsche Rentenversicherung Bund ein Mitbestimmungsrecht bei der Entscheidung zukommt, ob auf sozialen Medien eine Seite oder ein Kanal mit einer Kommentarfunktion eingerichtet wird.

I. Mitbestimmungsrecht des Personalrats für technische Einrichtungen zur Beschäftigtenüberwachung

Gemäß § 80 Abs. 1 Nr. 21 BPersVG hat der Personalrat[1] ein Mitbestimmungsrecht bei der „Einrichtung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen."[2] Das Mitbestimmungsrecht des Personalrats dient dem Schutz des Persönlichkeitsrechts der Beschäftigen, das durch eine ständige technische Überwachung am Arbeitsplatz beeinträchtigt sein könnte.

Hierbei wird das Erfordernis, dass die Einrichtung zur Überwachung der Beschäftigten bestimmt sein muss, weit verstanden.

II. Die Auffassung des BVerwG zur Einschaltung des Personalrats für die Einrichtung von sozialen Medien

Ausgangspunkt des Urteils des BVerwG (Az. 5 P 16.21) waren die Seiten und Kanäle der Deutsche Rentenversicherung Bund bei Facebook, Instagram und Twitter, die der Rentenversicherungsträger etwa zur Presse- und Öffentlichkeitsarbeit, aber auch zur Personalgewinnung nutzt. Die erstellten Beiträge können Nutzer kommentieren und dabei auch das Verhalten oder die Leistung einzelner Beschäftigter thematisieren. Aufgrund der Kommentare, die auch für den Arbeitgeber einsehbar sind, könnte in den Seiten und Kanälen eine Einrichtung gesehen werden, die zur Überwachung von Beschäftigten bestimmt ist.[3]

In seinem Urteil stellte das BVerwG fest, dass bereits das Speichern von Nutzerkommentaren mit verhaltens- oder leistungsbezogenen Angaben als selbstständige (Überwachungs-)Leistung einer technischen Einrichtung anzusehen sei. Aus der grundsätzlich bestehenden Gefahr, dass die Dienststelle diese Daten auswerten könnte, ergebe sich aus der Sicht eines objektiven

1 Vgl. zum Verhältnis des Personalrats zum Datenschutzbeauftragten auch Tech, Betriebsratsmitglieder als Datenschutzbeauftragte? „Nein!? Doch! Ohh!", DFN-Infobrief Recht 09/2023.

2 Für die Beschäftigten der Deutschen Rentenversicherung Bund ist das Bundespersonalvertretungsgesetz einschlägig. Hochschulen unterliegen regelmäßig dem jeweiligen Landespersonalvertretungsrecht. Hier bestehen inhaltlich vergleichbare Regelungen, etwa für NRW in § 72 Abs. 3 Nr. 2 LPVG NRW.

3 Vgl. zur gleichen Problematik bei Betriebsräten Sporleder, Big Brother „LIKEs" watching you, DFN-Infobrief Recht 09/2015; Strobel, LIKE – aber bitte nur mit Zustimmung, DFN-Infobrief Recht 09/2017; Strobel, Gezwitschert wird auch nur mit Zustimmung, DFN-Infobrief Recht 03/2019.

Betrachters ein Überwachungsdruck bei den Beschäftigten. Für eine „Bestimmung“ zur Überwachung i. S. d. § 80 Abs. 1 Nr. 21 BPersVG reiche deshalb die objektive Eignung der Datenspeicherung zur Überwachung aus.
Eine solche objektive Eignung könne allerdings nicht abstrakt festgestellt werden, sondern hänge davon ab, wie hoch im konkreten Fall die Wahrscheinlichkeit sei, dass verhaltens- und leistungsbezogene Kommentare, die einen Überwachungsdruck erzeugen, eingestellt würden. Die Wahrscheinlichkeit für solche Kommentare könne insbesondere anhand des Auftritts der Dienststelle in den sozialen Medien bewertet werden. Bedeutsam sei, ob über die Kanäle über konkrete Beschäftigte und deren Tätigkeiten berichtet werde. Werde auf der Seite lediglich sachbezogen, ohne Bezug zu bestimmten Beschäftigten, informiert, bestehe regelmäßig eine geringe Wahrscheinlichkeit von Kommentaren mit Überwachungsdruck. Daneben sei aber auch das tatsächliche Nutzerverhalten relevant. Sofern im Verlaufe des Betriebs eine relevante Zahl an verhaltens- und leistungsbezogenen Kommentaren abgegeben würden, könne die Eignung zur Überwachung auch entgegen einer ursprünglichen Prognose bejaht werden. Würden Kommentare hingegen ohne vorherige Auswertung schnellstmöglich gelöscht, könne dies gegen eine Eignung zur Überwachung – und somit gegen ein Mitbestimmungsrecht des Personalrats bei der Einrichtung der Seite – sprechen.

Die Feststellung, ob im konkreten Fall auch tatsächlich eine erhöhte Wahrscheinlichkeit von Kommentaren mit Überwachungsdruck bestand, obliegt der niedrigeren Instanz des OVG Berlin-Brandenburg, an die das BVerwG die Sache zurückverwies.

III. Relevanz für wissenschaftliche Einrichtungen

Dem Urteil lassen sich wichtige Anhaltspunkte entnehmen, anhand derer wissenschaftliche Einrichtungen feststellen können, ob ihr Personalrat vor der Einrichtung einer Seite auf sozialen Medien eingeschaltet werden muss.[4] Für die Öffentlichkeitsarbeit von wissenschaftlichen Einrichtungen stellen soziale Medien häufig ein unverzichtbares Medium dar. Sollen die jeweiligen Seiten derart gestaltet werden, dass mit hoher Wahrscheinlichkeit Kommentare zu dem Verhalten und der Leistung von Beschäftigten abgegeben werden, sollte vor der Einrichtung die Zustimmung des Personalrats eingeholt werden.

4 Vgl. zu datenschutzrechtlichen Herausforderungen beim Betrieb von Fanpages auch Rennert, Ciao, Fanpages!, DFN-Infobrief Recht 04/2023.

Impressum

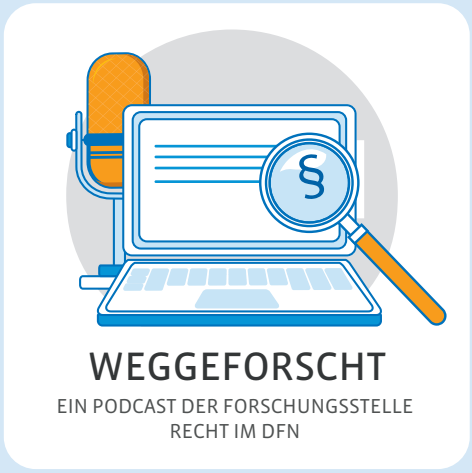
Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

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