NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

10 / 2022
Oktober 2022

Bußgeldberechnung für Dummies

EDSA veröffentlicht Leitlinien zur einheitlichen Bestimmung von Bußgeldern bei Verstößen gegen die DSGVO

Drum prüfe, wer sich online schindet

Ein Überblick über die Rechtslage bei Online-Prüfungen

Die Beschäftigung mit Beschäftigtendaten

Vorlagefragen des VG Wiesbaden an den EuGH stellen den Beschäftigtendatenschutz auf den Prüfstand

Kurzbeitrag: Post(ulation) aus Luxemburg

Der EuGH zur Prozessvertretung durch Hochschullehrer

Bußgeldberechnung für Dummies

EDSA veröffentlicht Leitlinien zur einheitlichen Bestimmung von Bußgeldern bei Verstößen gegen die DSGVO

von Johannes Müller

Im Rahmen der Verhängung von Bußgeldern wegen Datenschutzverstößen stehen den Aufsichtsbehörden hohe Ermessensspielräume zu, da die Datenschutzgrundverordnung (DSGVO) hier nur wenig konkrete Vorgaben reicht. Die vom Europäischen Datenschutzausschuss (EDSA) veröffentlichten Leitlinien sollen den Aufsichtsbehörden eine Orientierungshilfe bei der einheitlichen Bemessung von Bußgeldern geben. Hierzu haben sie überwiegend die Schwere des Verstoßes und den Umsatz eines Unternehmens zu berücksichtigen.

I. EDSA Leitlinien zur einheitlichen Berechnung von Bußgeldern innerhalb der EU

Der EDSA hat am 12.5.2022 eine erste Version von Leitlinien[1] verabschiedet, die nationale Aufsichtsbehörden dabei unterstützen sollen, im Sinne der DSGVO angemessene Bußgelder für Datenschutzverstöße zu verhängen. Zur Erstellung dieser Leitlinien wurde der EDSA unmittelbar durch Art. 70 Abs. 1 lit. k DSGVO beauftragt, die Veröffentlichung wurde dementsprechend mit Spannung erwartet. Bei der EDSA handelt es sich um eine Einrichtung der Europäischen Union, die durch Inkrafttreten der DSGVO geschaffen wurde. Der Ausschuss setzt sich aus den Leitungen der jeweiligen Aufsichtsbehörden aller Mitgliedsstaaten und dem europäischen Datenschutzbeauftragten zusammen. Er soll zu einer einheitlichen Anwendung der Vorschriften der DSGVO beitragen, hierzu soll er insbesondere den Austausch der nationalen Sicherheitsbehörden fördern. Zur Unterstützung einer einheitlichen Anwendung des DSGVO erlässt er unter anderem Stellungnahmen und Leitfäden. Mit den nun veröffentlichten Leitlinien möchte der EDSA den nationalen Aufsichtsbehörden eine Orientierungshilfe anbieten, die zu einer einheitlichen Bußgeldfestsetzung bei Datenschutzverstößen durch die nationalen Aufsichtsbehörden beitragen soll. Vergleichbare Unterstützungshilfen bei der Ermittlung von Bußgeldern existierten zuvor primär auf nationaler Ebene, etwa das Bußgeldkonzept der Datenschutzaufsichtsbehörden des Bundes und der Länder. Ausgangspunkt für die Berechnung von Bußgeldern bei Datenschutzverstößen stellt Art. 83 DSGVO dar. Dieser nennt zwar einzelne Kriterien, die bei der Bemessung von Bußgeldern zu berücksichtigen sind und gibt verschiedene Höchstgrenzen eines Bußgeldes an, konkrete Einordnungen von Datenschutzverstößen und Festlegungen von Bußgeldern ergeben sich hieraus allerdings nicht. Hierbei sollen nun die Leitlinien helfen.

II. Schrittweise Berechnung von Bußgeldern

Die Leitlinien nennen verschiedene Schritte, die bei der Ermittlung eines Bußgeldes durchlaufen werden müssen.

1. Konkurrenzen

Zunächst beschäftigen sie sich mit möglichen Konkurrenzen, also dem Verhältnis von mehreren Rechtsverstößen durch ein Unternehmen zueinander. Werden durch eine einzelne Handlung mehrere Verstöße gegen Datenschutzvorschriften begangen, so

1 In englischer Sprache abrufbar unter https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf - zuletzt abgerufen am 28.09.2022.

ist es zum einen möglich, dass die Anwendung einer (verstoßenen) Datenschutzvorschrift die Anwendung der weiteren ausschließt. In diesem Fall bemisst sich das Bußgeld allein anhand der noch anwendbaren Vorschrift, gegen die verstoßen wurde. Zum anderen ist es möglich, dass die Normen, gegen die verstoßen wurde, in Idealkonkurrenz zueinanderstehen, die Anwendung der einen Norm die andere also nicht ausschließt. In diesem Fall sind alle (verstoßenen) Datenschutzvorschriften bei der Bemessung des Bußgeldes zu berücksichtigen, hierbei darf das gesamte Bußgeld gemäß Art. 83 Abs. 3 DSGVO jedoch nicht die gesetzlich vorgesehene Höchstgrenze für den schwerwiegendsten Verstoß überschreiten. Liegen ohnehin mehrere Handlungen vor, die Datenschutzverstöße darstellen, werden auch mehrere Bußgelder verhängt

2. Schwere des Verstoßes

Als Ausgangspunkt der eigentlichen Berechnung der Bußgelder dienen nach dem Leitfaden die Höchstgrenzen der Bußgelder, die Art. 83 DSGVO für unterschiedliche Datenschutzverstöße vorsieht. Diese liegen abhängig von der Norm, gegen die verstoßen wurde, entweder bei 10 Millionen Euro (bzw. 2 Prozent des Jahresumsatzes, sofern dieser höher ist) oder bei 20 Millionen Euro (bzw. 4 Prozent des ggf. höheren Jahresumsatzes). In den meisten Fällen sind die absoluten Höchstgrenzen maßgeblich, da die relativen Werte erst bei Unternehmen mit besonders hohem Umsatz zum Tragen kommen. Im Rahmen der weiten Spannbreite eines möglichen Bußgeldes (0 bis 10 Millionen Euro bzw. 0 bis 20 Millionen Euro) nehmen die Leitlinien nun zunächst eine Eingrenzung in drei Kategorien anhand der Schwere des Verstoßes vor. Handelt es sich um einen leichten Verstoß soll sich zunächst für die Bußgeldhöhe eine Spannbreite von 0 bis 10 Prozent der Höchstgrenze nach Art. 83 DSGVO ergeben, bei einem mittleren Verstoß eine Spannbreite von 10-20 Prozent und bei einem schweren Verstoß eine solche von 20-100 Prozent der vorgesehenen Höchstgrenze. Zur Bestimmung der Schwere des Verstoßes nennen die Leitlinien als Kriterien mitsamt ausführlicher Erläuterung die Art, den Umfang (etwa länderübergreifend) und den Zweck der Datenverarbeitung, die Zahl der (tatsächlich oder potentiell) betroffenen Datensubjekte, die Art und das Ausmaß eines etwaigen entstandenen Schadens, die Dauer des Verstoßes, subjektive Merkmale des Datenverarbeiters (vorsätzliches oder fahrlässiges Handeln) und die Kategorie der betroffenen personenbezogenen Daten (etwa besonders sensible, in Art. 9 und 10 DSGVO genannte Daten). Punktuelle Einordnungen (z. B. bei mehr als 1.000 betroffenen Datensubjekten liegt ein mittlerer Verstoß vor) nehmen die Leitlinien nicht vor, solche könnten der Komplexität des individuellen Falles jedoch auch nicht gerecht werden. Als konkrete Anhaltspunkte können stattdessen die in den Leitlinien dargestellten ausführlichen Beispiele dienen, die verschiedene lebensnahe Fälle anhand der genannten Kriterien untersuchen und in eine der drei Kategorien einordnen. Aus diesen wird auch deutlich, dass ein Abwägen der verschiedenen Kriterien stattzufinden hat, und ein gegenseitiges Ausgleichen möglich ist.

3. Umsatz

Diese beschriebene Einordnung wird nun durch die Berücksichtigung des Umsatzes des Unternehmens ergänzt, um eine angemessenes Bußgeld zu erreichen, das der Größe des Unternehmens entspricht. Liegt der jährliche Umsatz unter 2 Millionen Euro, kann das Bußgeld auf 0,2 Prozent der vorher berechneten Spannbreite reduziert werden, bei einem Umsatz unter 10 Millionen Euro auf 0,4 Prozent und bei einem Umsatz unter 50 Millionen Euro ist eine Reduktion auf 2 Prozent der berechneten Spannbreite möglich. Bei einem Umsatz zwischen 50 Millionen und 100 Millionen Euro kann die Aufsichtsbehörde erwägen, das Bußgeld auf 10 Prozent, bei einem Umsatz zwischen 100 Millionen und 250 Millionen auf 20 Prozent und bei einem Umsatz über 250 Millionen Euro auf 50 Prozent zu reduzieren. Nicht ganz eindeutig kann aus den Leitfäden entnommen werden, ob sich die Reduktion auf die gesamte Spannbreite oder lediglich die untere Grenze bezieht. Im folgenden veranschaulichenden Beispiel wird angenommen werden, dass sich die Reduktion auf die gesamte Spannbreite bezieht:
Ein Unternehmen mit einem Umsatz von 30 Millionen Euro nimmt eine Datenverarbeitung unter Verstoß gegen Art. 6 DSGVO vor, der Verstoß wird von der zuständigen Aufsichtsbehörde als mittel schwer eingeordnet.
Art. 83 Abs. 5 DSGVO nennt für Verstöße gegen Art. 6 DSGVO als Höchstgrenze eines Bußgeldes den Wert von 20 Millionen Euro. Aufgrund der mittleren Schwere des Verstoßes ist nun zunächst von einer Spannbreite des Bußgeldes zwischen 2 Millionen und 4 Millionen Euro (10 bis 20 Prozent) auszugehen. Dieses kann nun aufgrund des Umsatzes, der zwischen 10 und 50 Millionen Euro liegt, auf bis zu 2 Prozent des Ausgangswertes reduziert werden. Hieraus ergäbe sich dann eine Spannbreite des Bußgeldes zwischen 40.000 und 80.000 Euro.

Zur korrekten Bestimmung des genauen Umsatzes eines Unternehmens treffen die Leitlinien in einem eigenen Kapitel Aussagen. Das Unternehmen selbst ist unter Zugrundelegung einer wirtschaftlichen und nicht juristischen Betrachtungsweise zu bestimmen. Auch mehrere selbständige juristische Personen können ein Unternehmen darstellen, sofern sie eine wirtschaftliche Einheit bilden. Den Umsatz eines Unternehmens definieren die Leitlinien als die Summe aller verkauften Waren und Dienstleistungen. Dieser soll der Gewinn- und Verlustrechnung entnommen werden, zu deren Aufstellung Unternehmen verpflichtet sind.

4. Erschwerende und mildernde Umstände

Zudem sollen individuelle Umstände berücksichtigt werden, die nicht bereits im Rahmen der Feststellung der Schwere des Verstoßes Eingang gefunden haben. Diese Umstände finden sich auch in Art. 83 DSGVO wieder. Sie können sich auf das zu verhängende Bußgeld sowohl erschwerend als auch mildernd auswirken. Als Beispiele können hierbei die Maßnahmen genannt werden, die der Datenverarbeiter vornimmt, um den Schaden zu verringern, das Vorkommen vorheriger Datenschutzverstöße oder ob die verarbeitende Person den Datenschutzverstoß freiwillig gemeldet hat. Die Leitfäden weisen hierbei ausdrücklich darauf hin, dass die zuständige Aufsichtsbehörde jeglichen erschwerenden oder mildernden Umstand zu berücksichtigen hat, auch wenn ein solcher Umstand nicht in den Leitfäden genannt wird.

5. Wirksamkeit, Verhältnismäßigkeit und Abschreckung

Die Leitlinien betonen wiederholt, dass sie keine rein mathematische Berechnung von Bußgeldern für Datenschutzverstöße bezwecken. Neben den genannten Kriterien, aus denen sich mögliche Spannbreiten für Bußgelder ergeben können, sollen alle Bußgelder unter Berücksichtigung der Gesichtspunkte der Wirksamkeit, Verhältnismäßigkeit und der abschreckenden Wirkung verhängt werden. Dies ergibt sich auch bereits aus Art. 83 Abs. 1 DSGVO. Ein Bußgeld ist wirksam, wenn der mit ihm befolgte Zweck erreicht wird. Im Rahmen der Verhältnismäßigkeit muss stets beachtet werden, dass das Bußgeld nicht höher ausfällt als es erforderlich ist, um die Ziele der DSGVO zu erreichen. Hierbei können in besonderen Fällen auch wirtschaftliche Gesichtspunkte eine Rolle spielen, eine schlechte finanzielle Lage allein soll jedoch nicht zur Reduktion des Bußgeldes führen. Maßgeblich für die abschreckende Wirkung ist nicht allein die Art und Höhe des Bußgeldes, sondern auch die Wahrscheinlichkeit, dass sie überhaupt verhängt wird und ein Datenschutzverstoß geahndet wird.

III. Relevanz der Leitlinien

Die Leitlinien stellen eine bloße Orientierungshilfe dar. Sie sind kein geltendes Recht und erzeugen keine unmittelbare Bindung für Aufsichtsbehörden oder Gerichte. Angesichts der Natur des EDSA als unmittelbar durch die DSGVO geschaffenes Gremium, das sich aus den Leitungen der Aufsichtsbehörden der Mitgliedstaaten zusammensetzt und der Tatsache, dass die DSGVO selbst den EDSA mit der Erstellung dieser Leitlinien beauftragt, ist ihnen dennoch eine hohe Relevanz beizumessen. Da die DSGVO ein einheitliches Datenschutzrecht in der Europäischen Union bezweckt, das auch eine einheitliche Verhängung von Geldbußen umfasst, ist davon auszugehen, dass die nationalen Aufsichtsbehörden sich nun primär hieran als Entscheidungshilfe orientieren. Entscheidet sich eine Aufsichtsbehörde in einem bestimmten Fall ein bestimmtes Bußgeld zu verhängen, bindet sie sich nun selbst. Hat sie später über einen vergleichbaren Fall zu entscheiden, muss sie auch eine vergleichbare Entscheidung wieder treffen, also ein vergleichbares Bußgeld erneut verhängen, sofern kein sachlicher Grund für eine abweichende Entscheidung besteht. So wird bei konsequenter Anwendung der Leitlinien durch die Behörden diesen auch eine immer höhere praktische Relevanz beigemessen.

IV. Ausblick und Bedeutung für die Hochschulen und wissenschaftliche Einrichtungen

Bei der ersten Version der veröffentlichten Leitlinien handelt es sich zunächst um eine Konsultationsfassung. Bis zum 27.6.2022 konnten etwa Unternehmen oder Branchenverbände Stellungnahmen hierzu einreichen. Es bleibt abzuwarten, ob in der nächsten Version signifikante Änderungen vorgenommen wurden. Wünschenswert wäre eine Klarstellung zu den Fragen, ob sich die umsatzbasierte Reduktion auf die gesamte Spannbreite der möglichen Geldbuße oder lediglich die Untergrenze bezieht.
Besondere Relevanz entfalten die Leitlinien für all diejenigen Einrichtungen, die aufgrund von Datenschutzverstößen Adressaten

von Bußgeldern sein können. Dies können grundsätzlich sowohl natürliche als auch juristische Personen sein, mit ersteren befassen sich die Leitlinien allerdings nicht. Bußgelder können allerdings nur gegen nichtöffentliche Stellen verhängt werden. Art. 83 Abs. 7 DSGVO hat zwar den einzelnen Ländern die Möglichkeit eröffnet, Bußgelder auch gegen öffentliche Stellen und Behörden zu regeln, von dieser Möglichkeit hat der deutsche Gesetzgeber jedoch keinen Gebrauch gemacht. Einrichtungen des öffentlichen Rechts können also nicht Adressat von Bußgeldern sein, hierzu zählen auch öffentliche Universitäten als Körperschaften des öffentlichen Rechtes. Etwas anderes gilt gemäß § 2 Abs. 5 BDSG lediglich dann, sofern die öffentlichen Stellen als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. [2]Im Regelfall gilt jedoch für wissenschaftliche Einrichtungen, dass primär nur private, nicht öffentlich-rechtliche organsierte Hochschulen oder sonstige private wissenschaftliche Einrichtungen bei Datenschutzverstößen mit Bußgeldern zu rechnen haben. Hier bestehen nun Anhaltspunkte, anhand derer sie eine eigene Einschätzung bezüglich der Höhe möglicher Bußgelder vornehmen können, nachdem sie selbst festgestellt haben, dass sie gegen DSGVO-Bestimmungen verstoßen haben. Ebenso fällt es nun leichter zu bestimmen, ob ein bereits verhängtes Bußgeld angemessen im Sinne der DSGVO oder zu hoch ist. Eine nun festgestellte starke Abweichung von den Leitlinien der EDSA könnte Anhaltspunkte dafür bieten, eine Entscheidung der Aufsichtsbehörde anzufechten und gerichtlich die Unverhältnismäßigkeit der Bußgeldhöhe feststellen zu lassen. In diesem Sinne sind die Leitlinien imstande, einen gewichtigen Beitrag zur Rechtssicherheit zu setzen.

2 Hierzu auch Uphues, Kuschelkurs hat ausgedient, DFN-Infobrief Recht 04/2019; John, Unus pro omnibus, omnes pro uno, DFN-Infobrief Recht 05/2022.

Drum prüfe, wer sich online schindet

Ein Überblick über die Rechtslage bei Online-Prüfungen

von Justin Rennert

Die Behörde der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen (LDI NRW) hat eine Handreichung zu Online-Prüfungen an Hochschulen veröffentlicht. Die Handreichung soll Hochschulen dabei helfen, Online-Prüfungen datenschutzkonform auszugestalten. Denn spätestens seit der Corona-Pandemie ist klar: Online-Prüfungen werden zukünftig zum Prüfungsalltag gehören wie der Kugelschreiber und die Packung Traubenzucker. Der vorliegende Beitrag fasst die Handreichung zusammen und gibt einen Überblick über die Rechtslage in allen Bundesländern.

I. Einleitung

Ungeachtet der weiteren pandemischen Entwicklung in diesem Herbst und Winter ist es für Hochschulen wichtig, einen datenschutzkonformen Einsatz von Prüfungstools zu gewährleisten. Die LDI NRW hat im Juli 2022 hierzu eine Handreichung veröffentlicht.[1] Als praktische Handreichung einer Aufsichtsbehörde haben die Hinweise keinen Gesetzesrang und sind nicht rechtsverbindlich. Jedenfalls für nordrhein-westfälische Hochschulen entfaltet die Handreichung allerdings trotzdem eine gewisse Bindungswirkung: Es ist damit zu rechnen, dass die LDI NRW ihre Aufsicht über die Prüfungspraxis der Hochschulen des Landes künftig entsprechend der Handreichung ausüben wird. Praktiken, von denen sie in der Handreichung ausdrücklich abrät, könnte sie künftig möglicherweise als Datenschutzverstoß verfolgen. Für Hochschulen außerhalb des Landes NRW bietet die Handreichung jedenfalls eine gewisse Orientierung. Die Rechtsunsicherheiten unter Prüfenden hinsichtlich des Einsatzes von Prüfungssoftware sind mancherorts groß. Die datenschutzrechtliche Praxis im einwohnerstärksten Bundesland ist als Orientierungspunkt nicht zu vernachlässigen.

II. Warum sind Online-Prüfungen datenschutzrechtlich relevant?

Im Rahmen von Online-Prüfungen verarbeiten Hochschulen eine Vielzahl personenbezogener Daten. Dazu gehören insbesondere der Name und die Matrikelnummer sowie Audio- und Videoaufnahmen der Studierenden. Häufig zwingen Online-Prüfungstools die Studierenden dazu, ihre Webcam dauerhaft angeschaltet zu lassen. Das dabei entstehende Live-Video des Oberkörpers der Studierenden ist durch das Recht am eigenen Bild in besonderer Weise verfassungsrechtlich geschützt. Die Verarbeitung personenbezogener Daten muss im Einklang mit der DSGVO erfolgen. Die Handreichung der LDI NRW zielt daher darauf ab, Konformität mit der DSGVO zu erzeugen.

Die DSGVO erlaubt Datenverarbeitungen nur dann, wenn sie sich auf einen Erlaubnistatbestand stützen. Internetnutzer kommen in der Regel bewusst nur mit dem Erlaubnistatbestand der Einwilligung in Berührung, also der ausdrücklichen Erklärung des von der Datenverarbeitung Betroffenen, mit der Datenverarbeitung einverstanden zu sein. Eine Einwilligung ist für Online-Prüfungen aber nicht ohne weiteres möglich. Denn die DSGVO verlangt, dass der Betroffene die Einwilligung „freiwillig“ erteilt. Eine Einwilligung ist nur dann freiwillig erteilt, wenn der Betroffene bei einer Verweigerung der Einwilligung

1 Handreichung zu Online-Prüfungen an Hochschulen, abrufbar unter: https://www.ldi.nrw.de/system/files/media/document/file/handreichung_online_pruefung.pdf - zuletzt abgerufen am 21. September 2022.

keine Nachteile befürchten muss. Damit ist eine Freiwilligkeit bei Online-Prüfungen meist nicht gegeben. Denn wenn der Studierende die Prüfung ansonsten gar nicht absolvieren könnte, so drohen ihm für seinen weiteren Studienverlauf erhebliche Nachteile, insbesondere eine Verlängerung der Studienzeit.

Damit müssen Hochschulen auf einen anderen Erlaubnistatbestand zurückgreifen. In Betracht kommt hier insbesondere Art. 6 Abs. 1 e) DSGVO. Dieser Tatbestand ist einschlägig, wenn die Verarbeitung „für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt". Hierfür müssen die Mitgliedstaaten allerdings noch eine zusätzliche Rechtsgrundlage schaffen. In Deutschland sind es die Länder, die für die Hochschulgesetzgebung zuständig sind. Nordrhein-Westfalen hat in seinem Hochschulgesetz eine solche Rechtsgrundlage geschaffen. § 64 Abs. 2 S. 2 des Hochschulgesetzes NRW erlaubt es den Universitäten selbst, in den Prüfungsordnungen Online-Prüfungen vorzusehen. Die Universitäten müssen dann in den Prüfungsordnungen allerdings auch Bestimmungen zum Umgang mit personenbezogenen Daten der Studierenden treffen. Anders als manch anderes Bundesland hat der nordrhein-westfälische Gesetzgeber den Erlaubnistatbestand also relativ abstrakt und knapp gehalten. Im Hochschulgesetz selbst finden sich keine Einschränkungen, wie mit den erhobenen Daten der Studierenden zu verfahren ist. Die Hochschulen sind bei Erstellung ihrer Prüfungsordnungen frei und könnten auch tiefgreifende Eingriffe in die informationelle Selbstbestimmung vorsehen, zum Beispiel die dauerhafte Speicherung von Video- und Audiomaterial der Studierenden auch über die Prüfung hinaus. Derart tiefgreifende Eingriffe stünden aber im Widerspruch mit der DSGVO. Die Handreichung der LDI NRW soll Hochschulen mithin insbesondere bei Erstellung der Prüfungsordnungen im Hinblick auf Online-Prüfungen eine Orientierung bieten. Nachfolgend werden die Empfehlungen der LDI NRW kurz vorgestellt.

III. Die Handreichung der LDI NRW

Kernstück der Handreichung ist die tabellenhafte Darstellung einzelner Prüfungsmodalitäten und ihre datenschutzrechtliche Beurteilung.

1. Authentifizierung der Prüflinge

Die Prüfung beginnt bei der Authentifizierung der Prüflinge mittels eines gültigen Lichtbildausweises. Die Authentifizierung muss zum Schutz der personenbezogenen Daten für jeden Prüfling einzeln unter Ausschluss der übrigen Prüflinge erfolgen. Eine Authentifizierung in einem Gruppen-Videocall hält die LDI NRW hingegen für unzulässig. Gleiches gilt für die Anfertigung von Screenshots vom Authentifizierungsprozess. Ebenso hält die LDI NRW den Einsatz von Gesichtserkennungssoftware zur Authentifizierung für unzulässig.

2. Video- und Audioüberwachung der Prüflinge

Die LDI NRW hält die Live-Überwachung der Studierenden für zulässig. Studierende dürfen also dazu verpflichtet werden, das Audio- und Videosignal ihres Endgerätes dauerhaft anzuschalten. Die Studierenden könnten auch, so die LDI NRW, dazu verpflichtet werden, sich und ihren Arbeitsplatz ständig sichtbar zu halten. Eine Aufzeichnung und Speicherung des Bild- und Tonmaterials hält die LDI NRW hingegen grundsätzlich für unzulässig, es sei denn, es besteht der Verdacht eines Täuschungsversuchs. Kommt beim Prüfungspersonal ein solcher Verdacht auf, so dürfen sie den weiteren Prüfungsverlauf aufzeichnen. Sie müssen die Prüflinge allerdings von der Aufzeichnung in Kenntnis setzen. Die Live-Überwachung hat durch menschliches Aufsichtspersonal zu erfolgen. Eine automatisierte Überwachung ist nach Einschätzung der LDI NRW nur bei Massenprüfungen zulässig. Einen verpflichtenden 360°-Schwenk durch die Prüfungsumgebung der Prüflinge hält die LDI NRW für unzulässig. Der Studierende kann hierzu nur bei Verdacht eines Täuschungsversuchs verpflichtet werden.

3. Sonstige technische Maßnahmen

Die LDI NRW hält es auch für zulässig, Prüflingen die Verwendung eines virtuellen Hintergrundes zu untersagen. Zudem dürfe das Prüfungspersonal mit technischen Mitteln die copy-and-paste-Funktion der Endgeräte der Studierenden deaktivieren. Gleiches gilt für die Rechtsklick-Funktion sowie die Möglichkeit zum Öffnen und Schließen von Browsertabs.

4. Möglichkeit der Präsenzprüfung für Studierende

Nach Einschätzung der LDI NRW sollte Studierenden die Wahlmöglichkeit verbleiben, auf die Online-Prüfung zu verzichten und die Prüfung stattdessen in den Räumlichkeiten der Hochschule zu absolvieren.

IV. Gesetzliche Vorschriften zu Online-Klausuren in den Bundesländern

Betrachtet man das gesamte Bundesgebiet, so wird eine Zweiteilung deutlich: Manche Bundesländer gewähren den Hochschulen wie das Land NRW relativ viel Autonomie und treffen abstrakte, knappe Vorgaben in ihren Hochschulgesetzen. Andere Bundesländer hingegen regeln die Datenverarbeitung und die Modalitäten von Online-Prüfungen detailliert in ihren Hochschulgesetzen oder entsprechenden Verordnungen. Nachfolgend findet sich eine übersichtsweise Darstellung der Regelungen in den übrigen 15 Bundesländern:

1. Baden-Württemberg:

In Baden-Württemberg erlaubt § 32a des Landeshochschulgesetzes seit dem 31. Dezember 2020 das Abhalten von Online-Prüfungen. Der Baden-Württembergische Gesetzgeber hat die Fernprüfungen somit relativ umfassend per Parlamentsgesetz geregelt. Die Hochschulen müssen die Online-Prüfung in ihren Prüfungsordnungen allerdings zusätzlich ausdrücklich vorsehen. Das Gesetz schreibt jeder Online-Prüfung zwingend eine Authentifizierung der Studierenden mit Lichtbildausweis vor. Aufgrund des Gesetzes können Studierende dazu verpflichtet werden, die Kamera- und Mikrofonfunktion ihres Computers zu aktivieren. Das Bild- und Tonmaterial kann sodann live durch das Aufsichtspersonal der Hochschulen ausgewertet werden. Eine Aufzeichnung und spätere Auswertung (also eine Speicherung des Bild- und Tonmaterials) erklärt die § 32a LHG BW allerdings für unzulässig. Die Hochschulen können für die Prüfung zwischen verschiedenen Modalitäten wählen: eine reine Fernprüfung, bei der die Studierenden von zuhause aus an der Prüfung teilnehmen, sowie eine Online-Prüfung in den Räumlichkeiten der Hochschule oder in einem Testzentrum. Bei reinen Fernprüfungen muss Studierenden eine Alternative zu der Fernprüfung angeboten werden, insbesondere eine termingleiche Präsenzprüfung. Zusätzlich hat der Baden-Württembergische Landesbeauftragte für den Datenschutz ähnlich wie in NRW eine Handreichung zu Online-Prüfungen veröffentlicht.[2]

2. Bayern:

In Bayern regelt die „Bayerische Fernprüfungserprobungsverordnung“ (BayFEV) seit September 2020 die Modalitäten von Online-Prüfungen. Das Gesetz schreibt vor jeder Online-Prüfung zwingend eine Authentifizierung der Studierenden mit Lichtbildausweis vor. Zudem sind Studierende bei jeder Online-Klausur verpflichtet, die Kamera- und Mikrofonfunktion ihres Computers zu aktivieren. Das Bild- und Tonmaterial kann sodann live durch das Aufsichtspersonal der Hochschulen ausgewertet werden. Eine Aufzeichnung und spätere Auswertung erklärt die BayFEV für unzulässig. Ist das Format der Online-Prüfung nicht durch ein pandemisches Infektionsgeschehen bedingt, so haben Studierende nach der Verordnung grundsätzlich ein Wahlrecht. Die Hochschule muss den Studierenden eine termingleiche Präsenzprüfung als Alternative anbieten.

3. Berlin:

In Berlin erlaubt § 32 Abs. 8 des BerlHG Hochschulen, in ihrer Rahmenstudien- und –prüfungsordnung auch digitale Prüfungen vorzusehen. Weitere Regeln finden sich im Hochschulgesetz nicht.

4. Brandenburg:

In Brandenburg ist bei Redaktionsschluss kein Gesetz oder Verordnung in Kraft, das die Datenverarbeitung im Rahmen von Online-Prüfungen ermöglicht. Die Hochschulen ermöglichen die Online-Prüfungen in ihren Prüfungsordnungen allerdings gleichwohl, wie an der Allgemeinen Studienordnung der Universität Potsdam beispielhaft deutlich wird.[3]

---

2 Handreichung zu Online-Prüfungen an Hochschulen, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/07/20210715_Handreichung-Online-Pruefungen.pdf - zuletzt abgerufen am 20. September 2022.

3 Fünfte Satzung zur Änderung der Neufassung der allgemeinen Studien- und Prüfungsordnung für die nicht lehramtsbezogenen Bachelor- und Masterstudiengänge an der Universität Potsdam, abrufbar unter: https://www.uni-potsdam.de/fileadmin/projects/ambek/Amtliche_Bekanntmachungen/2021/ambek-2021-02-010-012.pdf - zuletzt abgerufen am 21. September 2022.

5. Bremen:

In Bremen gibt es seit Februar 2021 ebenso wie in Bayern eine eigene Verordnung für den digitalen Prüfungsbetrieb, die „Digitalprüfungsverordnung“. Auch die Bremischen Vorschriften erklären eine Video- und Audioüberwachung der Studenten für zulässig, nicht allerdings eine Aufzeichnung und Speicherung dieser Daten. Grundsätzlich besteht für Studierende die Wahlmöglichkeit, statt der Online-Prüfung eine Präsenzprüfung wahrzunehmen. Die Hochschulen können das Wahlrecht im Einzelfall aufgrund besonderer Umstände aber entfallen lassen.

6. Hamburg:

In der Freien und Hansestadt Hamburg sind Online-Prüfungen aufgrund von § 60 Abs. 2a Hamburgisches Hochschulgesetzes zulässig. Die Hochschulen müssen die Online-Prüfung in ihren Prüfungsordnungen allerdings explizit vorsehen. Dabei müssen sie auch Regeln zum Datenschutz der Studierenden treffen.

7. Hessen:

In Hessen gilt seit dem 28. Dezember 2021 eine Neufassung des § 23 des Hessischen Hochschulgesetzes. Dieser löst die bis dahin gültige Fernprüfungsverordnung ab. Der Hessische Gesetzgeber setzt damit ähnlich wie Baden-Württemberg auf ein relativ detailliertes Parlamentsgesetz. Im Unterschied zu vielen anderen Bundesländern erlaubt das Hessische Gesetz dem Prüfungspersonal ausdrücklich, den Funktionsumfang der Endgeräte der Studierenden einzuschränken. So kann zum Beispiel die copy-and-paste-Funktion unterbunden werden. Das Gesetz geht auch in anderen Punkten über die Regelungen anderer Bundesländer hinaus: So ist nicht nur eine Live-Überwachung, sondern auch eine Aufzeichnung und kurzzeitige Speicherung der Video- und Audioaufnahmen der Studierenden zulässig. Die Daten dürfen allerdings nur solange vorgehalten werden, wie dies „zu Kontrollzwecken unbedingt erforderlich ist“. Zudem ist nicht nur eine manuelle Überwachung der Daten durch das Hochschulpersonal, sondern auch eine automatisierte Überwachung der Studierenden durch Software-Lösungen zulässig. In einem solchen Fall müssen die Studierenden allerdings ausdrücklich einwilligen.

Auch die Hessischen Regeln schreiben vor, dass Studierenden die Wahlmöglichkeit einer termingleichen Präsenzprüfung verbleibt.

8. Mecklenburg-Vorpommern:

In Mecklenburg-Vorpommern regelt § 7a des Landeshochschulgesetzes MV die Verarbeitung personenbezogener Daten bei Online-Prüfungen. Online-Prüfungen sind damit auch in MV grundsätzlich möglich. Die Live-Überwachung des Bild- und Tonmaterials der Studierenden ist zulässig, die Speicherung des aufgezeichneten Materials nur, wenn schon während der Live-Überwachung Täuschungshandlungen festgestellt wurden. Das mecklenburgische Gesetz erklärt die Online-Prüfung in § 38 Abs. 11 LHG MV für freiwillig. Den Studierenden muss also die Wahlmöglichkeit einer anderen Prüfungsform verbleiben.

9. Niedersachsen:

Das Niedersächsische Hochschulgesetz (NHG) ermöglicht in seinem § 7 Abs. 4 das Abhalten von Online-Prüfungen. Die Hochschulen müssen dies in ihren Prüfungsordnungen allerdings explizit vorsehen und dabei Bestimmungen zum Datenschutz treffen. Ein Wahlrecht für Studierende sieht das Gesetz dabei nicht vor. Generelle Erlaubnisnorm für die Verarbeitung personenbezogener Daten im Hochschulbetrieb ist § 17 Abs. 1 NHG. Die Vorschrift differenziert nicht zwischen Live-Überwachung und Aufzeichnung und Speicherung des Bild- und Tonmaterials der Studierenden. Allerdings hat der Niedersächsische Landesdatenschutzbeauftragte ähnlich wie in NRW in einer Handreichung bereits darauf hingewiesen, dass die Aufzeichnung nur in Ausnahmefällen, insbesondere bei konkretem Täuschungsverdacht, zulässig ist. [4]

10. Rheinland-Pfalz:

In Rheinland-Pfalz sind Online-Prüfungen bis heute durch die „Landesverordnung zur Erprobung elektronischer Fernprüfungen an den Hochschulen“ geregelt. Wie auch der Freistaat Bayern hat Land die Online-Prüfungen damit noch nicht in ein permanentes Gesetz überführt. Die Erprobungsverordnung ist allerdings noch bis zum 31. März 2026 gültig und Online-Prüfungen sollen auch losgelöst von einer pandemiebedingten Ausnahmesituation möglich sein Inhaltlich sieht die Verordnung ebenfalls eine Live-Überwachung der Studierenden vor, untersagt aber eine

4 Eckpunkte für die datenschutzkonforme Durchführung von Online-Prüfungen in den niedersächsischen Hochschulen, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/weitere_themen_von_a_z/hochschulen/eckpunkte_fur_die_datenschutzkonforme_durchfuhrung_von_online_prufungen/ - zuletzt abgerufen am 20. September 2022.

Aufzeichnung und Speicherung des Bild- und Tonmaterials. Studierenden steht grundsätzlich ein Wahlrecht einer termingleichen Präsenzprüfung zu. Das Wahlrecht entfällt nur dann, wenn die Online-Prüfung infolge einer Naturkatastrophe oder einer außergewöhnlichen Notsituation (insb. einer Pandemie) notwendig wird.

11. Saarland:

Das Saarland hat die Online-Prüfungen in § 63 Abs. 6 des Saarländischen Hochschulgesetzes geregelt. Danach können die Hochschulen die Online-Prüfung in ihren Prüfungsordnungen aus wichtigem Grund oder zur Erprobung neuer Prüfungsmodelle vorsehen. Ein Wahlrecht für Studierende sieht das Gesetz dabei nicht vor.

12. Sachsen:

Im Freistaat Sachsen ermöglicht § 35 Abs. 1 des Sächsischen Hochschulfreiheitsgesetzes das Abhalten von Online-Prüfungen. Die Hochschulen müssen diese in ihren Prüfungsordnungen explizit vorsehen. Die Datenverarbeitung im Prüfungsbetrieb ist grundsätzlich erlaubt durch § 14 des Sächsischen Hochschulfreiheitsgesetzes.

13. Sachsen-Anhalt:

In Sachsen-Anhalt ist ebenso wie Rheinland-Pfalz noch eine Fernprüfungserprobungsverordnung in Kraft, die „Verordnung zur Erprobung elektronischer Fernrprüfungen an den Hochschulen im Land Sachsen-Anhalt“. Danach ist eine Live-Überwachung der Studierenden zulässig, nicht jedoch eine Aufzeichnung und Speicherung des Bild- und Tonmaterials. Studierenden verbleibt grundsätzlich das Wahlrecht einer termingleichen Präsenzprüfung.

14. Schleswig-Holstein:

In Schleswig-Holstein können die Hochschulen gem. § 51 Abs.6 Hochschulgesetz SH Online-Prüfungen abhalten. Sie müssen dabei Regelungen zum Datenschutz treffen.

15. Thüringen:

Im Freistaat Thüringen erlaubt § 55 Abs. 2 des Thüringischen Hochschulgesetzes den Hochschulen selbst, Online-Prüfungen in den Prüfungsordnungen vorzusehen. Dabei müssen sie auch Bestimmungen zum Datenschutz treffen.

V. Fazit

Aus den Empfehlungen der LDI NRW sowie den gesetzlichen Regelungen vieler Bundesländer lässt sich ein gemeinsames Muster ableiten. Fast alle Bundesländer halten die Live-Überwachung der Prüflinge für zulässig, nicht jedoch die Aufzeichnung und Speicherung des Bild- und Tonmaterials. Die tiefgreifendsten Eingriffe erlaubt die Hessische Regelung, nach der auch eine Speicherung für einen gewissen Zeitraum zulässig ist. In Brandenburg fehlt zum Redaktionsschluss eine geeignete gesetzliche Grundlage für die Online-Prüfungen. Begrüßenswert ist, dass zahlreiche Landesgesetzgeber die Online-Prüfungen umfassend in einem Parlamentsgesetz geregelt haben. Dies schafft zusätzliche Rechtssicherheit. In Bundesländern, in denen bloß knappe Regelungen in den Hochschulgesetzen existieren, entsteht bei den Hochschulen häufig weiterer Klärungsbedarf. Wie in NRW geschehen wird es sodann notwendig, dass die Landesdatenschutzbeauftragten zusätzliche Empfehlungen herausgeben. Die Empfehlungen decken sich allerdings vollständig mit dem, was andere Bundesländer bereits in Gesetzesform geregelt haben.

Die Beschäftigung mit Beschäftigtendaten

Vorlagefragen des VG Wiesbaden an den EuGH stellen den Beschäftigtendatenschutz auf den Prüfstand

von Nicolas John

Der Beschäftigtendatenschutz spielt im DFN-Infobrief Recht immer wieder eine Rolle.[1] Die Anknüpfungspunkte hierfür sind vielfältig. Dieser Fall des Verwaltungsgerichts (VG) Wiesbaden dreht sich um die zentrale hessische Erlaubnisnorm im Beschäftigungskontext. Das Gericht teilt dabei die Rechtsansichten des Bundesarbeitsgerichts (BAG) nicht und legt dem Gerichtshof der Europäischen Union (EuGH) Fragen im Vorabendentscheidungsverfahren über die Zulässigkeit des hessischen Paragraphen vor. Die Ausführungen des EuGHs könnten dabei weitreichende Auswirkungen auf die Anwendung inhaltsgleicher Normen im Bundesdatenschutzgesetz oder in anderen landesrechtlichen Regelungen haben.

I. Hintergrund

Um den reibungslosen Ablauf des Distanzunterrichts während der Pandemie in hessischen Schulen zu ermöglichen, kamen dort im Jahr 2020 wie vielerorts Videokonferenzsysteme zum Einsatz. Dabei wurden von den Schüler:innen bzw. den Eltern Einwilligungen eingeholt, um die Nutzung zu ermöglichen. Gegenüber dem Lehrpersonal hatte sich der Dienstherr hingegen nicht auf individuelle Einwilligungen gestützt, sondern auf § 23 Abs. 1 S. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG).

Der Inhalt der Norm lässt sich insoweit zusammenfassen, als dass sie die Verarbeitung von Beschäftigtendaten dann erlaubt, wenn dies für die Durchführung des Beschäftigtenverhältnisses erforderlich ist. Eine gesonderte Einwilligung der Arbeitnehmenden ist dann nicht mehr vonnöten. Die Norm findet ihren Ursprung in Art. 88 Datenschutz-Grundverordnung (DSGVO). Danach können Mitgliedstaaten eigene spezifische Regelungen im Bereich des Beschäftigtendatenschutzes erlassen.
Dieser Sachverhalt und die Frage, ob der Einsatz von Videokonferenzsystemen für den Distanzunterricht nur dann möglich ist, wenn das Lehrpersonal dazu seine Einwilligung gegeben hat, war im Dezember 2020 schließlich Gegenstand eines Verfahrens vor dem VG Wiesbaden. Anstatt sich jedoch mit der durch § 23 Abs. 1 HDSIG vorausgesetzten Erforderlichkeit der Datenverarbeitung im Beschäftigungsverhältnis auseinanderzusetzen, zweifelten die Richter schon daran, ob die Norm den Voraussetzungen der Öffnungsklausel des Art. 88 DSGVO gerecht wird und ob die hessischen Vorgaben überhaupt herangezogen werden können. Da es hier um die Auslegung eines europäischen Rechtsaktes geht, setzte die Kammer das Verfahren Ende Dezember 2020 aus und legte dem EuGH die Frage zur Vorabentscheidung vor.[2]

Brisant ist die Vorlage insbesondere deshalb, weil der Wortlaut der Norm dem des § 26 Abs. 1 S. 1 des Bundesdatenschutzgesetzes (BDSG) entspricht. So wird die Diskussion zwar nun vorerst vor dem EuGH um die hessische Datenschutzvorschrift geführt, doch ist das Ergebnis des Verfahrens ebenso für die Vorgaben des BDSG sowie ähnlich lautende landesdatenschutzrechtliche Normen von Bedeutung.

1 So z .B.: Gielen, 2020: Odyssee im Beschäftigtendatenschutz, DFN-Infobrief Recht 5/2021; John, Mein Name ist Hase, ich weiß von nichts, DFN-Infobrief Recht 6/2020; Mörike, Anweisung vom Chef: Willige ein!, DFN-Infobrief Recht 2/2019.

2 VG Wiesbaden Beschluss v. 21.12.20 Az. 23 K 1360/20.WI.PV.

II. Auffassung des VG Wiesbaden

Bislang geht das BAG in seiner Rechtsprechung davon aus, dass § 26 BDSG unter die Öffnungsklausel des Art. 88 DSGVO falle und dass dies derartig offenkundig sei, „dass für vernünftige Zweifel kein Raum" bleibe und eine Vorlage an den EuGH somit nicht nötig sei.[3]

Diese Rechtsprechung stellt das VG Wiesbaden mit seiner Vorlage nun explizit infrage. Es ist der Auffassung, dass mit der hessischen Erlaubnisnorm keine „spezifischere Vorschrift" i.S.d. Art. 88 Abs. 1 DSGVO vorliege. Die Auffassung begründet es mit den allgemeinen Erlaubnistatbeständen des Art. 6 Abs. 1 lit. b) und lit. f) DSGVO. So sei bei Datenverarbeitungen zur Vertragserfüllung lit. b) heranzuziehen, wenn dies für die Erfüllung des Vertrages erforderlich ist. Lit. f) setze für eine zulässige Datenverarbeitung eine umfassende Abwägung der Interessen des Verantwortlichen und der betroffenen Person voraus.

Die Regelung des § 23 HDSIG (und damit auch des § 26 BDSG) hingegen verlange in jedem Fall nur das Vorliegen der „Erforderlichkeit" der Datenverarbeitung für das Beschäftigungsverhältnis. Die Norm würde aber auch für Datenverarbeitungen jeglicher Beschäftigtendaten herangezogen werden, welche nicht nur das eigentliche Kernarbeitsvertragsverhältnis betreffen. Eine Interessenabwägung verlange die Vorschrift aber nicht. In diesem Fall sehe also die allgemeinere Erlaubnisnorm der DSGVO höhere Anforderungen vor als das HDSIG. Daraus schlussfolgert das Verwaltungsgericht, dass es sich nicht um eine „spezifischere Vorschrift" i.S.d. Art. 88 Abs. 1 DSGVO handeln könne.

Darüber hinaus sei bei der Beurteilung, ob eine spezifischere Vorschrift vorliege, Art. 88 Abs. 2 DSGVO ebenfalls zu beachten. Dieser verlangt, dass die spezifischeren Vorschriften „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf […] die Überwachungssysteme am Arbeitsplatz" treffen. Das sei durch die Vorgabe der „Erforderlichkeit" des HDSIG allein aber nicht hinreichend sichergestellt.

Zwar verweise § 23 Abs. 5 HDSIG (und auch § 26 Abs. 5 BDSG) auf Art. 5 DSGVO, doch ändere dies nach der Auffassung des Verwaltungsgerichts nichts. Art. 5 DSGVO legt die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten fest, z.B. Rechtmäßigkeit der Verarbeitung, Transparenz, Zweckbindung oder der Grundsatz der Datensparsamkeit. Zwar seien Verantwortliche angehalten, diese allgemeinen Grundsätze zu beachten, das müssen sie aber ohnehin – auch ohne den Hinweis des Abs. 5. Zudem müsse nach Art. 88 Abs. 2 DSGVO schon die Vorschrift selbst in ihrem Regelungsgehalt die nötigen Gewährleistungen treffen und könne die Aufgabe nicht auf die verantwortliche Person abwälzen.

Das VG Wiesbaden stellt mit diesen Argumenten die Europarechtskonformität der hessischen Landesdatenschutznorm infrage. Sollte die Norm nicht den Voraussetzungen des Art. 88 DSGVO entsprechen, möchte das Gericht daraus schlussfolgernd vom EuGH wissen, ob die Norm dann überhaupt für Datenverarbeitungen in Arbeits- und Dienstverhältnissen herangezogen werden kann. Um diese Fragen zu klären, war die Vorlage an den EuGH aus Sicht des Verwaltungsgerichts erforderlich.

III. Auffassungen der juristischen Literatur

Doch nimmt das VG Wiesbaden dabei denkbar wenig Bezug auf die durchaus vorhandene juristische Literatur, die in großen Teilen dieser Ansicht widerspricht.
Die meisten Stimmen in der Literatur sehen § 26 Abs. 1 BDSG (und somit auch § 23 Abs. 1 HDSIG) in Übereinstimmung mit der Rechtsprechung des BAG als spezifischere Vorschrift i.S.d. Art. 88 DSGVO an. Insbesondere sei die Regelung durch die schon ergangene Rechtsprechung soweit gefestigt und ausgeformt, dass für die Anwender zumeist Rechtsicherheit bestehe. In der Folge müsse § 26 BDSG (und somit auch § 23 Abs. 1 HDSIG) als spezielleres Gesetz vor den allgemeineren Vorschriften der DSGVO für den Beschäftigtendatenschutz angewendet werden. Auch die Bundesregierung hatte schon zu Zeiten der Reform des BDSG ihre Auffassung kundgetan, dass sie bezüglich der Formulierung des § 26 BDSG keinen Änderungsbedarf sehe.[4]

Es formiert sich jedoch auch Widerstand auf der Linie des VG Wiesbaden gegen diese Auffassung. Die Kritiker:Innen der Vorgaben bemängeln insbesondere, dass es sich bei § 26 BDSG

3 BAG Beschluss v. 7.5.2019 Az. 1 ABR 53/17, Rn. 48.

4 BT-Drs. 18/11655, S. 30.

um eine Generalklausel handele und diese daher nicht als „spezifischere Vorschrift“ tauge. Eine solche sei nicht in der Lage, die allgemeinen Vorgaben der DSGVO zu konkretisieren. Zwar räumen auch die kritischen Stimmen ein, dass nicht alle Sachfragen durch eine Klausel geregelt werden könnten und die Klärung dieser Fragen den Gerichten obliege. Doch dürfe die Umsetzung des europäischen Rechts durch die Auslegung der Vorgaben durch Gerichte nur eine unterstützende Wirkung haben und nicht die Umsetzung ersetzen. Diese Aufgabe liege primär beim Gesetzgeber. Daher sei der Erlass eines differenzierenden Beschäftigtendatenschutzgesetzes notwendig.

IV. Auffassung des Generalanwalts

Am 30. Juni 2022 fand in der Sache die mündliche Verhandlung vor dem EuGH statt. Bevor der EuGH nun ein Urteil in der Rechtssache spricht, hat der sog. Generalanwalt die Aufgabe, den Sachverhalt unabhängig von Parteien und Gericht zu prüfen und dem EuGH anschließend in Form von sog. Schlussanträgen einen Vorschlag für das Urteil zu machen. Der EuGH ist aber nicht an diesen Urteilsvorschlag gebunden, er kann ihm auch widersprechen und anders entscheiden.

Am 22. September 2022 stellte der Generalanwalt in der Sache nun die erwarteten Schlussanträge.[5] In seinen Anträgen schließt er sich zumindest teilweise der Auffassung des VG Wiesbaden an. Demzufolge lege § 23 HDSIG keine spezifischeren Vorgaben i.S.d. Art. 88 Abs. 1 DSGVO fest. Vielmehr wiederhole er lediglich die Ermächtigung. Darüber hinaus könne sich der nationale Gesetzgeber nicht auf die Beschränkung zurückziehen, dass der Verantwortliche geeignete Maßnahmen ergreifen muss, wie es in § 23 Abs. 5 HDSIG der Fall ist. Die hessische Norm sei daher keine „spezifischere Vorschrift“ i.S.d. Art. 88 DSGVO.

Als Folge hieraus stellt er fest, dass die Norm im Beschäftigungskontext nicht anwendbar sei und die allgemeinen Regelungen der DSGVO heranzuziehen seien. Offen lässt der Generalanwalt allerding, ob die Norm im Kontext anderer Öffnungsklauseln wie zum Beispiel Art. 6 Abs. 1 lit. e), Abs. 2 DSGVO (der Verarbeitung personenbezogener Daten zum Zwecke der Wahrnehmung einer Aufgabe im öffentlichen Interesse) weiterhin anwendbar bleibt.

V. Mögliche Auswirkungen

Die Schlussanträge des Generalanwalts sind ein Paukenschlag für das deutsche Beschäftigtendatenschutzrecht. Zwar ist der EuGH an diese nicht gebunden, doch folgt der EuGH statistisch gesehen in der Mehrzahl der Fälle den Vorschlägen der Generalanwaltschaft.

Würde sich der EuGH nun also der Argumentation des Generalanwalts anschließen, hätte dies die Unanwendbarkeit von § 23 Abs. 1 HDSIG im Beschäftigtendatenschutzrecht zur Folge und die datenschutzrechtliche Zulässigkeit des Vorgehens des Dienstherrn gegenüber dem Lehrpersonal in Hessen würde sich allein nach Art. 6 DSGVO richten. Diese Möglichkeit lässt zumindest der Generalanwalt zu. Ob das Verwaltungsgericht in diesem Fall zu dem Schluss gelangt, dass die Durchführung der Lehrveranstaltung rechtmäßig war, ist offen.
Doch viel mehr Auswirkung hätte die Entscheidung des EuGHs außerhalb des Verfahrens vor dem VG Wiesbaden. Denn durch die inhaltliche Übereinstimmung der hessischen Norm zu § 26 BDSG muss davon ausgegangen werden, dass eine entsprechende Entscheidung des EuGHs auch dazu führt, dass die Norm des BDSGs nicht mit den Voraussetzungen des Art. 88 DSGVO zu vereinbaren ist.

Zwar haben EuGH-Urteile im Vorlageverfahren nur für die an dem jeweiligen Rechtsstreit beteiligten Parteien Wirkung. Faktisch würden die Fachgerichte aber im Einzelfall der Rechtsauffassung des EuGHs folgen. Rechtsstreitigkeiten, welche sich um die Anwendbarkeit des § 23 Abs. 1 HDSIG drehen, würden entsprechend behandelt werden. Da § 26 BDSG (oder andere entsprechende Landesdatenschutzvorgaben) inhaltlich mit der hessischen Vorschrift übereinstimmt, ist davon auszugehen, dass Gerichte auch diese Normen nicht mehr zur Rechtfertigung der Verarbeitung von Beschäftigtendaten ausreichen lassen könnten. Soweit der deutsche Gesetzgeber den Beschäftigtendatenschutz dann weiterhin autonom i.S.d. Öffnungsklausel des Art. 88 DSGVO selbst regeln wollen würde, müsste eine neue und differenzierte Regelung erlassen werden, die den Vorgaben des EuGHs entspricht.

Lässt der EuGH § 23 Abs. 1 HDSIG (und damit § 26 Abs. 1 BDSG) als spezifischere Vorschrift gelten, kann es hingegen bei der

5 Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona, C-34/21, abrufbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=266121&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=431915 (zuletzt abgerufen am 23.09.2022).

gewohnten Praxis bleiben. Damit wären nämlich auch die entsprechenden landesrechtlichen Vorschriften abgesichert, die Äußerungen des EuGHs wären auch in umgekehrter Richtung vollumfänglich auf inhaltsgleiche Normen anzuwenden.

Unabhängig vom Ausgang des Urteils wird in jedem Fall die Diskussion um ein eigenes Beschäftigtendatenschutzgesetz neu belebt werden. Für ein solches hatte bei der Reform des BDSG seinerzeit der politische Konsens gefehlt. So wies der Bundesrat schon damals die Bundesregierung darauf hin, dass seiner Auffassung nach die Vorschriften im Beschäftigtendatenschutz, also besagter § 26 BDSG, die Vorgaben der DSGVO nicht ausreichend umsetzen würden.[6] Richtungsweisend zeigt sich daher nun der Koalitionsvertrag der aktuellen Bundesregierung: Die Koalitionsparteien haben die Neuregelung des Beschäftigtendatenschutzes explizit festgehalten.[7] Das Urteil des EuGHs wird daher in dieser Diskussion auch eine entscheidende Rolle spielen.

Wie sich das Urteil auf Hochschulen und Forschungseinrichtungen auswirkt, hängt damit ebenfalls maßgeblich von der Entscheidung ab. Soweit der EuGH den hessischen Paragraphen im Beschäftigungskontext für unanwendbar erklären sollte, ist auch Hochschulen zu raten, sich nicht mehr auf entsprechende Erlaubnisnormen als Verarbeitungsgrundlage zu stützen. Vielmehr wären nur noch die allgemeinen Erlaubnistatbestände des Art. 6 DSGVO heranzuziehen. Abhilfe könnte in diesem Fall nur der Gesetzgeber mit neuen, spezifischeren Vorschriften schaffen. Insoweit bleibt nicht nur das Urteil des EuGHs abzuwarten, sondern auch der Einsatz des Gesetzgebers.

6 BT-Drs. 18/11655, S. 15.

7 Koalitionsvertrag 2021 - 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokraten (FDP), S. 14.

Kurzbeitrag: Post(ulation) aus Luxemburg

Der EuGH zur Prozessvertretung durch Hochschullehrer

von Justin Rennert

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 14. Juli 2022 über die Postulationsfähigkeit von Hochschullehrern vor europäischen Gerichten entschieden. Der Gerichtshof stellte dabei fest: An deutschen staatlichen oder staatlich anerkannten Hochschulen beschäftigte Rechtslehrer dürfen ihre eigene Hochschule vor dem Europäischen Gericht (EuG) und dem Europäischen Gerichtshof vertreten. Sie dürfen mithin wie Anwälte wirksam Prozesshandlungen für die eigene Hochschule vornehmen.

I. Sachverhalt und erstinstanzliche Entscheidung des EuG

Der Entscheidung des EuGH lag folgender Sachverhalt zugrunde: Die Universität Bremen hatte vor dem EuG gegen eine Entscheidung der Europäischen Exekutivagentur für die Forschung (REA) geklagt. Die REA hatte einen Projektfinanzierungsantrag der Universität Bremen abgelehnt. Die Universität Bremen begehrte sodann die Nichtigerklärung der ablehnenden Entscheidung. Mit der Vertretung vor dem EuG beauftragte die Universität einen bei ihr angestellten Juraprofessor, der zugleich Koordinator des geplanten Projekts war. Das EuG entschied daraufhin nicht zur Sache, sondern hielt die Klage für unzulässig, weil sich die Universität nicht durch einen bei ihr beschäftigten Hochschullehrer vertreten lassen dürfe. Die Vertretung widerspreche Art. 19 Abs. III-IV der auch für das EuG anwendbaren Satzung des EuGH. Diese Vorschriften würden die Unabhängigkeit des Prozessvertreters gegenüber der Prozesspartei verlangen. Dies bedeute, dass sich der Prozessvertreter in keinem irgendwie gearteten Beschäftigungsverhältnis mit der vertretenen Partei befinden dürfe. Im zu entscheidenden Fall habe sich der Juraprofessor aber in einem öffentlich-rechtlichen Beschäftigungsverhältnis mit der Universität befunden. Er habe aufgrund seiner Stellung als Projektkoordinator sogar ein unmittelbares Interesse an der Entscheidung über den Rechtsstreit.

II. Die letztinstanzliche Entscheidung des EuGH

Der EuGH als nächsthöhere Instanz hat die Argumentation des EuG mit seiner Entscheidung nun verworfen. Zwar gelte auch für Hochschullehrer das Erfordernis der hinreichenden Unabhängigkeit von der Prozesspartei. Der Juraprofessor sei im vorliegenden Fall aber hinreichend unabhängig von seiner Anstellungskörperschaft. Die Prozessvertretung sei nicht Teil seiner eigentlichen Forschungsarbeit und er sei diesbezüglich nicht weisungsgebunden. Die Prozessvertretung hänge in keiner Weise mit seinen akademischen Tätigkeiten zusammen. Der Fall eines in einem öffentlich-rechtlichen Dienstverhältnisses angestellten Hochschullehrers sei nicht vergleichbar mit dem Fall eines Syndikusanwalts, der seinen privatrechtlich organisierten Arbeitgeber vertritt. Das öffentlich-rechtliche Beschäftigungsverhältnis spreche gerade dafür, dass der Hochschullehrer bei der Prozessvertretung hinreichend unabhängig von seiner akademischen Tätigkeit ist. Hochschullehrer seien im Rahmen ihrer akademischen Tätigkeit zudem durch die Forschungs- und Lehrfreiheit geschützt, was ihnen zusätzliche Unabhängigkeit verleihe.

III. Konsequenzen für Hochschulen

Nach der Entscheidung des EuGH ist klar: An deutschen staatlichen oder staatlich anerkannten Hochschulen beschäftigte Rechtslehrer sind vor den Europäischen Gerichten

postulationsfähig. Hochschulen sind mithin nicht darauf angewiesen, einen Rechtsanwalt mit der Vertretung zu beauftragen, sofern sie Partei eines Rechtsstreits vor den europäischen Gerichten sind. Das Urteil des EuGH gilt nur für in Deutschland beschäftigte „Rechtslehrer", d.h. Personen mit originärer selbstständiger juristischer Lehrbefugnis. Das umfasst sowohl Juraprofessorinnen und -professoren an Universitäten und Fachhochschulen als auch Lehrbeauftragte. Hochschullehrer anderer Fächer sind hingegen nicht postulationsfähig. Für Rechtslehrer sorgt das Urteil allerdings für Klarheit. Der EuGH hat zu erkennen gegeben, dass er die Postulationsfähigkeit nur in Fällen offensichtlicher Interessenkollision ablehnen würde. Dies sei dann der Fall, wenn der Prozessvertreter offensichtlich nicht in der Lage ist, den Mandanten durch bestmöglichen Schutz seiner Interessen zu verteidigen.

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