NEU: Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

6 / 2023
Juni 2023

ID(een) muss man haben

Zur Überarbeitung der eIDAS-Verordnung und der Einführung einer digitalen Brieftasche

Scoring – bald nur noch als Entscheidung auf dem Platz?

VG Wiesbaden rüttelt an den Grundfesten der Scoringpraxis

Beschäftigtendatenschutz von A bis Z

VG Hannover zur Arbeitnehmerüberwachung bei Amazon

Kurzbeitrag: Alles neu macht der EuGH

Der deutsche Beschäftigtendatenschutz steht auf der Kippe

ID(een) muss man haben

Zur Überarbeitung der eIDAS-Verordnung und der Einführung einer digitalen Brieftasche

von Pascal Sonak

Bereits im Jahr 2014 wurde die Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt verabschiedet. Diese enthielt Regelungen bezüglich elektronischer Signaturen, Dienste rund um elektronische Siegel und Webseiten-Zertifikate oder die Zustellung elektronischer Einschreiben. Im Rahmen ihrer Digitalstrategie legte die Europäische Kommission im Jahr 2021 einen Entwurf für die Überarbeitung dieser Richtlinie vor. Teil des Entwurfs ist unter anderem die Einführung einer „European Digital Identity Wallet" zur EU-weiten digitalen Identifizierung und Authentifizierung. Nachdem der Rat der Europäischen Union bereits im vergangenen Jahr seine Position für eine Reform der eIDAS-Verordnung verabschiedete, konnten sich nun auch die Abgeordneten des Europäischen Parlaments auf eine gemeinsame Position für eine Neuauflage der Verordnung aus dem Jahr 2014 einigen.

I. Überblick

Viele alltägliche Vorgänge, wie die Eröffnung eines Bank- oder Depotkontos, das Freischalten einer SIM- oder verschiedenste Anträge bei Behörden erfolgen mittlerweile überwiegend digital. Gemeinsam haben all diese Abläufe, dass sie eine Verifizierung der Identität des Nutzers erfordern. Die anbietenden Unternehmen oder Behörden können oder müssen so sicherstellen, dass die Identität der beantragenden Person auch mit der tatsächlichen Identität der Person übereinstimmt. Eine schnelle und sichere Identifizierung im Internet ist somit Voraussetzung für das reibungslose Funktionieren des digitalen Marktes oder der digitalen Verwaltung. In Deutschland gibt es zu diesem Zweck bereits seit November 2010 den Personalausweis mit Online-Ausweisfunktionen. Dessen tatsächlicher Anwendungsbereich bleibt jedoch stark hinter dem der Identifikationsverfahren privater Anbieter zurück. Auch eine überwiegende Anzahl der deutschen Behörden greift nicht auf die Funktionen des Online-Ausweises zu, sondern verlangt noch immer das persönliche Erscheinen.[1] Darüber hinaus ist ein digitaler Nachweis über die Identität in den wenigsten der 27 EU-Mitgliedstaaten Standard. Eine flächendeckende, EU-weite digitale Identifikation ist bislang nicht möglich.

Zur Beseitigung dieses Missstandes und zur Förderung eines EU-weiten vertrauenswürdigen digitalen Identitätsnachweises, legte die EU-Kommission im Jahr 2021 einen Gesetzesentwurf zur Novellierung der eIDAS-Verordnung[2] vor.

Wesentliche Neuerung des Entwurfs ist die für alle Mitgliedstaaten verpflichtende Einführung einer EU-Identity Wallet (Art. 6a ff. Entwurf). Dabei handelt es sich um eine „digitale Brieftasche", in der hoheitliche Dokumente wie der Personalausweis oder der Führerschein aber auch andere Dokumente wie Zeugnisse oder Gesundheitsbescheinigungen digital abgelegt werden können. Nach dem Entwurf kommt den digitalen Identitätsnachweisen dabei die gleiche Wirkung wie papiergebundenen Dokumenten zu. Es soll so eine universell, auch offline nutzbare Möglichkeit für die (auch insb. grenzüberschreitende) Identifizierung und

1 Vgl. z.B. Spiegel, https://www.spiegel.de/netzwelt/netzpolitik/online-personalausweis-und-co-deutschlands-behoerden-bleiben-eine-digital-wueste-a-00000000-0002-0001-0000-000175304180 (zuletzt abgerufen am 1.5.2023).

2 Entwurf abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 (zuletzt abgerufen am 1.5.2023).

Authentifizierung gegenüber Unternehmen und Behörden geschaffen werden. Parallel soll so außerdem die Unabhängigkeit von privaten Anbietern zur digitalen Identifizierung gefördert werden.

II. Datenschutzrechtliche Besonderheiten

Es liegt dabei in der Natur der Sache, dass es bei der Verwendung einer digitalen Brieftasche mit Ausweisdokumenten und anderen elektronischen Attributsbescheinigungen zur Verarbeitung personenbezogener Daten kommt. Unter den zu verarbeitenden und gespeichert Daten sind dabei auch besonders sensitive Daten nach Art. 9 DSGVO. Um die Akzeptanz eines digitalen Ausweises zu gewährleisten, wurden besonders durch den Parlamentsänderungsentwurf neben der Nutzerfreundlichkeit insbesondere auch Aspekte der Datensicherheit berücksichtigt. Die Änderungen gehen dabei teilweise weit über die ursprüngliche Fassung des Kommissionsentwurfs hinaus.

In Art. 5 Abs. 1 des Parlamentsentwurfs sind sowohl der Grundsatz der Datenminimierung als auch Privacy by Design und Privacy by Default festgehalten. Es sollen also nur so viele persönliche Daten wie nötig verarbeitet werden. Darüber hinaus müssen technische Einstellungen der digitalen Wallet, ähnlich zu Cookie-Bannern, auf die datenschutzfreundlichste Alternative voreingestellt sein. Der Parlamentsentwurf sieht außerdem Möglichkeiten für eine vereinfachte Wahrnehmung von Betroffenenrechten vor. Eine Beschwerde über mögliche Datenschutzverstöße soll direkt aus der digitalen Wallet heraus an die zuständige nationale Behörde möglich sein. Außerdem sollen weitere Rechte, wie das Recht auf Löschung oder das Recht auf Datenübertragbarkeit auf einfache Weise von betroffenen Personen durchgesetzt werden können. Darüber hinaus ist im Parlamentsentwurf vorgesehen, dass in Situationen, in denen nur bestimmte Attribute, nicht aber die gesamte Identität des Nutzenden geprüft werden muss (bspw. im Rahmen einer Altersüberprüfung) sog. zero-knowledge-proofs zum Einsatz kommen sollen. Das bedeutet, dass Nutzer so beispielsweise bestätigen können, dass sie das erforderliche Mindestalter zur Nutzung eines Service bereits erreicht haben, ohne jedoch ihr genaues Alter, ihr Geburtsdatum oder andere Informationen zu ihrer Identität preiszugeben. Des Weiteren setzt der Entwurf der Parlamentarier fest, dass Daten rein lokal gespeichert werden, sofern der Nutzende nicht einer anderweitigen Speicherung zugestimmt hat.

Ebenso soll ein Tracking des Nutzerverhaltens technisch ausgeschlossen sein. Schließlich wird die Quellenoffenheit der digitalen Wallet festgesetzt, um durch Transparenz das Vertrauen und die Akzeptanz unter den Nutzenden zu stärken.

III. Probleme

Trotz der Bemühungen der Parlamentarier könnte es jedoch zu datenschutzrechtlichen Problemen kommen.

1. Überidentifikation

Zurzeit gibt es nur eine sehr begrenzte Anzahl von Anwendungsfällen, die eine digitale Identitätsüberprüfung durch private Unternehmen erfordern. Durch die Bereitstellung einer Infrastruktur für eine einfache und schnelle digitale Identifikation könnten Unternehmen in der Folge jedoch geneigt sein, in Sachverhalten, in denen bislang keine Identifizierung notwendig war, diese nun zusätzlich zu verlangen. Dies wird begünstigt durch den Gesetzestext des Kommissionsentwurfs. Hier heißt es, dass die Unternehmen der Mitgliedstaaten lediglich mitzuteilen haben, dass sie die Dienste der digitalen Wallet zur Identifikation nutzen. Es wäre für Unternehmen nach dem Kommissionsentwurf somit möglich, bereits bei Erstellung eines Online-Kontos oder bei Abschluss einer Online-Bestellung stets eine digitale Identifikation zu verlangen.

Der Parlamentsentwurf versucht dem entgegenzuwirken und sieht eine Registrierungspflicht für Unternehmen vor, die personenbezogene Daten aus der Wallet abfragen wollen. Bei sensitiven Daten nach Art. 9 DSGVO soll für eine Freischaltung darüber hinaus eine Genehmigung der zuständigen Behörde in den Mitgliedstaaten erforderlich sein.

Außerdem regeln weitere Normen des Parlamentsentwurfs, dass die Nutzung von Pseudonymen permanent zulässig sein soll und weder durch Vertrag noch durch AGB ausgeschlossen werden kann. So müssen Nutzende nach einer ggf. erforderlichen Identifizierung in sozialen Netzwerken oder Foren via digitaler Wallet nicht mit Klarnamen auftreten. Augenscheinlich bleibt so ggü. den anderen Nutzenden die Anonymität gewahrt, der Einsatz von Pseudonymen lässt sich jedoch selbstverständlich von Ermittlungsbehörden zurückverfolgen. Ebenso legt der Parlamentsentwurf fest, dass, falls eine Identifizierung per

Klarname nicht vorgeschrieben sein sollte, die Überprüfung in erster Linie ohne elektronische Identifizierung und Authentifizierung erfolgen solle. An einer präzisen Aufzählung der Anwendungsfälle für die Verwendung der digitalen Wallet im Gesetzestext fehlt es jedoch.

Schließlich normiert der Parlamentsentwurf, dass die Nutzung der digitalen Wallet freiwillig und kostenlos sein muss. Es dürfen den EU-Bürgern keine Nachteile durch die Nichtnutzung entstehen. Konsequenzen für den Fall, dass Unternehmen oder Einrichtungen eine nicht erforderliche digitale Identifikation verlangen, oder mehr Informationen abfragen als zur Nutzung ihrer Dienste eigentlich erforderlich sind, fehlen bislang auch im Parlamentsentwurf.

2. Einführung einer dauerhaften Personenkennziffer

Der Kommissionsentwurf sieht vor, dass zusätzlich zu den Personenidentifizierungsdaten eine von den Mitgliedstaaten vergeben Personenkennziffer, die für die Identifizierung in allen Bereichen erforderlich sein soll, aufgenommen werden soll. Ebenso sieht auch der Parlamentsentwurf die Einführung einer solchen Kennziffer vor. Der Anwendungsbereich beschränkt sich aber auf natürliche Personen bei grenzüberschreitenden Sachverhalten im öffentlichen Bereich und auf jene Mitgliedstaaten, die bereits über eine solche Kennziffer verfügen.[3]

Verbände und Datenschützer kritisieren, dass die Einführung einer solchen Ziffer es ermöglichen könnte, alle Nutzerinnen und Nutzer der digitalen Wallet in Europa eindeutig zu identifizieren. Außerdem sei das Missbrauchspotenzial enorm. Zwar erteilte auch das Bundesverfassungsgericht einer solchen Kennziffer in seinem Volkzählungsurteil in der Vergangenheit aufgrund von Bedenken hinsichtlich des Rechts auf informationelle Selbstbestimmung eine generelle Absage.[4] Jedoch ist die Einführung einer Personenkennziffer nach den aktuellen Gegebenheiten unter strengen Voraussetzungen möglich.[5] Art. 87 der DSGVO sieht die Möglichkeit der Einführung einer solchen Kennziffer sogar explizit vor.

IV. Fazit und Auswirkungen für Hochschulen und wissenschaftliche Einrichtungen

Für Hochschulen und wissenschaftliche Einrichtungen ist die Identifikation von alltäglicher Bedeutung. Ob bei der Immatrikulation, beim Einlass zu einer Klausur, in der Bibliothek oder sogar an der Mensa-Kasse – täglich identifizieren sich Studierende, Lehrende, Forschende und Universitätspersonal.
Eine digitale Identifikation könnte die hier erforderlichen Verfahren vereinfachen und so zu Entlastungen führen. Ebenso könnten Sicherheitsstandards bei Anmeldeverfahren oder Zahlungen durch eine digitale Identifikation erhöht und dabei aber vereinfacht werden.

Wie die digitale Brieftasche am Ende insbesondere datenschutzrechtlich eingekleidet werden soll, bleibt abzuwarten. Da zusammen mit den letzten Änderungsanträgen der Parlamentarier der Beschluss zur Aufnahme institutioneller Verhandlungen gefasst wurde, müssen nun im üblichen Trilog-Verfahren die Meinungsverschiedenheiten zwischen Rat und Parlament überwunden werden. Mit einer finalen Version der überarbeiteten eIDAS-Verordnung wird derzeit im vierten Quartal 2023 gerechnet.

---

3 In Europa verfügen beispielsweise Frankreich, Österreich, Dänemark, Schwede, Norwegen und Finnland bereits über eine vergleichbare Personenkennziffer.

4 BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83, ua.

5 Vgl. Martini/Wagner/Wenzel, Rechtliche Zulässigkeit einer Personenkennziffer, ZD-Aktuell 2017, 04272.

Scoring – bald nur noch als Entscheidung auf dem Platz?

VG Wiesbaden rüttelt an den Grundfesten der Scoringpraxis

von Ole-Christian Tech

Scoring ist in aller Munde- für die meisten als unliebsame und meist intransparente Praxis von Wirtschaftsauskunfteien, wie der SCHUFA Holding AG. Der Anwendungsbereich des mathematischen Verfahrens, mit dem menschliches Verhalten prädiziert wird, ist jedoch bereits heute sehr viel breiter. So werden Scoring Modelle ebenso in der medizinischen Forschung verwendet, um etwa auf Basis von Krankheitsbildern oder Verletzungsmustern Behandlungsansätze oder Präventionskonzepte zu erarbeiten.
Scoring Systeme sind längst im Einsatz und der Gesetzgeber hat diese als Unterfall des Profilings[1] mit Art. 22 Datenschutzgrundverordnung (DSGVO) und § 31 Bundesdatenschutzgesetz (BDSG) ausdrücklich erlaubt. Dennoch ist die Frage, welche Pflichten die Beteiligten hierbei erfüllen müssen aktuell hochumstritten.
Artikel 22 Abs. 1 DSGVO lautet: „Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt."
Das Verwaltungsgericht (VG) Wiesbaden meldet nun fundamentale Zweifel bezüglich der Legalität von Scoring Modellen in Deutschland und der datenschutzrechtlichen Rollenverteilung zwischen der Auskunftei und der einmeldenden Stelle an.

I. Was ist passiert?

Hintergrund ist die Klage eines Betroffenen gegen den Landesdatenschutzbeauftragten als Aufsichtsbehörde. Der Klägerin wurde nach negativer Beauskunftung durch die Beigeladene die Kreditierung durch einen Dritten verweigert. In der Folge verlangte die Klägerin neben der Löschung ihrer Auffassung nach falscher Eintragungen von der SCHUFA Auskunft über die gespeicherten Daten. Die SCHUFA teilte der Klägerin daraufhin in groben Zügen die grundsätzliche Funktionsweise ihrer Score-Wert-Berechnung mit, nicht jedoch, welche Einzelinformationen mit welcher Gewichtung in die Berechnung einfließen. Gegen diese Auskunft erhob die Klägerin dann Beschwerde beim Landesdatenschutzbeauftragten mit dem Begehren, dieser solle gegenüber der SCHUFA verfügen, dass diese dem klägerischen Begehren nach Auskunft und Löschung nachzukommen habe. Diese lehnte das Begehren schriftlich ab, worauf die Klägerin gegen den Landesdatenschutzbeauftragten klagte.

1 In Art. 4 Nr. 4 DSGVO legal definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".

Das VG Wiesbaden setzte das Verfahren (VG Wiesbaden Beschl. v. 1.10.2021 – 6 K 788/20.WI) aus und legte dem europäischen Gerichtshof unter anderem die nachfolgende Frage zur Auslegung der DSGVO und des BDSG zur Vorabentscheidung vor.

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 Europäischen Gerichtshof (EuGH) zur Vorabentscheidung zu stellen. Ziel ist es, eine einheitliche Anwendung des Unionsrechts sicherzustellen und Rechtssicherheit für alle Beteiligten zu schaffen.

Die Vorlagefrage hat hierbei das Potential die bestehende Scoring Praxis grundlegend in Frage zu stellen und wird daher nun näher untersucht. Die Vorlagefrage lautet wie folgt:
Ist Art. 22 Abs. 1 der Verordnung (EU) 2016/6791 dahingehend auszulegen, dass bereits die automatisierte Erstellung eines Wahrscheinlichkeitswertes über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung darstellt, die der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wenn dieser mittels personenbezogener Daten der betroffenen Person ermittelte Wert von dem Verantwortlichen an einen dritten Verantwortlichen übermittelt wird und jener Dritte diesen Wert seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person maßgeblich zugrunde legt?
In der Sache geht es um die Frage, was genau eine „Entscheidung“ im Sinne des Art. 22 Abs. 1 DSGVO ist und zu welchem Zeitpunkt diese ergeht.

Ist der erstellte Score lediglich eine Entscheidungsgrundlage für einen späteren Vertragsschluss, ist der Vertragsschluss eine Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO und die Rechtslage bleibt insoweit unverändert.
Ist jedoch bereits der Score selbst als eine „Entscheidung“ zu betrachten, fällt die aktuelle Scoring Praxis unter Art. 22 Abs. 1 DSGVO und wäre somit an dessen Absatz 2 zu messen. Dieser sieht drei mögliche Rechtsgrundlagen für Profiling vor, die nachfolgend beschrieben werden.

II. Die Rechtslage

Nach der Systematik des Art. 22 DSGVO besteht zunächst ein Verbot der automatisierten Entscheidungen im Einzelfall- einschließlich Profiling- in Absatz 1. Der Absatz 2 enthält dann aber die folgenden 3 Ausnahmen von diesem Verbot:

1. Art. 22 Abs. 2 lit. a) DSGVO

Dieser verlangt, dass die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist. Hieran werden von Teilen der Literatur hohe rechtliche Anforderungen gestellt. So müssen etwa alternative Wege zum Vertragsabschluss oder zur Erfüllung des Vertrages tatsächlich ausgeschlossen sein.

2. Art. 22 Abs. 2 lit. b) DSGVO

Art. 22 Abs. 2 lit. b) erlaubt Profiling aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, sofern diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten.

Eine solche Rechtsvorschrift wurde in Deutschland mit dem sog. „SCHUFA Paragraphen“ in § 31 BDSG für Wirtschaftsauskunfteien geschaffen. Eine vergleichbare Regelung findet sich für Krankenversicherungen in § 37 BDSG. Besonders bei ersterem ist die Vereinbarkeit mit Unionsrecht jedoch umstritten. Das VG Wiesbaden hält diesen für rechtswidrig, unter anderem, da § 31 BDSG lediglich die „Verwendung“ des „Wahrscheinlichkeitswert“ regelt, nicht aber die Erstellung des Wahrscheinlichkeitswerts selbst.

3. Art. 22 Abs. 2 lit. c) DSGVO

Hiernach ist Profiling dann erlaubt, wenn es mit ausdrücklicher Einwilligung der betroffenen Person erfolgt. Die Anforderungen an diese entsprechen grundsätzlich denen aus Art. 7 DSGVO, wobei aufgrund der vergleichsweise hohen Komplexität von Scoring Systemen hiermit hohe Anforderungen an die Informiertheit der Einwilligung korrespondieren.

III. Der Status Quo

Bisher haben weite Teile der Literatur und Rechtsprechung fast selbstverständlich angenommen, das Scoring selbst sei keine Entscheidung i.S.d. Art. 22 Abs. 1 DSGVO.
Die Gründe hierfür liegen denkbar nah: Der Wortlaut gibt vor, dass die Entscheidung selbst „ausschließlich auf einer automatisierten Verarbeitung“ beruhen muss. Das Merkmal der Ausschließlichkeit wird verbreitet sehr weit ausgelegt, sodass schon ein menschlicher Entscheidungsträger ausreicht, der nur einen weiteren Aspekt als Bewertungskriterium neben dem Score Wert anwendet.
Vereinfacht gesagt, ist der Score Wert in dieser Lesart nur eine Entscheidungsempfehlung. Hat eine natürliche Person eine tatsächliche Möglichkeit von der Entscheidungsempfehlung abzuweichen, beruht die Entscheidung nicht „ausschließlich“ auf der automatisierten Verarbeitung und somit ist nur die Entscheidung der natürlichen Person eine Entscheidung i.S.d Art. 22 Abs. 1 DSGVO.

Dies wird auch mit teleologischen Erwägungen gestützt, wonach ratio legis des Art. 22 Abs. 1 DSGVO nicht das Verbot von Entscheidungsunterstützung und -vorbereitung durch Profiling ist, sondern der Schutz des Betroffenen davor einer automatisierten Entscheidungsfindung „unterworfen“ zu sein, also keinerlei menschlichen Kontrollmechanismus mehr zu haben. Ein durch mathematische Verfahren ermittelter Wert wird jedoch in der Regel nur als Entscheidungsgrundlage verwendet, an die sich eine menschliche Entscheidung, z.B. über einen Vertragsschluss oder dessen Konditionen anschließt.

IV. Die Argumente der Gegenseite

Es lassen sich jedoch einige Argumente für die Rechtsauffassung des VG Wiesbaden ins Feld führen. Hierfür bedarf es lediglich der Anwendung rechtswissenschaftlichen Handwerkzeugs.
Zunächst dient der Wortlaut der Norm als Ausgangspunkt, indem eine grammatikalische Auslegung Argumente für diese Rechtsposition liefert.

Der Score ist- etwas vereinfacht gesagt- eine Bewertung. Diese Bewertung erfolgt aber nicht für eine individuelle Leistung, sondern für einen Wahrscheinlichkeitswert. Um diese Bewertung ermitteln zu können, bedarf es eines bestimmten algorithmischen Verfahrens. Das ist das Profiling. Profiling ist also eine Datenverarbeitung als Mittel zum Zweck der Bewertung. Der Score aber ist die Bewertung, also das Resultat und folglich nicht das Mittel. Damit ist der finale Score Wert dann eine Entscheidung, nämlich als Resultat des vorherigen mathematischen Zuweisungs- und Bewertungsprozesses. Diese Lesart mag auf den ersten Blick kleinkariert erscheinen, ist deswegen aber nicht weniger zutreffend.

Nochmal zur Erinnerung: Die Erstellung des Scores ist damit nicht per se unzulässig, wenn sie eine „Entscheidung“ nach Art. 22 Abs. 1 DSGVO ist, sie wäre dann aber eben nur mit Einwilligung zulässig.

Auch systematische Erwägungen lassen sich anführen. So sieht das VG Wiesbaden eine Rechtsschutzlücke darin, dass der Auskunftsanspruch der betroffenen Person Art. 15 Abs. 1 lit. h) DSGVO leerlaufen könnte. Der Verantwortliche, der hinter dem Scoring Verfahren steht, wäre mangels „einer automatisierten Entscheidungsfindung“ nicht Adressat der Norm. Derjenige Verantwortliche, der den Scoring Wert nutzt, um eine Entscheidung basierend auf dieser automatisiert zu treffen, wäre zwar Adressat der Norm und somit auskunftsverpflichtet, hat aber gar keine Informationen über das Zustandekommen des Score Werts und kann diesen Anspruch somit schon gar nicht erfüllen. Dieses Ergebnis erscheint systemwidrig.
Nur wenn man bereits den Score Wert selbst als Entscheidung begreift könnte man dieses Dilemma umgehen.

Bei realistischer Betrachtung ist es so, dass die Ermittlung des Scorewertes geradezu automatisch eine korrespondierende Entscheidung herbeiführt, insbesondere bei negativen Scoring Ergebnissen. Diese können dann in erheblicher Weise beeinträchtigende Entscheidungen für den Betroffenen darstellen. Als Beispiel können hier etwa Online Versandhändler dienen, die Ihre Entscheidung, ob sie eine bestimmte Zahlungsmodalität anbieten oder nicht, von dem Scorewert abhängig machen.
Auch teleologisch lässt sich diese Auffassung untermauern: Erwägungsgrund 71 der DSGVO erklärt - etwas verkürzt - jede Person sollte das Recht haben, keiner Entscheidung zur Bewertung von persönlichen betreffenden Aspekten ohne jegliches menschliche Eingreifen unterworfen zu werden.
Genau das ist aber das Resultat einer immer weiter voranschreitenden Digitalisierung in allen denkbaren Lebensbereichen. Dies zu berücksichtigen ist also keine Hinwegsetzung über einen gesetzgeberischen Willen im Wege einer zu extensiven Auslegung, sondern lediglich das Anerkenntnis einer Lebensrealität.

V. Schlussanträge des Generalanwalts

Am 16.03.2023 hat der Generalanwalt Priit Pikamäe seine Schlussanträge für das Vorlageverfahren vorgelegt.
Dabei stellte er fest, dass aus dem Fehlen einer Legaldefinition für die „Entscheidung“ darauf geschlossen werden kann, dass der Gesetzgeber eine weite Definition angenommen habe. Dabei stellt er darauf ab, dass eine Entscheidung nicht nur rechtlich, sondern auch rein tatsächlich auf gleich beeinträchtigende Art und Weise wirken kann. Dies stützt er auch auf den Normzweck, gemäß dem die Betroffenen vor diskriminierenden oder ungerechten Auswirkungen geschützt werden sollen. Folglich liegt nach seiner Ansicht eine „Entscheidung“ i.S.d. Art. 22 DSGVO vor (EuGH, Schlussanträge des Generalanwalts vom 16.3.2023 – C-634/21, Rn. 37-39).
Daneben ließ er jedoch offen, ob der Score der Auskunftei unmittelbar für die Entscheidung wirkt. Dies ist nach seiner Ansicht eine Tatsachenfrage, die auch von den Umständen des Einzelfalls und den Arbeitsweisen in der Bank abhängig ist.
Es bleibt daher abzuwarten, ob der EuGH, wie häufig, den Schlussanträgen des Generalanwalts folgt. Zudem sind die Tatsachenfragen durch die ursprüngliche Instanz abzuwarten.

VI. Relevanz für Hochschulen und Ausblick

Scoring Verfahren sind wie eingangs erwähnt bereits weit verbreitet. Im Wirtschaftsverkehr sind Wirtschaftsauskunfteien kaum wegzudenken, aber auch in Verhaltensforschung, medizinischen Diagnostik oder Geeignetheitsentscheidung für Personalmaßnahmen oder die Studienplatzvergabe sind sie einsetzbar.
Eine wirklich klare Rechtslage wird es erst geben, wenn der europäische Gerichtshof das letzte Wort hierzu gesprochen hat. Anwender von Scoring Verfahren sind jedoch gut beraten, ihre gegenwärtige Praxis kritisch zu hinterfragen. Beispielsweise sollte darauf geachtet werden, dass Sachbearbeiter die Entscheidungen treffen, tatsächlich eigene Ermessensspielräume haben und nicht etwa durch verbindliche Leitfäden unmittelbar an den Score Wert gebunden sind. Denn im zuletzt genannten Fall wäre das bloße Abnicken der natürlichen Person eine bloße Formalie und der Score Wert bereits die kritische Entscheidung i.S.d. Art. 22 Abs. 1 DSGVO, wofür womöglich gar keine der oben genannten Rechtsgrundlagen nach Art. 22 Abs. 2 DSGVO einschlägig ist.

Beschäftigtendatenschutz von A bis Z

VG Hannover zur Arbeitnehmerüberwachung bei Amazon

Von Johannes Müller

Das Verwaltungsgericht (VG) Hannover hat sich in seiner Entscheidung (Az. 10 A 6199/20) mit dem Einsatz von Technologien durch Amazon beschäftigt, die es dem Unternehmen erlauben in seinem Logistikzentrum die Arbeitsleistung von Mitarbeitern zu überwachen. Hierbei hatte es die Persönlichkeitsrechte der Mitarbeiter mit den unternehmerischen Interessen von Amazon in Abwägung zu bringen.

I. Technologien, die Arbeitnehmerüberwachung ermöglichen

Die zunehmende Digitalisierung des Arbeitsplatzes führt automatisch zu einem Einsatz neuer Technologien, um Betriebsabläufe zu optimieren. Hierbei erfolgt häufig – beabsichtig oder unbeabsichtigt – eine Verarbeitung von Mitarbeiterdaten, die zu unterschiedlichen Zwecken genutzt werden können. Durch diese Datenverarbeitungen können Persönlichkeitsrechte von Arbeitnehmern betroffen werden, Unternehmen begeben sich hierbei schnell in einen juristischen Graubereich.[1] In der Vergangenheit hat das Bundesarbeitsgericht (BAG) (Az. 2 AZR 681/16) etwa den Einsatz eines Keyloggers am Dienst-PC als rechtswidrig angesehen. Dieser ermöglichte es, ein sehr umfassendes Profil von der dienstlichen und privaten Nutzung des PCs durch den Arbeitnehmer zu erstellen.[2]

Unternehmen wie der Onlineversandhändler Amazon, die für ihren hocheffizienten Geschäftsbetrieb bekannt sind, stehen häufig medial in der Kritik, ihre Mitarbeiter einer hohen Arbeitsbelastung auszusetzen. Dieser effiziente Geschäftsbetrieb kann mit Werkzeugen zur Überwachung des Arbeitsplatzes einhergehen. So ließ Amazon 2018 in den USA ein elektronisches Überwachungsarmband patentieren, das Bewegungen der Beschäftigten durch Ultraschall-und Funktechnologie erfassen und nachvollziehen kann.[3] Auch wenn der Einsatz dieser Technik in Deutschland nicht bekannt ist, veranlassten andere Technologien von Amazon eine Kontrolle durch die Datenschutzbehörden. In einem Logistikzentrum, das Amazon im niedersächsischen Winsen betreibt, findet eine Aufzeichnung der Arbeitsschritte von Beschäftigten durch Handscanner statt. Diese Scanner erfassen, welches Produkt in welchen Transportkorb oder in welches Regalfach gelegt werden und verknüpfen diese Arbeitsschritte durch eine Softwareauswertung mit dem jeweiligen Profil der Mitarbeiter. Diese minutengenaue Aufzeichnung der Leistungswerte gab Amazon die Gelegenheit, auf Leistungsschwankungen in den einzelnen Arbeitsbereichen reagieren zu können. Ebenso wurden die Daten genutzt, um den Mitarbeitern Feedback zu ihrer Leistung zu geben. Dies bot der Landesdatenschutzbeauftragten Anlass, die dortigen Datenerhebungen auf ihre Rechtmäßigkeit zu überprüfen. 2020 untersagte die Landesdatenschutzbeauftragte mittels eines Bescheids die dauerhafte Erhebung der Qualitäts- und Quantitätsleistungsdaten der Arbeitnehmer. Gegen diese Untersagungsverfügung erhob Amazon Klage.

1 Kartheuser/Pabst, Wo liegen die Grenzen der Arbeitnehmerüberwachung?, https://www.lto.de/recht/kanzleien-unternehmen/k/arbeitsrecht-mitarbeitende-ueberwachung-leistungskontrolle-10a619920-urteil-vg-hannover-amazon (zuletzt abgerufen am 5.5.2023).

2 Vgl. zum vorinstanzlichen Urteil des LAG Hamm auch Leinemann, Der „Key“ zum Erfolg?, DFN-Infobrief Recht 04/2017.

3 Dubois, Amazon patentiert Überwachungs-Armbänder, https://www.faz.net/aktuell/wirtschaft/digitec/amazon-patent-auf-ueberwachungs-armbaender-gewaehrt-15427727.html (zuletzt abgerufen am 5.5.2023)

II. Unternehmerische Freiheit vs. Persönlichkeitsschutz des Arbeitnehmers

Die Rechtmäßigkeit des Einsatzes solcher Handscanner richtet sich nach nationalem Datenschutzrecht. Zwar ist der Schutz personenbezogener Daten grundsätzlich abschließend auf europäischer Ebene durch die Datenschutzgrundverordnung (DSGVO) geregelt, diese sieht jedoch für bestimmte Bereiche Öffnungsklauseln vor, die es den Mitgliedstaaten erlauben, eigene nationale Regelungen zum Datenschutz zu treffen. So regelt Art. 88 Abs. 1 DSGVO, dass die Mitgliedstaaten durch Rechtsvorschriften spezifischere Regelungen zur Gewährleistung des Schutzes der Rechte und Freiheiten bei der Verarbeitung von personenbezogenen Beschäftigtendaten im Beschäftigtenkontext treffen dürfen. Von dieser Möglichkeit hat der deutsche Gesetzgeber in § 26 BDSG Gebrauch gemacht. § 26 Abs. 1 S. 1 BDSG regelt, dass personenbezogene Daten von Beschäftigten unter anderem verarbeitet werden dürfen, wenn dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist.[4] Um zu bestimmen, ob eine Datenverarbeitung im individuellen Fall tatsächlich erforderlich ist, müssen die unterschiedlichen betroffenen Interessen miteinander abgewogen werden. Im Rahmen des Einsatzes von Handscannern durch Amazon und deren Auswertung mittels Software stehen sich das Allgemeine Persönlichkeitsrecht der betroffenen Beschäftigten und das wirtschaftliche Interesse des Unternehmens Amazon gegenüber.

Das Allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG ist in Form des Rechts auf informationelle Selbstbestimmung betroffen, das es einer Person erlauben soll, grundsätzlich selbst entscheiden zu können, ob und zu welchem Zweck personenbezogene Daten erhoben werden. Demgegenüber haben Unternehmen grundsätzlich ein legitimes Interesse daran ihre Arbeitsabläufe unter Einsatz neuer Technologien zu optimieren und effektiver zu gestalten.

III. Die Entscheidung des VG Hannover

Diese unterschiedlichen Interessen hatte das VG Hannover im Rahmen seines Urteils über die Rechtmäßigkeit der Untersagungsverfügung durch die Landesdatenschutzbeauftragte zu berücksichtigen. Die Verhandlung fand auch im Logistikzentrum von Amazon selbst statt, sodass das Gericht die Möglichkeit erhielt, das Fulfillment-Center zu besichtigen.

Das VG Hannover nahm an, dass im Ergebnis die Interessen der Klägerin Amazon überwiegen würden. Die Datenverarbeitung sei einerseits erforderlich für die Steuerung der Logistikprozesse im Fulfillment-Center. Durch Umverteilungen von Beschäftigten könne Amazon auf Grundlage der Datenauswertung auf die bestehenden erheblichen Schwankungen der Leistungsfähigkeit der Mitarbeiter in den einzelnen Prozesspfaden reagieren. Dies ermögliche einen reibungslosen Ablauf der Prozesse (insbesondere die Vermeidung von Warenstau) und hierdurch die Einhaltung von Liefergarantien. Ohne die quantitative und qualitative Überwachung der Betriebsprozesse in Echtzeit seien insbesondere ad hoc Maßnahmen bei Störungen in solch komplexen Prozessabläufen nicht möglich. Anderseits könne Amazon aufgrund der Datenauswertung individuellen Qualifizierungsbedarf für Beschäftigte erkennen. Zudem würden die Daten eine objektive Grundlage für Feedback, Personal- und Beförderungsentscheidungen geben.

Der Eingriff in die informationelle Selbstbestimmung der Beschäftigten stehe demgegenüber nicht außer Verhältnis zu den legitimen Interessen des Unternehmens. Gegen einen besonders intensiven Eingriff spreche, dass die Datenerhebung nicht heimlich erfolge, sondern den Beschäftigten gegenüber vollkommen offen kommuniziert werde. Darüber hinaus finde keine Verhaltenskontrolle statt, da Kommunikation und physische Bewegungen nicht erfasst würden. Nicht die Privatsphäre, sondern lediglich die berufliche Sphäre sei betroffen.
Durch die Datenerhebung würde zudem kein unzumutbarer permanenter Anpassungs- und Leistungsdruck auf die Mitarbeiter ausgeübt werden, da diese bei Personalentscheidungen nicht alleinentscheidend sei, sondern auch weitere Fähigkeiten und persönliche Merkmale einbezogen würden.

Schließlich fanden auch Stellungnahmen der Mitarbeiter, die vor Gericht als Zeugen befragt wurden, Eingang in die Urteilsfindung. Nach eigener Auffassung einiger Mitarbeiter stellte die Erfassung der Arbeitsschritte keine erhebliche Belastung dar. Stattdessen erkannte man an, dass die Verarbeitung der personenbezogenen Daten zur effizienten Steuerung der Betriebsabläufe erforderlich sei. Weiterhin würden die Beschäftigten die Möglichkeit

4 Die Unionsrechtskonformität von § 26 BDSG wird stark in Zweifel gezogen, vgl. hierzu John, Kurzbeitrag: Alles neu macht der EuGH, DFN-Infobrief Recht 06/2023. Im Falle der Rechtswidrigkeit von § 26 BDSG richtet sich die Rechtmäßigkeit der Datenverarbeitung nach den Bestimmungen der DSGVO. Auch hierbei kann eine vergleichbare Interessenabwägung vorgenommen werden.

schätzen, objektives Feedback und faire Personalentscheidungen zu erhalten. Dies sei erst durch die Überwachung möglich. In der Tatsache, dass die Beschäftigten selbst die Überwachung nicht als erhebliche Belastung wahrnehmen und augenscheinlich zugunsten von Amazon Stellung beziehen, zeigt sich eine Besonderheit des Falls. Sie ist darin begründet, dass dem Urteil kein Rechtsstreit zwischen Amazon und den Beschäftigten selbst zugrunde liegt, sondern zwischen Amazon und der Landesdatenschutzbeauftragten von Niedersachsen. Die Betroffenen der Datenverarbeitung selbst sahen sich anscheinend aber gar nicht als Opfer eines Datenschutzverstoßes.

Allerdings ist das Urteil noch nicht in Rechtskraft erwachsen, die Landesdatenschutzbeauftragte Niedersachsen hat Berufung eingelegt, der Sachverhalt liegt nun dem OVG Lüneburg vor (Az. 11 LC 105/23).

IV. Auswirkungen für wissenschaftliche Einrichtungen

Das Urteil beschäftigt sich mit einer Problematik, der in Zukunft eine zunehmend größere Relevanz zukommen wird. Der Einsatz moderner Technologien kann einerseits Betriebsabläufe optimieren, birgt häufig aber auch andererseits das Risiko einer Überwachung von Beschäftigten. Auch unterschiedliche Lösungen zur Arbeitszeiterfassung haben das Potential in das Persönlichkeitsrecht von Arbeitnehmern einzugreifen.[5] Auch wissenschaftliche Einrichtungen werden sich mit der Frage beschäftigen müssen, welche Technologien zur Arbeitsoptimierung sie einsetzen möchten. Hierbei kann das Urteil entscheidende Anhaltspunkte geben, um zu bewerten, ob eine Verletzung der Datenschutzrechte der Beschäftigten vorliegt. Insbesondere ist zu berücksichtigen, ob auch privates Verhalten von Beschäftigten überwacht wird und wie vorhersehbar der Eingriff für die Beschäftigten selbst ist. Im Einzelfall muss stets untersucht werden, wie stark die Einrichtung aus unternehmerischer Perspektive tatsächlich von dem Einsatz der Technologie profitiert.

5 Vgl. zur Pflicht zur Arbeitszeiterfassung Voget, Die letzte Stunde hat geschlagen!, DFN-Infobrief Recht 05/2023.

Kurzbeitrag: Alles neu macht der EuGH

Der deutsche Beschäftigtendatenschutz steht auf der Kippe

von Nicolas John

Schon im DFN-Infobrief 10/2022[1] wurden die Vorlagefragen des Verwaltungsgerichts (VG) Wiesbaden an den Gerichtshof der Europäischen Union (EuGH) thematisiert. Das Verwaltungsgericht hatte dem EuGH im Kontext einer hessischen Erlaubnisnorm aus dem Datenschutz Fragen über die Vereinbarkeit der Vorschrift mit dem geltenden Europarecht vorgelegt. Nun hat dieser entschieden.

I. Verfahrenslauf

In Hessen sollte während der Corona-Pandemie der Schulunterricht in den digitalen Raum verlegt werden. Von Schüler:innen bzw. Eltern holte man hierzu Einwilligungen ein, für die Datenverarbeitung der Lehrer:innen stellte man auf den § 23 Abs. 1 S. 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) ab. Dieser ist nahezu inhaltsgleich mit dem bundesweit geltenden § 26 BDSG sowie vieler anderer Landesdatenschutznormen im Beschäftigungskontext.
Gegen die Datenverarbeitung auf Grundlage des § 23 HDSIG klagte der Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kulturministerium vor dem VG Wiesbaden. Dieser stellte die Erforderlichkeit der Datenverarbeitung in Frage. Doch das Verwaltungsgericht sah sich aber nicht imstande, über die Rechtmäßigkeit der Datenverarbeitung zu entscheiden. Grund hierfür waren die Zweifel des Gerichts über die Europarechtskonformität der hessischen Datenschutznorm. Daher legte es dem EuGH Fragen zur Rechtmäßigkeit des § 23 HDSIG mit Blick auf die DSGVO vor.[2] Nun hat der EuGH sein Urteil veröffentlicht.[3]

II. Entscheidung

Art. 88 DSGVO ermöglicht es dem deutschen Gesetzgeber als Öffnungsklausel, abweichend von den Vorgaben der DSGVO im Beschäftigungskontext eigene, nationale Regelungen aufzustellen. Allerdings muss die nationale Erlaubnisnorm hierfür „spezifischer" sein. Um diesen Punkt drehten sich die Vorlagefragen des VG Wiesbaden. Dieses hatte Zweifel, ob § 23 HDSIG eine solche „spezifischere Norm" sei.

Der EuGH entschied nun, dass die Zweifel des Verwaltungsgerichts begründet waren. Denn um als spezifischere Norm i.S.d. Art. 88 DSGVO zu gelten, muss diese die Voraussetzungen des Abs. 2 erfüllen, was bei der hessischen Erlaubnisnorm nicht der Fall sei. Danach müsste die *„spezifischere"* Norm *„geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person"* umfassen. Der § 23 HDSIG dagegen wiederhole die Voraussetzungen des Art. 88 DSGVO lediglich, ohne weitere Anforderungen an den Verantwortlichen zu stellen.

III. Auswirkungen in der Praxis

Das Urteil des EuGHs ändert den Beschäftigendatenschutz in Deutschland nun nicht unmittelbar. Bindungswirkung entfaltet die Entscheidung des EuGHs zunächst nur für das VG Wiesbaden, welches nun anhand der Vorgaben des EuGHs in seinem Urteil feststellen muss, ob die Datenverarbeitungen der personenbezogenen Daten der Lehrer:innen rechtmäßig war.

1 John, Die Beschäftigung mit Beschäftigtendaten, DFN-Infobrief Recht 10/2022.

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

3 EuGH, Urt. v. 30.03.2023, Az. C-34/21, Hauptpersonalrat der Lehrerinnen und Lehrer.

Langfristig wird die Entscheidung des EuGHs für den Beschäftigtendatenschutz allerdings weitreichende Folgen haben. Der Umstand, dass § 23 HDSIG nahezu den gleichen Wortlaut wie § 26 BDSG und vieler weiterer Erlaubnisnormen aus den verschiedenen Landesdatenschutzgesetzen aufweist, zeigt, dass angenommen werden muss, dass auch diese Normen nicht den europäischen Vorgaben genügen.
Daher ist jedes Unternehmen und jede Einrichtung gut beraten, Datenverarbeitungen im Beschäftigungskontext nicht mehr auf diese wohl europarechtswidrigen Erlaubnisnormen zu stützen, sondern vorerst auf die allgemeinen Vorgaben der DSGVO wie Art. 6 zurückzugreifen und zu prüfen, welche alternativen Rechtsgrundlagen hier zur Verfügung stehen.

In jedem Fall kann das Lippenbekenntnis des Gesetzgebers aus dem Koalitionsvertrag[4] sowie der Datenschutzbehörden[5] aufgrund des Urteils des EuGHs kein reines Gedankenspiel mehr bleiben. Vielmehr muss die Neuregelung des Beschäftigtendatenschutzes zeitnah umgesetzt werden, damit die Rechtssicherheit wiederhergestellt werden kann.

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

5 DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf (zuletzt abgerufen 3.5.2023).

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