In Kooperation mit:
Bitkom
BvD
davit im DAV
eco
VAUNET

ZD ZEITSCHRIFT FÜR DATENSCHUTZRECHT

Herausgeber: RA Prof. Dr. Jochen Schneider · Prof. Dr. Thomas Hoeren · Prof. Dr. Martin Selmayr · RA Dr. Axel Spies · RA Tim Wybitul

AUS DEM INHALT

Beilage
Leserumfrage mit Gewinnspiel

www.zd-beck.de

C.H.BECK

Seiten 181–240
16. Jahrgang 1. April 2026

4/2026

linkedin.com/showcase/zeitschriftzd

O850202604

DeutscheAnwaltAkademie

davit
DAV IT-RECHT

13. Deutscher IT-Rechtstag

„Vertrags-Praxis für KI-basierte und andere digitale Produkte – Die EU-Digitalrechtsakte in der Vertragsgestaltung und Compliance“

23. und 24. April 2026 • Präsenz in Berlin & Online

IT-Rechtsabend am Donnerstag ab 19:00 Uhr

Vortragsthemen

- **Keynote**
  Marco-Alexander Breit, Abteilungsleiter für Digitalpolitik und Wirtschaft, Bundesministerium für Digitales und Staatsmodernisierung
- **Impulsvorträge von Vertretern aus Bundesnetzagentur, EU-Parlament und BfDI**
  mit anschließender interaktiver Diskussion mit Teilnehmern und Teilnehmerinnen
- **Probleme der Begrifflichkeit und der Querverbindungen der Anforderungen der Digitalakte an den Beispielen Interoperabilität und Kompatibilität: Für die Praxis nicht umsetzbar**
- **Lizenzierung von Daten und Werken zum Training von KI-basierten digitalen Produkten, einschließlich Lizenzmetriken in der Leistungskette bei Nutzung und Vertrieb KI-basierter digitaler Produkte**
- **Datenlizenzen nach Data Act – mit FRAND-Regelungen zum KI-Training**
- **Anforderungen nach DSGVO – JC oder AVV, Art. 9 DSGVO – Was bedeutet die EuGH-Rechtsprechung für die Praxis?**
- **IT- und Produktsicherheitsanforderungen nach KI-VO, DSGVO, CRA und DORA**
- **NIS-2 Anforderungen in der Lieferkette**
- **Typische Risikoszenarien bei KI-basierten digitalen Produkten**
- **Produkthaftung, Gewährleistung und Schadensersatzansprüche bei Schäden durch KI-basierte digitale Produkte**
- **Ansprüche des Verbrauchers beim Vertrieb digitaler Produkte**
- **Regress in der Lieferkette**
- **Accountability und Beweislast nach aktueller Rechtsprechung: Mängel, Produkthaftung und Regress**
- **Zusammenfassung und Ausblick für Vertragsgestaltung und Compliance**

Weitere Informationen und Anmeldung unter: www.anwaltakademie.de

Die Veranstalter danken für die Unterstützung der Zeitschriften „**MMR**“ und „**ZD**“ des **Verlags C. H. Beck**.

MMR MultiMedia und Recht

ZD DATENSCHUTZ

C.H.BECK

In Kooperation mit:
Bitkom
BvD
davit im DAV
eco
VAUNET

ZEITSCHRIFT FÜR DATENSCHUTZRECHT

ZD

INHALT

4/2026 Seiten 181–240

Newsdienst ZD Aktuell
Inklusive Online-Newsdienst

linkedin.com/showcase/zeitschriftzd

Beilage
Leserumfrage mit Gewinnspiel

KIR | MMR | ZD | bitkom events

29.09. Futurium | 30.09. Online

Privacy Conference

On 29 & 30 September 2026, privacy experts from various data protection authorities, international companies and outstanding start-ups come together at Bitkom's Privacy Conference to discuss the latest trends in data protection, international data transfers and cooperation for the data economy.

#pco26
www.privacy-conference.com

Zeitschrift für Datenschutzrecht – ZD
www.zd-beck.de

Anke Zimmer-Helfrich | Chefredakteurin
Nina Himmelstoß | Redakteurin
Christine Völker-Albert | Redakteurin
Karin Löscher | Redaktionsassistentin

Herausgeber:
Prof. Dr. Thomas Hoeren, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster – RA Prof. Dr. Jochen Schneider, CSW Rechtsanwälte, München – Prof. Dr. Martin Selmayr, Botschafter der Europäischen Kommission in Rom, früher Generalsekretär der Kommission – RA Dr. Axel Spies, Partner, Potomac Law, Washington, D.C. – RA Tim Wybitul, FA Arbeitsrecht, Partner, Latham & Watkins LLP, Frankfurt/M.

Wissenschaftsbeirat:
RAin Dr. Astrid Auer-Reinsdorff, FA IT-Recht, Berlin/Lissabon, Vorstand Deutscher Anwaltverein – Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – Dr. Stefan Brink, Geschäftsführender Direktor Institut wida, Berlin/LfDI Baden-Württemberg a.D. – RAin Isabell Conrad, CSW Rechtsanwälte, München – RAin Susanne Dehmel, Mit-glied der Geschäftsleitung Bitkom e.V., Berlin – Dr. Oliver Draf, LL.M., Leiter Konzern-Datenschutz der Volkswagen AG, Wolfsburg – RA Dr. Jens Eckhardt, FA IT-Recht, Düsseldorf/Vorstand (Recht) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. – Dr. Eugen Ehmann, Regierungspräsident von Unterfranken a.D., Würzburg – RAin Prof. Dr. Sibylle Gierschmann, LL.M., Hamburg/Co-Leiterin Fachausschuss Datenschutz der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) – RA Dr. Stefan Hanloser, München – Prof. Dr. Gerrit Hornung, LL.M., Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Umweltrecht, Universität Kassel – RA Dr. Sebastian Kraska, externer Datenschutzbeauftragter, IITR GmbH, München – RA Dr. Matthias Lachenmann, Partner, BHO Legal PartG mbB, Datenschutzbeauftragter (UDISzert), Gesellschafter, BHO Consulting GmbH, Köln – Prof. Dr. Thomas Petri, Der Bayerische Landesbeauftragte für den Datenschutz, München – Prof. Dr. Andreas Popp, M.A., Inhaber des Lehrstuhls für Deutsches und Europäisches Straf- und Strafprozessrecht, FB Rechtswissenschaft, Universität Konstanz – Prof. Dr. Alexander Roßnagel, Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Wiesbaden/Universitätsprofessor für Öffentliches Recht, Universität Kassel/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) – Heiko Markus Roth, LL.M., Datenschutzbeauftragter im Konzernfeld – RAin Barbara Schmitz, BAY GmbH Wirtschaftsprüfungsgesellschaft Rechtsanwaltsgesellschaft, München – RA Dr. Christian Schröder, Partner und Leiter des Fachbereichs IP/IT & Data Protection Practice Group in der Kanzlei ORRICK, HERRINGTON & SUTCLIFFE LLP, Düsseldorf – RA Dr. Jyn Schultze-Melling, LL.M., CIPP/E, Partner, KPMG Law Rechtsanwaltsgesellschaft, Berlin – RA Thorsten Sörup, Partner, Andersen Rechtsanwaltsgesellschaft Steuerberatungsgesellschaft mbH, Frankfurt/M. – Prof. Dr. Indra Spiecker gen. Döhmann, LL.M., Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaften/Direktorin Forschungsstelle Datenschutz, Goethe-Universität Frankfurt – Prof. Dr. Björn Steinrötter, Juniorprofessor für IT-Recht und Medienrecht, Universität Potsdam – Barbara Thiel, Die Landesbeauftragte für den Datenschutz Niedersachsen a.D., Hannover – RA Florian Thoma, Senior Director, Global Data Privacy, Accenture AG, stv. Leiter des AK Datenschutz des Bitkom e.V. – Prof. Dr. Marie-Theres Tinnefeld, Professorin für Datenschutz und Wirtschaftsrecht, Hochschule München – Michael Will, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Ansbach

ZD FOKUS

Andreas Schmidt LfDI Mecklenburg-Vorpommern veröffentlicht Tätigkeitsbericht für das Jahr 2024

ZD-Aktuell 2026, 01142

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV), Sebastian Schmidt, hat am 3.2.2026 den 20. Tätigkeitsbericht zum Datenschutz für das Berichtsjahr 2024 vorgelegt. Neben der Darstellung von datenschutzrechtlichen Themen (zB Videoüberwachung oder Künstliche Intelligenz) wird die beratende Ausrichtung der Aufsichtsbehörde betont.

Im Vorwort hebt der LfDI MV die anhaltende Digitalisierung im öffentlichen und privaten Sektor hervor, welche zwar notwendig sei, gleichzeitig aber zu einem Anstieg von Gefahren durch erweiterte Zugriffsmöglichkeiten auf personenbezogene Daten führen könne. Größer werde somit auch das Bedürfnis nach Datenschutz als Grundrechtsschutz. Wichtig sei dabei die frühzeitige Berücksichtigung entsprechender Vorgaben, um den Mehraufwand durch die nachträgliche Umsetzung gesetzlicher Anforderungen zu vermeiden. Erfreulicherweise lasse sich in dieser Hinsicht beobachten, dass der LfDI MV mittlerweile häufig in einer frühen Phase beratend eingebunden werde.

Im Jahr 2024 verzeichnete die Aufsichtsbehörde insgesamt 969 eingehende Beschwerden. Dies stellt eine Zunahme gegenüber dem Vorjahr (898) dar. Im Gegensatz dazu sank die Zahl der gemeldeten Datenschutzverletzungen gem. Art. 33 Abs. 1 DS-GVO auf 290 Meldungen (Vorjahr: 401). In diesem Kontext zeigte sich bei den Verantwortlichen eine wachsende Sensibilität für die Sicherheit von IT-Systemen, welche durch Beratungen der Aufsichtsbehörde weiter ausgebaut werden soll.

Positive Rückschlüsse zieht der LfDI MV zudem aus den im Berichtszeitraum durchgeführten Vor-Ort-Kontrollen (zB bei Videoüberwachung, S. 36). Denn solche erlauben neben einer direkten Kommunikation mit dem Verantwortlichen sowie der gezielten Klärung von Fragen auch die unmittelbare Einordnung der tatsächlichen Gegebenheiten, wodurch Aufwände und teilweise Verwaltungsverfahren vermieden werden können (S. 8).

Des Weiteren umfasst der rd. 80-seitige Tätigkeitsbericht ausgewählte thematische Schwerpunkte, insb.:

- „Technik und Organisation" (Kap. A.3.): zB Einsatz von Künstlicher Intelligenz (S. 11); Überarbeitung der Orientierungshilfe der Datenschutzkonferenz (DSK) zu Digitalen Diensten Version 1.2 (S. 16)
- „Wirtschaft" (Kap. A.5.): zB Videoüberwachung in Fitnessstudios (S. 35) oder auf einem Musikfestival (S. 37); Auskunfteien (S. 40)
- „Vereine, Parteien und Beschäftigtendatenschutz" (Kap. A.10.): zB Ungesicherte Aufbewahrung von Beschäftigtendaten (S. 63)
- „Bußgeldstelle und Justiziariat" (Kap. A.11.): zB Unbefugte Datenabfragen aus dienstlichen Systemen (S. 68); Ungesicherte Aufbewahrung von Gesundheitsdaten (S. 69)

ZB befasste sich die Aufsichtsbehörde aufgrund einer Beschwerde mit der „Einholung von Selbstauskünften bei Mietinteressierten" (S. 38). Die datenschutzrechtliche Zulässigkeit der Verarbeitung richte sich – wie aus der DSK-Orientierungshilfe Einholung von Selbstauskünften bei Mietinteressenten Version 1.0 (dazu ZD-Aktuell 2024, 01571) hervorgeht – nach der jeweiligen Phase des Auswahlverfahrens. Während für die Vereinbarung eines Besichtigungstermins Angaben zur Identifikation (zB Name, Vorname, Anschrift) auf Grundlage der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erhoben werden dürften, sei die Abfrage ergänzender Angaben (zB wirtschaftliche Verhältnisse) zu diesem Zeitpunkt regelmäßig unzulässig. Spätestens jedoch durch die „Erklärung der Mietinteressierten, eine konkrete Wohnung anmieten zu wollen, entsteht ein vorvertragliches Schuldverhältnis", sodass der Vermieter gem. Art. 6 Abs. 1 lit. b DS-GVO weitere Daten anfordern könne.

Vgl. auch Zur DSK-Orientierungshilfe „Digitale Dienste" vgl. ZD-Aktuell 2024, 01914; zur unbefugten Datenabfrage in Krankenhäusern vgl. Schmidt ZD-Aktuell 2024, 01657; Praxistipps zur Umsetzung des Datenschutzes im Berufsalltag von Heilberufen vgl. Schmidt ZD-Aktuell 2025, 01136; zur Einholung von Selbstauskünften bei Mietinteressenten ZD-Aktuell 2024, 01571 und ZD-Aktuell 2022, 00013.

Andreas Schmidt, LL.M.
ist Wirtschaftsjurist und bei der TÜV Saarland Solutions GmbH in Bonn tätig.

Sandra Schmitz-Berndt
Österreich: Datenschutzbehörde untersagt rechtswidriges Tracking von Schülern durch Microsoft

ZD-Aktuell 2026, 01155

Mit Bescheid v. 26.1.2026 hat die österreichische Datenschutzbehörde (DSB) (GZ: D135.026, 2025-0.768.263) festgestellt, dass die Microsoft Corporation personenbezogene Daten einer minderjährigen Beschwerdeführerin, die Microsoft 365 Education im schulischen Kontext verwendete, unrechtmäßig verarbeitet hat, und verpflichtete die Microsoft Corporation, innerhalb einer Frist von vier Wochen den Einsatz technisch nicht notwendiger Cookies ohne Einwilligung der Betroffenen hinsichtlich aller Nutzer zu unterlassen.

Hintergrund der Beschwerdesache ist, dass das Bundesministerium für Bildung, Wissenschaft und Forschung österreichischen (Bundes-)Schulen für den digitalen Unterricht Clouddienste privater Anbieter zur Verfügung stellt. Grundlage ist eine Rahmenvereinbarung u.a. mit der europäischen Niederlassung der Microsoft Corporation (Microsoft Ireland Operations Limited bzw. Microsoft Austria EDU). Verwendet wird insbesondere Microsoft 365 Education, das Anwendungen wie Word, Teams und SharePoint umfasst. Lehrkräften und Schülern werden dabei E--Mail-Adressen und Cloudspeicher bereitgestellt. Auf dem Endgerät der Bf., die im Verfahren durch die Nichtregierungsorganisation None of Your Business (NOYB) vertreten wurde, wurden im Juli 2023, während der Verwendung ihres Microsoft-Schul-Accounts und der Erstellung eines Word-Dokuments in der Online-Version (Browser-Version) von Microsoft 365 Education, u.a. mehrere in der Beschwerde näher bezeichnete Cookies durch die Anwendung installiert.

Bereits in der Beweiswürdigung setzte sich die DSB eingehend mit der Konzernstruktur von Microsoft auseinander, um zu klären, ob sich die Beschwerde zutreffend gegen die Microsoft Corporation in den USA richtet oder vielmehr eine europäische Tochtergesellschaft der richtige Beschwerdegegner wäre. Ausgehend davon, dass am Hauptsitz in den USA grundsätzliche Entscheidungen getroffen werden und bei der Nutzung des streitgegenständlichen Produkts personenbezogene Daten für eigene Geschäftszwecke des Konzerns verarbeitet werden, stellt die DSB fest, dass die Microsoft Corporation als datenschutzrechtlich Verantwortliche iSd Art. 4 Nr. 7 DS-GVO handelt. Die mögliche Mitverantwortung von Microsoft Ireland Operations wird zwar erwähnt, aber nicht vertieft, da diese nicht Partei des Verfahrens war. Somit ist die Microsoft Corporation für das Setzen und Auslesen der eingesetzten (Tracking-)Cookies sowie für die Übermittlung und weitere Verarbeitung jener personenbezogenen Daten anzusehen, die sie im Zusammenhang mit der Nutzung von Microsoft 365 Education erhält und zu eigenen Zwecken verarbeitet.

Die DSB stellte fest, dass für den Einsatz der Cookies keine Einwilligung erteilt worden war. Eine aktive Einwilligung war jedoch gem. § 165 Abs. 3 öTKG notwendig, da die genannten Cookies, die u.a. der Reichweitenmessung dienten, personenbezogene Daten enthielten und technisch nicht notwendig waren. Da kein Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO für eine zulässige Datenverarbeitung vorlag, war diese rechtswidrig. Zudem kam die DSB zu dem Ergebnis, dass eine Verletzung des Grundsatzes der Verarbeitung nach Treu und Glauben (Fairnessgrundsatz) gem. Art. 5 Abs. 1 lit. a DS-GVO gegeben ist, da durch die fehlende Einwilligung die Entscheidungsautonomie der Bf. beeinträchtigt war, die Möglichkeit eines späteren Widerrufs entfiel, die Kontrolle über die Datenverarbeitung eingeschränkt war und ein deutliches Kräfteungleichgewicht zwischen der Nutzerin und dem Unternehmen bestand.

Die Rechtswidrigkeit der Verarbeitung personenbezogener Daten beschränkt sich auf den Einsatz von (Tracking-)Cookies und ausdrücklich nicht auf die grundsätzliche Bereitstellung des Produkts Microsoft Education 365 und die Datenverarbeitung ausschließlich zu schulischen Zwecken. Da Microsoft überhaupt keinen Versuch unternommen hatte, eine Einwilligung für die Verarbeitung einzuholen, spielte das Alter der Betroffenen für die Frage einer eventuellen Gültigkeit einer Einwilligung letztlich bei der Entscheidungsfindung keine Rolle.

Die Entscheidung ist bereits die zweite in dieser Angelegenheit. Im Juni 2024 hatte NOYB zwei Beschwerden im Zusammenhang mit der Verwendung der Microsoft-Software für Unterrichtszwecke bei der DSB eingereicht. Hinsichtlich der weiteren Beschwerde hatte die DSB bereits im Oktober 2025 (GZ. D135.027, 2025-0.477.534) u.a. festgestellt, dass die betroffene Schule und das Bundesministerium für Bildung, Wissenschaft und Forschung als datenschutzrechtlich Verantwortliche das Recht der Bf. auf Auskunft gem. Art. 15 DS-GVO sowie auf Information gem. Art. 13 DS-GVO verletzt hatten, indem sie keine vollständige Auskunft über die bei der Nutzung von Microsoft Education 365 verarbeiteten Daten erteilt hatten.

■ Vgl. auch Hoffmann ZD-Aktuell 2024, 01806 mwN; Hessel ZD-Aktuell 2025, 01471 und Stoklas ZD-Aktuell 2025, 01412.

Dr. Sandra Schmitz-Berndt LL.M., LL.M., ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

DSK fordert klare gesetzliche Regelung für das Polizeiprojekt P20-Datenhaus

ZD-Aktuell 2026, 01144

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat auf ihrer Zwischenkonferenz am 29.1.2026 in Berlin mit einem einstimmigen Entschluss den Gesetzgeber aufgefordert, eine rechtliche Grundlage für den Betrieb des Polizeiprojekts P20-Datenhaus zu schaffen.

In dem Projekt P20 soll für die Polizeibehörden des Bundes und der Länder eine digitale Infrastruktur erstellt und dafür die stark zersplitterten polizeilichen IT-Systeme von Bund und Ländern modernisiert und harmonisiert werden. Ein wichtiger Schritt auf dem Weg zur Einführung der Software ist die Errichtung eines gemeinsamen Datenhauses, welches das zentrale Element der neuen IT-Infrastruktur bilden soll. Bisher fehlen für den Betrieb des gemeinsamen Datenhauses jedoch klare rechtliche Grundlagen sowie klare Reglungen zu den datenschutzrechtlichen Verantwortlichkeiten. Diese sind aber nötig, um den Betrieb des P20-Datenhauses zügig und rechtssicher weiterzuentwickeln.

CEF 2025: Ergebnisse der europaweiten Aktion zur Umsetzung des Rechts auf Löschung ZD-Aktuell 2026, 01159

Die Ergebnisse des „Coordinated Enforcement Framework" (CEF), einer europaweiten Aktion zur Umsetzung des Rechts der Bürgerinnen und Bürger auf Löschung ihrer personenbezogenen Daten in der Praxis liegen vor. Aus den Ergebnissen der Befragung haben die Aufsichtsbehörden Empfehlungen für Verantwortliche erarbeitet.

Der Europäische Datenschutzausschuss (EDSA) hat seine europaweite Prüfaktion zur Umsetzung des Rechts auf Löschung (s. dazu ZD-Aktuell 2025, 01202) beendet. Die 32 beteiligten europäischen Aufsichtsbehörden hatten einen einheitlichen Fragebogen an verantwortliche Stellen übersandt. 764 Behörden, Unternehmen und weitere Verantwortliche, darunter 60 in Deutschland, haben darauf geantwortet. Die Datenschutzbehörden haben daraus abgeleitet Empfehlungen für Verantwortliche und die Aufsichtsbehörden sowie den EDSA formuliert, die nun online im Abschlussbericht abrufbar sind. Die europaweite Aktion hatte das Ziel, den Aufsichtsbehörden genauer aufzuzeigen, wo genau Probleme bei der Umsetzung des Rechts auf Löschung liegen.

Die Antworten der Behörden, Unternehmen und anderen verantwortlichen Stellen waren aussagekräftig: Die Einhaltung der Datenschutzanforderungen des Art. 17 DS-GVO ist abhängig von der Größe, dem Sektor und der Branche, sowie der Anzahl der erhaltenen Löschersuchen, Verarbeitungsvorgängen sowie Kategorien personenbezogener Daten, die verarbeitet werden. Wesentliche Herausforderungen im Hinblick auf die Umsetzung von Art. 17 DS-GVO waren für Verantwortliche, dass mitunter klare interne Regelungen fehlen, wann und wie zu löschen ist, dass teilweise keine internen Schulungen durchgeführt werden und Rechtsunsicherheiten bei der Prüfung von Ausnahmetatbeständen und Aufbewahrungsfristen sowie bei den Anforderungen an die Löschung personenbezogener Daten in Back-Ups und bei den Anforderungen an die Anonymisierung von Daten bestehen.

Der EDSA-Abschlussbericht gibt zu den genannten Herausforderungen Empfehlungen für Verantwortliche. Zugleich dienen sie den Aufsichtsbehörden auch als eine Richtschnur, wenn sie mit Verantwortlichen ins Gespräch gehen. Der deutsche Annex zum EU-Abschlussbericht enthält eine Vielzahl an „Best Practices" zu den Themenkomplexen, die abgefragt wurden. Neben dem Fokus auf Tatsachenfeststellung („fact-finding") des CEF 2025 haben einige europäische Aufsichtsbehörden auch formelle Untersuchungen eingeleitet, bereits laufende Untersuchungen fortgesetzt oder planen auf Grundlage der gewonnenen Erkenntnisse, entsprechende weiterführende Maßnahmen umzusetzen.

■ Vgl. hierzu auch ZD-Aktuell 2025, 01202; ZD-Aktuell 2024, 01570; ZD-Aktuell 2025, 01107; ZD-Aktuell 2022, 01230; Roßnagel ZD 2021, 188; Stürmer ZD 2020, 626; LG Frankfurt/M. ZD 2019, 410; Leutheusser-Schnarrenberger ZD 2015, 149 und Kodde ZD 2013, 115.

Axel Spies USA: Kalifornien zwingt Datenhändler mit „Delete Request and Opt-out Platform" zum kollektiven Löschen ZD-Aktuell 2026, 01152

Mit der zum 1.1.2026 gestarteten „Delete Request and Opt-out Platform" (DROP) hat die California Privacy Protection Agency (CalPrivacy) ein in den USA bislang einzigartiges Instrument geschaffen: Verbraucherinnen und Verbraucher in Kalifornien können mit einer einzigen zentralen Anfrage die Löschung ihrer personenbezogenen Daten bei sämtlichen registrierten Datenhändlern („data brokers") verlangen. Obwohl die Pflicht zur tatsächlichen Umsetzung der Löschersuchen erst ab dem 1.8.2026 greift, haben sich bis dato mehr als 176.000 Kalifornier auf der Plattform registriert.

Besonders relevant für Unternehmen ist die äußerst weite gesetzliche Definition des „data broker". Auch Unternehmen, die „nur" Daten aus Drittquellen aggregieren – ohne direkte Kundenbeziehung – können erfasst werden. Die Regeln erfassen auch und gerade Unternehmen außerhalb Kaliforniens, sofern sie personenbezogene Daten kalifornischer Verbraucher sammeln und an Dritte „verkaufen", ohne zu diesen Verbrauchern eine unmittelbare Beziehung zu unterhalten. Verstöße gegen die Registrierungspflicht werden mit 200 US-Dollar pro Tag sanktioniert; unterlassene Löschungen können mit 200 US-Dollar pro Datensatz und Tag geahndet werden – ein erhebliches Bußgeldrisiko.

DROP könnte sich – ähnlich wie der California Consumer Privacy Act – zu einem regulatorischen Vorbild (evtl. auch für Europa) entwickeln und den Maßstab für weitere US-Bundesstaaten setzen (California Effect).

Regulatorischer Kontext: CCPA, Delete Act und die weite Definition des „Data Broker"

Die rechtliche Grundlage für DROP ist der Delete Act aus dem Jahr 2023 (dazu ausf. Spies ZD-Aktuell 2024, 01505) mit einer AusführungsVO aus November 2025, der das bestehende Datenschutzregime in Kalifornien ergänzt. Dieses Gesetz und die VO ergänzen den California Consumer Privacy Act (CCPA), das erste umfassende Verbraucherdatenschutzgesetz in den USA (Spies ZD 2023, 716; MMR 2022, 839). Der CCPA und seine Weiterentwicklungen gewähren kalifornischen Verbrauchern unter anderem diverse Auskunfts--, Lösch- und Widerspruchsrechte.

Der Delete Act adressiert gezielt darauf aufbauend die Datenhändler-Branche. Als „data broker" gilt danach jedes Unternehmen, das wissentlich personenbezogene Daten von Verbrauchern erhebt und an Dritte verkauft, ohne zu diesen Personen eine direkte Geschäftsbeziehung zu unterhalten: „‚Data broker' means a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." – California Civil Code § 1798.99.80(c) (as adopted by the California Delete Act / SB 362).

Diese Definition ist bewusst weit gefasst (Spies ZD-Aktuell 2024, 01505). Erfasst sein können etwa:

- Unternehmen, die personenbezogene Daten aus verschiedenen Quellen aggregieren und weiterveräußern,
- Anbieter von Datenanreicherungsdiensten,
- Betreiber von Tracking- oder Analyseinfrastrukturen, sofern sie personenbezogene Daten eigenständig kommerzialisieren sowie
- Unternehmen außerhalb Kaliforniens, sofern sie personenbezogene Daten kalifornischer Verbraucher verarbeiten und verkaufen.

Der Schlüsselbegriff „sell"(„verkauft") im kalifornischen Datenschutzrecht ist sehr weit gefasst. Er umfasst nicht nur klassische Geldzahlungen, sondern auch jeden Transfer oder jede Übermittlung personenbezogener Daten an eine andere juristische Person gegen einen „werthaltigen Vorteil" – also zB gegen Geld, Dienstleistungen, Provisionen oder vergleichbare Leistungen. Dieser Umfang entspricht der CCPA-Definition des Begriffs „sale" (dazu Spies ZD-Aktuell 2018, 04318; Spies ZD-Aktuell 2020, 07004; Spies MMR 2023, 70). Entscheidend ist auch nicht der Sitz des Unternehmens, sondern die Verarbeitung personenbezogener Daten von Personen mit Wohnsitz in Kalifornien. Damit entfaltet das Gesetz faktisch extraterritoriale Wirkung – vergleichbar mit der DS-GVO und diversen anderen EU-Vorschriften.

Die erfassten Datenhändler müssen sich jährlich bis zum 31. Januar bei CalPrivacy registrieren und eine Gebühr entrichten. Unterbleibt die Registrierung, droht ein Bußgeld von 200 USD pro Tag. Ab dem 1.8.2026 müssen registrierte Datenhändler zudem sämtliche über DROP eingehenden Löschersuchen innerhalb von 45 Tagen bearbeiten. Unterlassene oder verspätete Löschungen können mit 200 USD pro betroffenem Datensatz und Tag sanktioniert werden. Bei größeren Datenbeständen entsteht dadurch ein erhebliches kumulatives Haftungsrisiko.

Wichtig ist zudem, dass Unternehmen auch dann als Datenhändler gelten können, wenn sie ihrer Registrierungspflicht nicht nachgekommen sind. Die Nicht-Registrierung schützt somit nicht vor der materiellen Löschpflicht – im Gegenteil erhöht sie das Risiko zusätzlicher Sanktionen.

Die Rolle von CalPrivacy: Proaktive Aufsicht und technologische Infrastruktur

CalPrivacy ist die erste eigenständige Datenschutzaufsichtsbehörde in den USA mit dem gesetzlichen Mandat für die Datenschutzdurchsetzung. Sie treibt die praktische Umsetzung des Delete Act aktiv voran. Nach einer eher unspektakulären Einführung der Plattform hat die Behörde am 26.1.2026 zur „Privacy Week" in einer Pressemitteilung bekannt gegeben, dass sich bereits über 176.000 Personen für DROP registriert haben. Diese Zahl ist insofern bemerkenswert, als die Behörde bislang keine breit angelegte Werbekampagne gestartet hatte. Die hohe Resonanz zeigt, dass Verbraucher ein erhebliches Bedürfnis nach effektiven, niedrigschwelligen Löschmöglichkeiten haben.

Technisch basiert DROP auf einem zentralen, staatlich betriebenen System. Verbraucher identifizieren sich über ein sicheres Identitäts-Gateway (California Digital ID Platform); ihre Daten werden in gehashter Form an die Plattform übermittelt. Die registrierten Datenhändler müssen sich regelmäßig – mindestens alle 45 Tage – in ihre geschützten Konten einloggen oder eine API-Schnittstelle nutzen, um neue Löschanfragen abzurufen und zu verarbeiten. Anschließend ist der Status der Bearbeitung an die Plattform zurückzumelden.

CalPrivacy hat bereits mehrfach deutlich gemacht, dass sie die Registrierungspflichten konsequent durchsetzt und entsprechende Verfahren eingeleitet hat. Zudem wurde innerhalb der Behörde eine spezialisierte Einheit eingerichtet, die gezielt die Einhaltung der Pflichten durch die Data Brokers überwacht. Die Ankündigung einer „aggressiven" Durchsetzung signalisiert, dass DROP kein symbolisches Instrument ist, sondern ein ernstzunehmendes Vollzugsregime begründet.

Vergleich mit den europäischen Regelungen für Datenhändler

Im europäischen Kontext existiert kein eigenständiger „Data Broker Act". Die Tätigkeit von Datenhändlern unterliegt vielmehr den allgemeinen Vorgaben der DS-GVO und evtl. dem Digital Markets Act (DMA) für große Plattformbetreiber. Die DS-GVO kennt kein spezielles Berufsbild des Datenhändlers wie im Delete Act. Unternehmen, die personenbezogene Daten handeln oder aggregieren, sind als Verantwortliche einzuordnen, sofern sie über Zwecke und Mittel der Verarbeitung entscheiden. Sie unterliegen damit insb. den Regeln der Betroffenenrechten einschließlich Löschungsrecht („Recht auf Vergessenwerden", Art. 17 DS-GVO) und ggf. Datenschutz-Folgenabschätzungen usw.

Anders als in Kalifornien existiert jedoch in der EU kein staatlich betriebenes zentrales Löschportal, über das Betroffene mit wenigen Klicks sämtliche Datenhändler adressieren können. Verbraucher müssen ihre Rechte grds. ggü. jedem einzelnen Verantwortlichen geltend machen. Zwar bieten einzelne private Initiativen oder Dienstleister Unterstützung an, ein verpflichtendes, zentrales System fehlt bislang. In dieser Hinsicht geht Kalifornien einen innovativen Schritt: Das Recht auf Löschung wird nicht nur formal gewährt, sondern prozessual gebündelt und technisch operationalisiert. Die extraterritoriale Anknüpfung des Delete Act ist im Gesetz nicht explizit angesprochen aber ergibt sich aus dem CCPA und dem Kontext „doing business in California." Beide Regime stellen auf die Betroffenheit von Personen im jeweiligen Hoheitsgebiet ab, nicht allein auf den Unternehmenssitz. Für international tätige Datenhändler kann dies zu einer faktischen Harmonisierung ihrer Compliance-Strategien führen – oder, bei divergierenden technischen Anforderungen verschiedener US-Bundesstaaten, zu zusätzlicher Komplexität.

California Effect?

Für europäische Unternehmen mit US-Bezug, insb. mit Daten kalifornischer Verbraucher, empfiehlt sich eine sorgfältige Analyse, ob sie unter die weite Definition des Datenhändlers fallen. Wer personenbezogene Daten ohne direkte Kundenbeziehung sammelt und monetarisiert, könnte schneller als erwartet in den Anwendungsbereich von DROP geraten – mit entsprechendem Sanktionspotenzial. Kalifornien setzt damit erneut einen regulatorischen Impuls, der über die Grenzen des Bundesstaates hinauswirkt. Ob andere US-Bundesstaaten nachziehen (wie zB New York) und ob sich langfristig ein föderal fragmentiertes oder stärker harmonisiertes System entwickelt, bleibt abzuwarten. Fest steht jedoch: Die Zeiten unregulierter Datenhändler gehen auch in den USA ihrem Ende entgegen. Ob der deutsche oder der EU-Gesetzgeber die Regeln aufgreift und es einen „California Effect" als Gegenstück zum „Brussels Effect" (Spies ZD 2026, 124) geben wird, wird sich noch zeigen.

■ Vgl. hierzu auch Spies ZD-Aktuell 2024, 01505; Spies ZD 2023, 716; Spies MMR 2022, 839; Spies ZD-Aktuell 2018, 04318; Spies ZD-Aktuell 2020, 07004; Spies MMR 2023, 70 und Spies ZD 2026, 124.

RA Dr. Axel Spies
ist Partner der Potomac Law Group in Washington DC und Mitherausgeber der ZD.

BfDI: Ergebnisse der Konsultation zu personenbezogenen Daten in KI-Modellen

ZD-Aktuell 2026, 01162

Im Zeitraum vom 10.7.2025 bis zum 31.8.2025 führte die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) ein Konsultationsverfahren zum datenschutzkonformen Umgang mit personenbezogenen Daten in KI-Modellen durch. Die Ergebnisse wurden nun veröffentlicht.

In seiner Stellungnahme 28/2024v. 18.12.2024 stellte der Europäische Datenschutzausschuss fest, dass KI-Modelle personenbezogene Daten enthalten können, wenn sie mit personenbezogenen Daten trainiert wurden. Diese Feststellung wirft bedeutende Fragen im Hinblick auf den Schutz personenbezogener Daten auf. Die BfDI sah dementsprechend die Notwendigkeit, datenschutzrechtliche Herausforderungen bei der Planung, dem Training und der Nutzung solcher Modelle systematisch zu thematisieren. Der Schwerpunkt der Konsultation lag dabei auf großen Sprachmodellen (LLMs).

Ziel der Konsultation war es, in Anerkennung der technischen und rechtlichen Komplexität konkrete praktische Erfahrungen, technische Einschätzungen und normative Überlegungen von Akteurinnen und Akteuren aus verschiedenen Bereichen einzuholen. Gegenstand der Konsultation waren sieben Fragen zum Umgang mit personenbezogenen Daten in KI-Modellen. Eine weitere offene Frage diente dazu, ergänzende Hinweise aufzugreifen. Zusätzlich zur schriftlichen Konsultation führte die BfDI mehrere Austauschformate mit Vertreterinnen aus Wissenschaft, Wirtschaft, Zivilgesellschaft und öffentlichen Stellen durch. Insgesamt wurden 30 Stellungnahmen für den Konsultationsbericht ausgewertet.

Als Haupterkenntnisse fasst der Bericht die folgenden Ergebnisse zusammen, die im Bericht jeweils weiter ausgeführt werden:

- Bzgl. der Frage der Anonymität eines großen Sprachmodells lässt sich ein diverses Meinungsbild feststellen. Eine Mehrheit spricht sich für eine Anonymität des Modells unter gewissen Umständen aus.
- Die Positionen bzgl. des Risikos der Extraktion personenbezogener Daten variieren.
- Es wurden diverse technische Maßnahmen zur Reduktion des Extraktionsrisikos identifiziert.
- Die Eingabe eines Prompts führt nach mehrheitlicher Auffassung nur dann zu einer Verarbeitung der memorisierten Daten im KI-Modell, wenn sich diese Daten im Output wiederfinden.
- Es wurden einige Methoden zur Abschätzung der Menge personenbezogener Daten in LLMs vorgeschlagen.
- Bzgl. der Menge an personenbezogenen memorisierten Daten verwies die Mehrheit an Stellungnahmen darauf, dass eine rein quantitative Einschätzung nicht zielführend sei.
- Zu der Frage der Betroffenenrechte wurde für das Auskunftsrecht empfohlen, die entsprechenden Trainingsdaten, sofern vorhanden, aufzulisten. Bzgl. der Löschung memorisierter Daten aus dem Modell sprach sich eine Mehrheit der Stellungnahmen für Maßnahmen auf Systemebene aus, insb. da Methoden wie Machine Unlearning noch nicht einwandfrei einsetzbar seien.

Vgl. hierzu auch Hense MMR 2025, 927; Stoklas ZD-Aktuell 2025, 01303; Spies ZD 2025, 547; Schmitz ZD 2025, 61; ZD-Aktuell 2026, 01114; Schäfer ZD 2025, 12; Kindshofer ZD 2024, 673 und Le/Treibel ZD 2024, 370.

Christina Meese Schweden: Bußgeld gegen Vereinsverwaltungsplattform Sportadmin nach Datenleck

ZD-Aktuell 2026, 01153

Mit Entscheidung v. 26.1.2026 hat die schwedische Datenschutzbehörde (Integritetsskyddsmyndigheten – IMY) ein Bußgeld iHv 6 Mio. SEK (umgerechnet etwa 560.000 EUR) gegen die Plattform Sportadmin i Skandinavien AB verhängt, die Vereinen verschiedene Möglichkeiten zur Online-Verwaltung und -Organisation ihrer Mitglieder bereitstellt. Grund für das Bußgeld war ein Datenschutzvorfall im Zusammenhang mit einer Cyberattacke im Januar 2025, der zur Übertragung und Veröffentlichung von personenbezogen Daten von über 2 Mio. Betroffenen, darunter auch und vor allem minderjähriger Mitglieder etwa von Fußballvereinen, an und durch Unbekannte geführt hatte. Sportadmin hatte den Vorfall zwar ordnungsgemäß gemeldet, hatte nach Auffassung der IMY aber keine ausreichenden Sicherheitsmaßnahmen im Vorfeld ergriffen, um ihn zu verhindern.

Sportadmin bietet digitale Kommunikationsdienste im skandinavischen Raum an, darunter ein webbasiertes Verwaltungstool für Sportvereine und andere Organisationen, das verschiedene Funktionen für die Mitgliederverwaltung und Rechnungsstellung sowie auch die vereinfachte Erstellung von Webpräsenzen ermöglicht. Eine ebenfalls angebotene mobile Anwendung kann dabei nicht nur von den Leitern der Vereine, sondern auch von den Mitgliedern und den Erziehungsberechtigten der Mitglieder genutzt werden, um ihre Mitgliedschaft zu verwalten und sich mit ihrem Verein zu vernetzen. Am 16.1.2025 stellte Sportadmin einen Cyberangriff auf seine Systeme fest, der eine Schwachstelle in der SQL-Programmierung ausnutzte und sich so Zugriff auf den Server und die hierauf gespeicherten Daten verschaffte. (Mit-)Ursache war offenbar eine Codeänderung, die 2022 eine spezielle Variable in der Webseite von Sportadmin eingefügt und dabei Nutzerberechtigungen verändert hatte, aber nicht gegen SQL-Injektionen geschützt wurde. Die Daten, die auf diese Weise an den Angreifer übertragen wurden, wurden im März 2025 im Darknet veröffentlicht und beinhalteten u.a. vollständige Namen und Kontaktdaten, Geschlecht, Personennummern, Informationen über die Beziehung zwischen Erziehungsberechtigtem und Mitglied, Nationalität sowie die Sportart und den Verein, mit denen ein Registrierter in Verbindung stand. Darüber hinaus wurden vereinzelt innerhalb der Plattform – was den Betreibern nicht bekannt war – besondere Kategorien personenbezogener Daten wie Informationen zu Behinderungen oder Allergien verarbeitet. Betroffen von dem Angriff waren 2.126.075 Registrierte, die anhand ihrer Personennummer identifizierbar waren und bei denen es sich – wegen der Ausrichtung der Plattform auf lokale Sportvereine – zu einem großen Teil um Kinder und Jugendliche handelte. Sportadmin behandelte den Vorfall sofort nach seinem Bemerken als schwerwiegenden Sicherheitsvorfall und ergriff entsprechende Maßnahmen zur Minimierung der Schäden für Kunden und Nutzer, inklusive einer sofortigen

Abschaltung aller Dienste, und Kommunikation mit den Vereinen und Nutzern. Auch wurde der Vorfall der IMY gemeldet.
Die DS-GVO-konforme Reaktion änderte aber nichts an der Beurteilung der IMY, dass die im Vorfeld ergriffenen Maßnahmen zur Verhinderung eines solchen Vorfalls nicht ausreichend waren. Art. 32 Abs. 1 DS-GVO, der von Verantwortlichen geeignete technische und organisatorische Maßnahmen fordert, um ein angemessenes Sicherheitsniveau für die personenbezogenen Daten in dessen Diensten zu gewährleisten, sei nicht beachtet worden. Insbesondere hätte es vor dem Hintergrund der großen Menge an verarbeiteten Daten und deren teils besonderer Sensibilität (Minderjährige, Gesundheitsdaten, direkte Identifizierbarkeit der Nutzer etc.) besonders hoher Sicherheitsanforderungen bedurft, die nicht ergriffen worden seien. Sportadmin sei trotz des Wissens um die erhöhten Risiken von SQL-Injektionen nicht in der Lage gewesen, zu erkennen, dass die zum Schutz der Dienste vor solchen Eingriffen getroffenen Maßnahmen unzureichend waren. Auch bemängelte die Behörde, dass Sportadmin nicht in der Lage war, den Angriff rechtzeitig zu entdecken, um ihn zu verhindern oder zumindest seine Folgen zu begrenzen.
Bei der Bemessung des Bußgelds orientierte sich die IMY zunächst am Jahresumsatz der Lime-Gruppe, zu der Sportadmin gehört, und der sich 2024 auf etwa 685 Mio. SEK (etwa 65 Mio. EUR) belief. Erschwerend für die Bußgeldhöhe wurde die Menge und Art der betroffenen personenbezogenen Daten berücksichtigt, insbesondere, dass es sich bei den Betroffenen zu einem großen Teil um Minderjährige, also besonders schutzbedürftige Personen handelte. Zugunsten von Sportadmin wurde die Reaktion des Unternehmens auf den Vorfall und die offene Aufarbeitung in Zusammenarbeit mit der IMY berücksichtigt.

■ Vgl. zu DS-GVO-Bußgeldern in Schweden auch Schmitz-Berndt ZD-Aktuell 2025, 01215; Etteldorf ZD-Aktuell 2024, 01864; Etteldorf ZD-Aktuell 2024, 01693; Kollmann ZD-Aktuell 2023, 01442; Etteldorf ZD-Aktuell 2023, 01275 sowie MMR-Aktuell 2024, 01491 mwN.

Ass. iur. Christina Meese
ist Wissenschaftliche Referentin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

EDSA: Arbeitsprogramm 2026–2028 ZD-Aktuell 2026, 01163

Der Europäische Datenschutzausschuss (EDSA) hat sein Arbeitsprogramm für die Jahre 2026-2027 veröffentlicht.
Das Arbeitsprogramm basiert auf vier Pfeilern:

■ Mit Pfeiler I („Harmonisierung und Förderung von Compliance") plant der EDSA umfangreiche neue oder aktualisierte Leitlinien, u.a. zu Anonymisierung, Pseudonymisierung, berechtigtem Interesse, Kinder-Daten, „Consent or Pay"-Modellen, wissenschaftlicher Forschung, DPO-Guidelines und mehreren Einzelthemen wie Nutzerkonten im E-Commerce. Zudem sollen EU-weit einheitliche Vorlagen für Datenschutz-Folgenabschätzungen, Verarbeitungsverzeichnisse, Datenschutzverletzungen und Datenschutz-Hinweise entstehen. Der EDPB wird außerdem weiter Kodizes, Zertifizierungen und Monitoring-stellen prüfen und die EU-Gesetzgeber zu relevanten Vorhaben beraten.

■ Der Pfeiler II betrifft die Stärkung der gemeinsamen Durchsetzung der DS-GVO. Dazu gehören aktualisierte Leitlinien zu Kooperationsmechanismen wie Art. 60, 61 und 66 DS-GVO, eine Überarbeitung der Bußgeldleitlinien sowie systematische Austauschformate, Taskforces und das Coordinated Enforcement Framework, das 2026 die Transparenzpflichten (Art. 12–14 DS-GVO) überprüft. Zudem sollen technische Systeme wie die IMI-Plattform an neue rechtliche Vorgaben angepasst werden.

■ Pfeiler III widmet sich der wachsenden Zahl digitaler Regulierungsakte. Vorgesehen sind gemeinsame Leitlinien zum Zusammenspiel der DS-GVO mit KI-Verordnung, Digital Markets Act, Digital Services Act, politischer Werbung sowie AML/CFT-Regeln. Auch Best Practices für behördenübergreifende Zusammenarbeit und eine stärkere Einbindung anderer Regulierungsbehörden sind geplant. Zudem will der EDSA die technologische Entwicklungen beobachten und zu Themen wie generativer KI, Data Scraping, Telemetriedaten und Blockchain eigene Leitlinien entwickeln.

■ Pfeiler IV betrifft die internationale Dimension: Der EDSA möchte den globalen Datenschutzdialog stärken, insb. bei der Zusammenarbeit in der Durchsetzung. Er plant weiter an internationalen Datentransfermechanismen zu arbeiten – darunter Angemessenheitsbeschlüsse, Zertifizierungen und Standardvertragsklauseln – und die Kooperation mit Behörden aus Drittstaaten zu intensivieren, insb. solchen aus Ländern mit Angemessenheitsbeschluss.

■ Vgl. hierzu auch ZD-Aktuell 2025, 01431; ZD-Aktuell 2026, 01150; ZD-Aktuell 2026, 01132; Schmitz-Berndt ZD-Aktuell 2025, 01272 und Braun ZD-Aktuell 2024, 01691.

Hannah Waegner BMJV: Referentenentwurf zur IP-Adressspeicherung und Ausweitung der Datenerhebungsbefugnisse im Strafverfahren ZD-Aktuell 2026, 01151

Aktuell läuft das Verfahren für das Gesetz zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren. Der im Dezember vorgelegte Referentenentwurf hat die Verbesserung der Strafverfolgung im Digitalen zum Ziel. Neben einer vorgesehenen Speicherungspflicht für IP-Adressen ermöglicht der Entwurf nach dem Beschluss des BGH (MMR 2024, 676) auch wieder die Funkzellenabfrage bei erheblichen Straftaten. Die vorgesehenen Maßnahmen stoßen nun neben Lob auch auf weitreichende Kritik – so werden etwa erhebliche Zweifel an der Verfassungsmäßigkeit geäußert.
Bereits im Dezember 2025 legt das Bundesministerium für Justiz und Verbraucherschutz (BMJV) den Referentenentwurf des Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren vor. Dieses sieht Änderungen u.a. der StPO, des OWiG, des TKG, des TDDDG sowie des BKAG vor, wie auch aus der Synopse hervorgeht. Mit der Neufassung des § 176 TGK-E sollen Anbieter von Internetzugangsdiensten dazu verpflichtet werden, IP-Adressen von Nutzerinnen und Nutzern vorsorglich und anlasslos für eine Dauer von drei Monaten zu speichern. Während hierbei nur die Speicherung der „Verkehrsdaten zur Identifizierung von Anschlussinhabern" vorgesehen ist, enthält § 175 TKG-E eine Verarbeitungsbefugnis sämtlicher Verkehrsdaten zu Zwecken

ZEITSCHRIFT FÜR DATENSCHUTZRECHT
ZD
EDITORIAL
4/2026

10 Jahre Breyer – zum Personenbezug von Daten

Lesedauer: 7 Minuten

Seit der EuGH vor 10 Jahren in der Rs. Breyer zum Personenbezug dynamischer IP-Adressen auch für Webseitenbetreiber urteilte (EuGH ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel – Breyer), nachdem dieser für Internetzugangsanbieter bereits längere Zeit feststand (EuGH ZD 2012, 29 mAnm Meyerdierks – Scarlet Extended), streiten wir um den Personenbezug von Daten. Zugegebenermaßen taten wir das auch schon vorher, aber die Intensität ist seitdem doch eine andere.

Noch unter Geltung der Datenschutzrichtlinie (RL 95/46/EG) urteilte der EuGH in der Rs. Breyer (EuGH ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel), dass für einen Personenbezug auch eine indirekte Identifizierbarkeit ausreicht, die IP-Adresse also selbst keine unmittelbare Identifizierung der Person zulassen muss, sondern bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, die vernünftigerweise eingesetzt werden können, um die betreffende Person zu bestimmen (Rn. 39 ff.), und zwar auch dann, wenn sie in den Händen Dritter liegen (Rn. 43 ff.). In casu bejahte der EuGH auf Grundlage dieser Kriterien eine Identifizierungsmöglichkeit einer hinter einer IP-Adresse stehenden Person durch einen Webseitenbetreiber auf Grundlage eines rechtlichen Anspruchs zur Erlangung der beim Internetzugangsanbieter zu dieser IP-Adresse gespeicherten Klardaten (Rn. 47). Er dachte dabei wohl an eine Akteneinsicht gem. § 406e StPO aF in Erkenntnisse der Erhebung von Verkehrsdaten gem. § 100g StPO aF (Mantz/Spittka NJW 2016, 3579 (3583)), aus denen sich der hinter einer IP-Adresse stehende Anschlussinhaber ableiten lässt.

Diese Argumentation gilt bis heute fort, wurde das Judiz des EuGH in der Rs. Breyer (ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel) doch nahezu 1:1 in Erwägungsgrund 26 S. 3 DS-GVO aufgenommen. Und damit konnte in der Praxis auch lange und gut gearbeitet werden, wie nicht zuletzt die Entscheidungen des EuGH zum Personenbezug von Pressemitteilungen (EuGH Urt. v. 7.3.2024 – C-479/22 P – OC/Kommision) und Werbe-IDs (EuGH ZD 2024, 328 mAnm Halim/Marosi = MMR 2024, 390 mAnm Keppeler/Schneider – IAB Europe) belegen. Man könnte sagen, es handelt sich um einen beschränkt-objektiven (statt vieler Specht/Müller-Riemenschneider ZD 2014, 71 (74)), bzw. um einen erweitert-relativen Ansatz (statt vieler Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 278), wenn man in der Terminologie der vertretenen Theorien bleiben möchte.

Professorin Dr. Louisa Specht-Riemenschneider
ist Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Bonn.

Dr. Ruben Plum-Schneider
ist Persönlicher Referent der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in Bonn.

Zwei neuere Urteile des EuGH und der Digital Omnibus der EU-Kommission (COM(2025) 837 final) haben allerdings nochmal Schwung in die Debatte gebracht:

So hatte der EuGH 2023 über den Personenbezug von Fahrzeugidentifikationsnummern (FIN) zu entscheiden, die durch den Kfz-Hersteller Scania auf einer Webseite für Werkstätten bereitgestellt wurden (EuGH ZD 2024, 173 mAnm Hanloser – FIN). Im Einklang mit der Rs. Breyer (EuGH ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel) stellte der EuGH zunächst fest, dass die FIN für alle Akteure Personenbezug aufweist, die mit ihr den Halter des zugehörigen Fahrzeugs identifizieren können (Rn. 48). Dies umfasst zB Werkstätten, die für einen bekannten Kunden die FIN zwecks Ersatzteilbeschaffung verarbeiten – beschränkt-objektiver bzw. erweitert-relativer Ansatz, soweit so gut.

Für Diskussionen sorgt indes die beiläufige Ausführung des EuGH, dass die FIN auch „mittelbar für die Fahrzeughersteller, die die FIN bereitstellen, ein personenbezogenes Datum (darstellt), selbst wenn die FIN für sich genommen für die Fahrzeughersteller kein persönliches Datum darstellt" (Rn. 49).

Also einmal personenbezogen, immer personenbezogen?

Muss sich Scania die Identifizierungsmöglichkeit einzelner Werkstätten zurechnen lassen, die sie im Einzelnen gar nicht kennen und auf deren Inanspruchnahme Scania gar keinen Anspruch hat? Ein solcher gänzlich objektiver Ansatz würde zahlreiche Folgeprobleme aufwerfen, insbesondere die Bindung an die DS-GVO mit all ihren Verpflichtungen, obgleich Scania selbst keine Identifizierung vornehmen kann und nicht weiß, wer dies alles könnte. Zwar positioniert sich der EuGH in der darauffolgenden Rs. SRB klar für einen beschränkt-objektiven bzw. erweitert-relativen

Personenbezug, indem er festhält, dass „pseudonymisierte Daten ... nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden" müssen (EuGH ZD 2025, 631 Rn. 86 mAnm Roßnagel und mAnm Baumgartner = MMR 2025, 875 mAnm Monreal – SRB, sowie Grosmann/Luh EuZW 2025, 1112 f.). Der Gerichtshof erwähnt aber auch dort einen „indirekten" Personenbezug unter Bezugnahme auf seine Entscheidung in der Rs. FIN (s. Verweis in EuGH ZD 2025, 631 Rn. 84 mAnm Roßnagel und mAnm Baumgartner = MMR 2025, 875 mAnm Monreal – SRB) – und verwirrt damit die Rechtsanwender.

Man muss ein bisschen genauer lesen, um die Frage, wie es denn nun um den Personenbezug steht, zu beantworten. Denn letztlich verweist der EuGH in der Rs. FIN und in der Rs. SRB in seinen Ausführungen zum Personenbezug auf die Schlussanträge des Generalanwalts aus der Rs. FIN (GA Sánchez-Bordona SA v. 4.5.2023 – C-319/22; Bezugnahme auf Rn. 34 der FIN-Schlussanträge in Rn. 49 des FIN-Urteils; Bezugnahme auf Rn. 49 des FIN-Urteils in Rn. 84 des SRB-Urteils). Und der Generalanwalt verweist wiederum für die Terminologie des mittelbaren Personenbezugs auf den dem Verfahren zugrunde liegenden Vorlagebeschluss des LG Köln v. 4.5.2022 – 84 O 223/20. Die Lektüre des Vorlagebeschlusses wiederum zeigt unmissverständlich: Es besteht allein in dem Umfang ein Personenbezug für den Hersteller zur Debatte, in dem dieser eine „vernünftige tatsächliche oder rechtliche Möglichkeit zur Verfügung (hat), anhand der FIN Rückschlüsse auf eine natürliche Person zu ziehen" (S. 79 des Vorlagebeschlusses).

Es geht dem Generalanwalt und dem EuGH insoweit keineswegs um eine automatische Zurechnung des Personenbezugs iSe objektiven Ansatzes, sondern allein um die konsequente Anwendung der beschränkt-objektiven bzw. erweitert-relativen Theorie, die wir seit der Rs. Breyer kennen.

Das zeigt sich auch in der Conclusio des Generalanwalts zum Thema Personenbezug in der Rs. FIN: Er führt dort aus, dass FIN nur dann „personenbezogene Daten iSv Art. 4 Nr. 1 DS-GVO sind, sofern derjenige, der Zugang zu ihnen hat, über Mittel verfügen kann, die es ihm bei vernünftiger Betrachtung ermöglichen, sie zur Identifizierung des Eigentümers des jeweiligen Fahrzeugs zu nutzen" (GA Sánchez-Bordona SA v. 4.5.2023 – C-319/22 Rn. 42). Weiter heißt es: „Es ist Sache des vorlegenden Gerichts, zu prüfen, ob dem im konkreten Fall so ist" (GA Sánchez-Bordona SA v. 4.5.2023 – C-319/22 Rn. 42). Nur wenn ein Hersteller also ebenfalls über ausreichende Identifizierungsmittel iSv Erwägungsgrund 26 S. 3 DS-GVO verfügt, ist die FIN für ihn personenbezogen, zB beim Bestehen von vertraglichen oder gesetzlichen Auskunftsansprüchen des Herstellers gegen eine Werkstatt.

Letztlich geht es bei der Frage, ob ein Verantwortlicher einen Personenbezug herstellen kann, also um nichts anderes als um Wissenszurechnung (vgl. idS bereits EuGH ZD 2017, 24 Rn. 43 ff. mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel – Breyer; ausführlich dazu auch Roßnagel Anmerkung zu ZD 2025, 631 und Baumgartner Anmerkung zu ZD 2025, 631 sowie Grosmann/Luh EuZW 2025, 1112 f.). Das Wissen Dritter ist als Mittel zur Identifizierung des Betroffenen durch den Verantwortlichen zurechenbar, wenn und soweit sich der Verantwortliche diesem wahrscheinlich bedienen wird (idS auch Golland ZRP 2026, 2).

Damit kommt es nicht darauf an, wessen Sicht bei der Bestimmung des Personenbezugs zugrunde zu legen ist – die des Verantwortlichen oder die jedermanns. Es kommt stets und einzig auf die Sicht des Verantwortlichen an und es stellt sich allein die Frage, ob das Wissen Dritter ein Mittel ist, das nach allgemeinem Ermessen vom Verantwortlichen wahrscheinlich genutzt wird, um die betroffene Person zu identifizieren.

Die Rs. SRB sagt dazu: Verbotene Mittel werden nicht berücksichtigt. Und auch dann, wenn Daten verschlüsselt sind und der Schlüssel dem Verantwortlichen nicht zugänglich ist (zu den genauen Umständen der Rs. SRB vgl. EuGH ZD 2025, 631 Rn. 23 mAnm Roßnagel und mAnm Baumgartner = MMR 2025, 875 mAnm Monreal – SRB), er also nicht über Mittel verfügt, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffene Person zu identifizieren, liegt ein Personenbezug nicht vor. Auch kein mittelbarer Personenbezug:

„Wie in den Rn. 75 bis 77 des vorliegenden Urteils ausgeführt, kann die Pseudonymisierung also je nach den Umständen des Einzelfalls andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, sodass letztere für die anderen Personen nicht oder nicht mehr identifizierbar ist." (EuGH ZD 2025, 631 Rn. 87 mAnm Roßnagel und mAnm Baumgartner = MMR 2025, 875 mAnm Monreal – SRB)

Mitte 2025 hat der BGH dem EuGH erneut Fragen zum Personenbezug vorgelegt und dabei insbesondere danach gefragt, ob für einen Personenbezug bereits die abstrakte Identifizierungsmöglichkeit durch einen Dritten genügt (BGH ZD 2026, 94 mAnm Voigt/Horn = MMR 2026, 203 mAnm Ligocki/Wellmann). Worum es ging? Um IP-Adressen – vielleicht schließt sich also mit diesem Urteil endlich der Kreis zur Rs. Breyer aus dem Jahr 2016.

Lästige Datenschützer

Lesedauer: 7 Minuten

Es wirkt fast wie ein Ritual: Immer wenn Datenschutz unbequem wird, taucht jemand auf, der seine Abschaffung oder zumindest Entschärfung fordert.
Jüngst hat sich der nordrhein-westfälische Ministerpräsident Hendrik Wüst in diese Tradition eingereiht, indem er die Abschaffung des Amts der Landesbeauftragten für den Datenschutz ins Spiel brachte (https://www1.wdr.de/nachrichten/landespolitik/wuest-will-landesdatenschutzbeauftragte-abschaffen-100.html). Ein Vorschlag, der nicht nur politisch kurzsichtig ist, sondern auch verfassungsrechtlich unhaltbar und europarechtlich schlicht ausgeschlossen.

Warum Wüst falsch liegt

Die Idee, die unabhängige Datenschutzaufsicht abzuschaffen, verkennt die grundlegende Funktion dieses Amts: Es ist ein verfassungsrechtlich abgesicherter Schutzmechanismus gegen staatliche und private Eingriffe in die informationelle Selbstbestimmung. Gerade weil Datenschutz manchmal unbequem ist, braucht es eine Instanz, die nicht von politischen Opportunitäten abhängig ist.
Wüst argumentiert, Datenschutz bremse Innovation. Doch das ist ein Scheinargument. Datenschutz ist kein Innovationshindernis, sondern ein Qualitätsmerkmal moderner digitaler Gesellschaften. Innovation, die nur funktioniert, wenn Grundrechte geschliffen werden, ist keine, die Bestand hat.

Verstoß gegen die Verfassung

Die Nordrhein-Westfälische Verfassung (NRW Verf) verpflichtet das Land ausdrücklich zum Schutz der Grundrechte und zur Sicherung rechtsstaatlicher Kontrolle.
Art. 4 Abs. 2 NRW Verf lautet: „Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur in überwiegendem Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig."
Die unabhängige Datenschutzaufsicht ist ein zentraler Bestandteil dieser Kontrollarchitektur. Auch diese unabhängige Kontrolle wird explizit durch die Nordrhein-Westfälische Verfassung garantiert. Art. 77a Abs. 2 NRW Verf lautet: „Der Landesbeauftragte für den Datenschutz ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er kann sich jederzeit an den Landtag wenden."
Die unabhängige Kontrolle abzuschaffen, würde bedeuten, einen verfassungsrechtlich gebotenen Schutzmechanismus zu beseitigen, der gerade verhindern soll, dass staatliche Stellen unkontrolliert personenbezogene Daten verarbeiten.
Zudem ist die Unabhängigkeit der Aufsicht nicht optional. Sie ist verfassungsrechtlich notwendig, weil nur eine unabhängige Stelle effektiv gegen staatliche Behörden vorgehen kann, wenn diese gegen Datenschutzrecht verstoßen.

Rechtsprechung des BVerfG

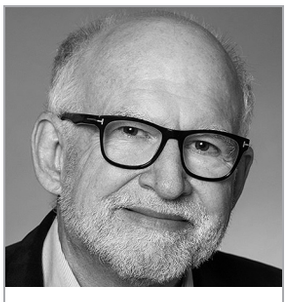
Das BVerfG hat in mehreren Entscheidungen klargestellt, dass Datenschutzaufsicht institutionell unabhängig sein muss. Grundrechte können nur dann wirksam geschützt werden, wenn es unabhängige Kontrollinstanzen gibt, die staatliches Handeln überprüfen können. Eine Abschaffung der Landesbeauftragten für den Datenschutz wäre mit dieser Vorgabe unvereinbar.

Verstoß gegen EU-Recht

Noch deutlicher wird es auf europäischer Ebene.
Die DS-GVO schreibt in Art. 51–54 DS-GVO zwingend vor, dass die Mitgliedstaaten völlig unabhängige Datenschutzaufsichtsbehörden haben müssen. Diese Unabhängigkeit ist nicht verhandelbar. Sie ist eine Kernvoraussetzung für die gesamte europäische Datenschutzarchitektur. Eine Abschaffung der Landesbeauftragten würde gegen die DS-GVO verstoßen. Deutschland kann sich nicht aussuchen, ob es eine unabhängige Datenschutzaufsicht haben möchte. Es muss sie haben.

Zentralisierung der Datenschutzkontrolle beim Bund?

Ministerpräsident Wüst hat weiterhin vorgeschlagen, die Datenschutzaufsicht vollständig auf die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zu übertragen. Auch damit liegt er falsch.
Die BfDI ist eine Bundesbehörde. Es würde der durch das Grundgesetz garantierten föderalen Ordnung widersprechen, wenn eine Bundesbehörde die Einhaltung des Datenschutzes bei Landesbehörden kontrollieren würde.
Das Grundgesetz ordnet die Ausführung der meisten Gesetze – auch des Datenschutzrechts – den Ländern zu (Art. 83 GG). Bund und Länder sind eigenständige Verwaltungsträger. Jeder Bereich darf nur von der Ebene kontrolliert werden, die dafür verfassungsrechtlich zuständig ist.
Würde die BfDI Landesbehörden kontrollieren, würde sie in die Verwaltungshoheit der Länder eingreifen. Die Landesregierungen wären nicht mehr demokratisch verantwortlich für ihre eigenen Behörden.



Peter Schaar
ist Vorsitzender der Europäischen Akademie für die Informationsfreiheit und den Datenschutz (EAID) und ehem. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI).

Fazit: Datenschützer sind ein Schutzschild, kein Hindernis

Datenschutzbeauftragte sind nicht lästig, sie sind notwendig. Sie schützen Bürgerinnen und Bürger vor Überwachung, Machtmissbrauch und Datenmissbrauch. Sie sorgen dafür, dass Digitalisierung rechtsstaatlich bleibt. Wer ihre Abschaffung fordert, stellt sich nicht gegen Bürokratie, sondern gegen Grundrechte. Eine generelle Übertragung der Datenschutzkontrolle auf die BfDI wäre mit der im Grundgesetz festgelegten föderalen Ordnung der Bundesrepublik Deutschland nicht vereinbar.
Wüsts Vorschläge sind daher nicht nur politisch unklug, sondern rechtlich ausgeschlossen. Die unabhängige Datenschutzaufsicht ist ein unverzichtbarer Bestandteil unserer zunehmend digitalisierten, freiheitlichen Ordnung – in Nordrhein-Westfalen, in Deutschland und in Europa.

VOLKER STÜCK / MARTIN JUNG / FRANZISKA KLEIN

Die moderne IT-Rahmen-Betriebsvereinbarung

Vorschlag und Erläuterung einer Musterbetriebsvereinbarung

Betriebsrat
Mitbestimmungsrechte
Arbeitsrecht
Compliance
Leistungs-/Verhaltenskontrolle
Beweisverwertung

■ Betriebe und Behörden sind zur Erbringung ihrer Leistungen auf den Einsatz moderner IT-Anwendungen angewiesen. Deren Implementierung und Anwendung setzt voraus, dass die aktuellen arbeits-, mitbestimmungs-, compliance- und datenschutzrechtlichen Anforderungen beachtet, aufeinander abgestimmt und angemessen austariert werden. Diese werden hier mit einer Musterbetriebsvereinbarung vorgestellt.

■ Companies and public authorities rely on modern IT applications to provide their services. The implementation and use of such applications requires that current labour and employment, co-determination, compliance and data protection requirements are observed, coordinated and appropriately balanced. This is shown here in a model works agreement.
Lesedauer: 28 Minuten

I. Digitalisierung und Spannungsfeld

Die zunehmende Digitalisierung betrieblicher Abläufe führt zu einem stetig wachsenden Einsatz von IT-Anwendungen, digitalen Tools und KI-basierten Systemen. Damit verstärkt sich das Spannungsverhältnis zwischen dem Recht des Beschäftigten auf informationelle Selbstbestimmung[1] einerseits und dem berechtigten Interesse des Arbeitgebers, Arbeitsprozesse effizient und zweckmäßig zu gestalten andererseits. Sowohl die Mitbestimmungsrechte des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG als auch die datenschutzrechtlichen Anforderungen[2] sind in diesem Kontext von zentraler Bedeutung. Sie bilden den Rahmen, in dem digitale Systeme rechtssicher eingeführt und genutzt werden können. Nach Erwägungsgrund 26 S. 5 DS-GVO entfällt diese Abwägung nur, wenn personenbezogene Daten vollständig anonymisiert werden, wobei es entscheidend auf den Verantwortlichen ankommt.[3]

In der Praxis erfolgt die Auflösung dieses Konflikts regelmäßig durch den Abschluss von Betriebsvereinbarungen. Besonders bewährt hat sich ein zweistufiges Modell:

- eine grundsätzliche IT-Rahmenvereinbarung (ggf. auch in Kombination mit KI-Rahmen[4])[5], die den allgemeinen Rahmen abdeckt,
- ergänzt durch spezifische Steckbriefe bzw. Anlagen zu spezifischen IT-Anwendungen.

Im Folgenden wird aufgezeigt, worauf zu achten ist und wie eine solche IT-Rahmenvereinbarung gestaltet werden kann.

II. Individualarbeitsrechtliche Aspekte

Das Direktionsrecht (§ 106 GewO; § 315 Abs. 3 BGB) des Arbeitgebers umfasst die Entscheidung, welche Arbeitsmittel – einschließlich IT-Systeme – den Beschäftigten zur Verfügung gestellt werden. Vom Arbeitnehmer kann grundsätzlich nicht verlangt werden, eigene Mittel auf eigene Kosten und eigenes Risiko einzusetzen,[6] unabhängig von einer „Bring your own (IT) device" (BYOD[7])-Regelung. Mitbestimmungsfrei ist die Einführung des Tools jedoch nur, wenn dieses keine Funktionen enthält, die zur persönlichen Leistungs- und Verhaltenskontrolle geeignet sind. Maßgeblich ist hierbei nicht die Absicht des Arbeitgebers, sondern die objektive Eignung des Systems, Daten zur Überwachung zu nutzen. Die Rechtsprechung unterscheidet zwischen:

- Arbeitsverhalten – mitbestimmungsfrei und
- Ordnungsverhalten – mitbestimmungspflichtig nach § 87 Abs. 1 Nr. 1 BetrVG.

Beispiele für mitbestimmungsfreie Anweisungen sind:

- das Verbot, dienstlich gestellte IT für private Zwecke zu nutzen,[8] oder
- das Verbot, private Telefonate mit dienstlichen oder privaten Smartphones während der bezahlten Arbeitszeit (außerhalb der unbezahlten Pausen) zu führen.[9]

Begrenzt wird das arbeitgeberseitige Weisungsrecht durch Gesetze und Betriebsvereinbarungen. Typische Beispiele aus der gerichtlichen Praxis:

- Hat der Arbeitgeber vor der Einrichtung des Gruppenkalenders in Outlook den Betriebsrat nicht gem. § 87 Abs. 1 Nr. 6 BetrVG beteiligt, ist eine einseitige Weisung zur Nutzung des Gruppenkalenders unwirksam. Eine entsprechende Abmahnung wegen Nichtbefolgung der mitbestimmungswidrigen Weisung ist daher ebenfalls unwirksam und aus der Personalakte zu entfernen.[10]
- Der Arbeitgeber kann von Arbeitnehmern bei Leistungsmängeln oder objektiv zweifelhafter Leistungserbringung im Home-

1 BVerfG v. 15.12.1983 – 1 BvR 209/83 – Volkszählungsurteil.
2 BAG ZD 2017, 344; BAG ZD 2017, 339 mAnm Tiedemann.
3 Vgl. EuGH ZD 2025, 631; Roßnagel ZD 2021, 189; Hornung/Wagner ZD 2020, 223; Sydow/Marsch, DS-GVO/BDSG/Ziebarth, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 24 ff.; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 4 Nr. 5 Rn. 23 sowie Rn. 50 ff.
4 Zu KI-Rahmen Pepping BB 2025, 1333; Kaufmann/Chakrabarti NZA 2025, 372; Heine/Köhler NZA 2025, 526.
5 Vgl. Holthausen NZA 2023, 1489; Ludwig/Hinze NZA 2021, 1444; BeckOK ArbR/Reufels, 19. Ed. 1.5.2025, Form. 11.13 Anm. 1; Koreng/Lachenmann DatenschutzR-FormHdB/Huth, 4. Aufl. 2025, Form. H. VIII. Anm. 1.-70; Niemeyer BRuR 2023, 69; Oberthür/Seitz, Betriebsvereinbarungen/Panzer-Heemeier, 3. Aufl. 2021, B. V; Grimm/Singraven, Digitalisierung und Arbeitsrecht, 2022, § 15; Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 79a Rn. 39; Körner NZA 2019, 1389.
6 BAG v. 10.11.2021 – 5 AZR 334/21 – Rider – Fahrrad und Smartphone.
7 Grimm/Singraven, Digitalisierung und Arbeitsrecht, 2022, § 29; Auer-Reinsdorff/Conrad, IT- und DatenschutzR-HdB/Conrad, 3. Aufl. 2019, § 37 Rn. 299; Kramer, IT-ArbR/Hoppe, 3. Aufl. 2023, § 2 Rn. 723 ff.
8 LAG Hamm MMR 2006, 700.
9 BAG MMR 2024, 323.
10 LAG Nürnberg ZD 2017, 439.

office[11] oder im Außendienst nach billigem Ermessen eine detaillierte Dokumentation der Arbeitsleistung oder Arbeitsberichte verlangen.[12] Dies kommt insbesondere dann in Betracht, wenn er keine persönliche und direkte, mitbestimmungsfreie[13] humane Führung/Kontrolle bevorzugt und eine „back/return to office"-Weisung erteilt[14] bzw. eine Zusatzvereinbarung zur Telearbeit kündigt[15] und den Arbeitnehmer gem. §§ 99, 95 Abs. 3 BetrVG zurück in den Betrieb versetzt[16]. Kommt der Arbeitnehmer dieser Anweisung nicht nach, verletzt er seine arbeitsvertraglichen Pflichten. Dies kann zunächst eine Abmahnung und bei fortgesetztem Verhalten eine verhaltensbedingte Kündigung nach sich ziehen.

Bei der Erteilung von Anweisungen sollte der Arbeitgeber jedoch beachten, dass nach dem BAG bereits die Nutzung von Excel-Listen/Anwesenheitstabellen nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig ist.[17] Eine ohne Zustimmung des Betriebsrats erteilte Weisung, Excel-Listen zu führen, wäre daher unbeachtlich. Die Arbeitsanweisung, solche Berichte als nicht filter-/addierbare Word-Dateien oder manuell in Papierform zu erstellen, ist aber mitbestimmungsfrei (§ 87 Abs. 1 Nr. 1, Nr. 6 BetrVG) möglich.[18] Abzuraten ist von einer dauerhaften, intensiven, anlasslosen Leistungskontrolle, etwa durch den Einsatz von Spähsoftware[19] mittels IT-Keylogger, offene oder verdeckte Videoüberwachung am Arbeitsplatz[20] oder verdeckte Observationen durch Detektive[21]. Hieran bestehen hohe datenschutzrechtliche Anforderungen, und ein rechtswidriger Exzess kann zu erheblichen rechtlichen Nachteilen führen, wie zB Entschädigungsansprüchen der Betroffenen (Art. 82 DS-GVO; § 823 BGB), behördlichen Bußgeldern (Art. 83 DS-GVO) und der Unzulässigkeit der Verwertung eines bestimmten Sachvortrags und von Beweismitteln in gerichtlichen Verfahren.[22]

III. Mitbestimmungsrechte des Betriebsrats

Sobald eine IT-Anwendung geeignet ist, Verhalten oder Leistungen der Beschäftigten zu überwachen, entsteht ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG, dh die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, sind mitbestimmungspflichtig.

Nach stRspr kommt es nicht auf die Zweckbestimmung bzw. Nutzungsabsicht des Arbeitgebers, sondern allein auf die Eignung der technischen Einrichtung zur Überwachung an sich an.[23] Zu den typischen Anwendungsfällen zählen Stechuhren, Videoüberwachung, E-Mail-Kommunikationssysteme[24], Microsoft 365[25] und Facebook-Unternehmensseiten[26]. Selbst ein Headset-System, das es den Vorgesetzten nur ermöglicht, die Kommunikation unter Arbeitnehmern mitzuhören, ist eine technische Einrichtung, die zur Überwachung der Arbeitnehmer iSd § 87 Abs. 1 Nr. 6 BetrVG bestimmt ist. Seine Einführung und Nutzung unterliegt auch dann der Mitbestimmungspflicht, wenn die Gespräche nicht aufgezeichnet oder gespeichert werden.[27] Auch ein Internetbrowser ist als technische Einrichtung anzusehen, die geeignet ist, Leistungs- und Verhaltensinformationen der Arbeitnehmer zu erfassen und auszuwerten.[28]

Praxistipp: Quasi jede digitale Neuerung – von der Zeiterfassungs-App über Office-Anwendungen bis zum cloudbasierten Task-Manager – unterliegt damit der zustimmungspflichtigen Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG, was sich als „Flaschenhals bzw. Bremsklotz" bei solchen Projekten erweisen kann und frühzeitig in der Planung berücksichtigt werden sollte. Zuweilen geht es Betriebsräten dabei auch nicht primär um die IT-Anwendung an sich, sondern sie nutzen das Mitbestimmungsrecht, um an anderer Stelle Zugeständnisse zu erreichen, zB bei Vergütungs-/Arbeitszeitfragen (sog. Koppelungsgeschäfte[29]). Dies ist zwar nicht vom Schutzweck des Mitbestimmungsrechts umfasst, lässt sich in der Praxis aber kaum erfolgreich verhindern, da die Anforderungen an den Nachweis eines Rechtsmissbrauchs hoch sind. Ein darüber hinausgehendes umfassendes, erzwingbares Mitbestimmungsrecht des Betriebsrats in Bezug auf datenschutzrechtliche Pflichten des Arbeitgebers besteht jedoch nicht, wie das LAG Hessen klar herausgestellt hat – der Betriebsrat ist nicht der „betriebliche Superdatenschützer"[30].

Beim zunehmend wichtiger werdenden betrieblichen Einsatz von KI[31] ist von Bedeutung, dass eine Offenlegung der Entscheidungsalgorithmen oder des Quellcodes regelmäßig nicht gefordert werden kann und auch nicht zur Transparenz beiträgt. Verantwortliche müssen im Fall automatisierter, ggf. KI-basierter Entscheidungen jedoch ausreichende und nachvollziehbare Informationen über die konkrete Entscheidung bereitstellen. Diese Informationen sind verständlich zu formulieren und sollen die betroffene Person in die Lage versetzen, ihre Rechte, insbesondere das Recht auf Anfechtung und Überprüfung der Entscheidung, wahrzunehmen.[32]

Arbeitgeber sind an den Inhalt der normativ wirkenden Betriebsvereinbarung gebunden, § 77 Abs. 1, Abs. 4 BetrVG. Ist dort abschließend vereinbart, welche Daten auch zu Test-/Pilotzwecken verarbeitet werden dürfen, so sind sie daran gebunden. Ein Verstoß kann einen betriebsverfassungsrechtlichen Durchführungs- bzw. Unterlassungsanspruch des Betriebsrats begründen[33] und datenschutzrechtlich für die betroffenen Beschäftigten einen Schadensersatzanspruch nach Art. 82 DS-GVO auslösen, wenn keine DS-GVO-Rechtfertigungsgrundlage vorliegt[34].

---

11 LAG Mecklenburg-Vorpommern v. 28.9.2023 – 5 Sa 15/23: Darlegungslast für Vergütungskürzung wegen Nichtleistung liegt beim Arbeitgeber.
12 BAG v. 19.4.2007 – 2 AZR 78/06; Peters, WeisungsR/Peters, 2. Aufl. 2021, Rn. 884.
13 GK-BetrVG/Gutzeit, 12. Aufl. 2022, BetrVG § 87 Rn. 535.
14 LAG München v. 26.8.2021 – 3 SaGa 13/21; Tödtmann/Quicker NZA 2025, 1279; Möllenkamp NZA-RR 2025, 65; Stück/Salo AuA 03/2024, 22.
15 LAG Hamm v. 16.3.2023 – 18 Sa 832/22; LAG Nürnberg v. 11.5.2021 – 7 Sa 289/20.
16 BAG v. 20.10.2021 – 7 ABR 34/20; LAG Düsseldorf v. 10.9.2014 – 12 Sa 505/14.
17 BAG ZD 2019, 131 mAnm Stück.
18 LAG Berlin-Brandenburg ZD 2017, 579; GK-BetrVG/Gutzeit, 12. Aufl. 2022, BetrVG § 87 Rn. 536.
19 BAG ZD 2018, 41 mAnm Tiedemann: Beweisverwertungsverbot wegen Datenschutzwidrigkeit.
20 LAG Hamm ZD 2026, 52 mAnm Stück: 15.000 EUR; LAG Hessen MMR 2011, 346: 7.000 EUR; LAG Rheinland-Pfalz v. 27.4.2017 – 5 Sa 449/16: 10.000 EUR für länger und anlasslos observierten Betriebsratsvorsitzenden.
21 Vgl. LAG Köln v. 11.2.2025 – 7 Sa 635/23; LAG Rheinland-Pfalz v. 27.4.2017 – 5 Sa 449/16.
22 BAG ZD 2018, 127: Konkurrenztätigkeit während Krankheit; LAG Köln v. 11.2.2025 – 7 Sa 635/23: Arbeitszeitbetrug eines Fahrkartenkontrolleurs; LAG Rheinland-Pfalz v. 13.7.2017 – 5 Sa 49/17.
23 Vgl. Übersicht bei Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 87 Rn. 242–251; GK-BetrVG/Gutzeit, 12. Aufl. 2022, BetrVG § 87 Rn. 582, 583.
24 BAG ZD 2021, 706 mAnm Tiedemann.
25 BAG MMR 2022, 867.
26 BAG v. 3.12.2016 – ABR 7/15: Arbeitgeber Facebookseite.
27 BAG ZD 2025, 115.
28 ArbG Hamburg ZD 2024, 354 mAnm Schoss.
29 Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 87 Rn. 27; GK-BetrVG/Gutzeit, 12. Aufl. 2022, BetrVG § 87 Rn. 382; GK-BetrVG/Franzen, 12. Aufl. 2022, BetrVG § 2 Rn. 14.
30 LAG Hessen ZD 2025, 532.
31 Vgl. Waas RdA 2022, 125; Meyer NJW 2023, 1841; Lang/Reinbach NZA 2023, 1273; Kössel DB 2024, 1069; Schemmel SPA 2024, 12; Kalbfus/Schöberle ArbRAktuell 2023, 251; Kaufmann/Chakrabarti NZA 2025, 372.
32 EuGH ZD 2025, 261 mAnm Radtke.
33 Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 87 Rn. 7; ErfK/Kania, BetrVG § 87 Rn. 8; BAG v. 18.11.2014 – 1 ABR 21/13.
34 BAG ZD 2025, 714.

Einen eigenen Unterlassungsanspruch neben der Löschung (Art. 17 DS-GVO) gewährt die DS-GVO jedoch nicht.[35]

Der Betriebsrat hat nach § 80 Abs. 1 Nr. 1 BetrVG ein allgemeines Überwachungsrecht auch im Hinblick auf die DS-GVO und das BDSG, soweit es sich um zugunsten der Arbeitnehmer geltende Vorschriften handelt. Der Betriebsrat ist verpflichtet, die entsprechenden Vorschriften konkret zu benennen, zB § 26 Abs. 1 S. 2 BDSG.[36] Hieraus ergibt sich auch ein Unterrichtungsrecht nach § 80 Abs. 2 BetrVG. Daraus folgt das Recht auf Vorlage und Erläuterung der Verarbeitungsprogramme bestehender Personaldatenbanken, auch sofern eine Verknüpfung der Personaldatenbank mit anderen Datenbanken möglich ist.[37] Nach dem sog. Drei-Säulen-Modell überwachen den betrieblichen Datenschutz, für den der Arbeitgeber verantwortlich ist (Art. 4 Nr. 7 DS-GVO), drei Funktionen:

- die Datenschutzaufsichtsbehörde,
- der bestellte Datenschutzbeauftragte und
- der Betriebsrat.

Aufgrund eines potenziellen Interessenkonflikts kann der Betriebsratsvorsitzende nicht zugleich der Datenschutzbeauftragte sein.[38] Aus § 80 BetrVG folgt aber kein umfassendes Mitbestimmungsrecht hinsichtlich der Einhaltung datenschutzrechtlicher Anforderungen, das auch über eine Einigungsstelle durchsetzbar wäre. Die Vorschrift eröffnet dem Betriebsrat keinen eigenen Gestaltungs-/Regelungsspielraum und kein Initiativrecht.[39]

Nach § 75 Abs. 2 BetrVG iVm Art. 1, 2 Abs. 1 GG haben Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie sind verpflichtet, die Selbstständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu unterstützen. Aus dem GG hat das BVerfG im „Volkszählungsurteil" den Datenschutz und das individuelle Grundrecht auf informationelle Selbstbestimmung abgeleitet.[40] Dies ist – neben der DS-GVO und dem BDSG – auch der gerichtliche (Kontroll-)Maßstab für Betriebsvereinbarungen, zB:

- Eine Betriebsvereinbarung über eine „Belastungsstatistik" zwecks Gefährdungsbeurteilung (§ 5 ArbSchG, § 87 Abs. 1 Nr. 7 BetrVG), die durch eine technische Überwachungseinrichtung iSd § 87 Abs. 1 Nr. 6 BetrVG dauerhaft die Erfassung, Speicherung und Auswertung einzelner Arbeitsschritte und damit des wesentlichen Arbeitsverhaltens der Arbeitnehmer anhand quantitativer Kriterien während ihrer gesamten Arbeitszeit vorsieht, stellt einen schwerwiegenden Eingriff in die Persönlichkeitsrechte der Arbeitnehmer dar. Ein solcher Eingriff ist nicht durch überwiegend schutzwürdige Belange des Arbeitgebers gedeckt, sodass die Regelung unwirksam ist.[41]
- Eine Betriebsvereinbarung, die vorsieht, dass der Betriebsrat zwangsweise an allen Personalgesprächen mit disziplinarischem Charakter teilnehmen muss, auch wenn der Arbeitnehmer dies nicht möchte, ist unwirksam, weil der Beschäftigte zum fremdbestimmten Objekt degradiert wird, statt selbstbestimmendes Subjekt und Herr des Verfahrens zu sein.[42] Gleiches gilt auch beim Betrieblichen Eingliederungsmanagement (BEM) nach § 167 Abs. 2 SGB IX.[43]

Betriebsvereinbarungen müssen einen angemessenen Ausgleich zwischen dem Interesse des Arbeitgebers an der entsprechenden Verarbeitung von Beschäftigtendaten und den berechtigten Belangen der Arbeitnehmer am Eingriff in Persönlichkeitsrechte herstellen[44] und dürfen das Schutzniveau der DS-GVO nicht unterschreiten[45].

Als Verantwortlicher iSd Art. 4 Nr. 7 DS-GVO ist der Arbeitgeber verantwortlich für den Datenschutz und haftbar für Entschädigungen und Bußgelder nach Art. 82, 83 DS-GVO. Nach § 79a S. 2 BetrVG ist der Arbeitgeber auch der für die Verarbeitung personenbezogener bzw. personenbeziehbarer Daten Verantwortliche iSd datenschutzrechtlichen Vorschriften, soweit der Betriebsrat zur Erfüllung seiner gesetzlichen Aufgaben solche Daten verarbeitet.[46] Der Betriebsrat selbst hat in seinem Verantwortungsbereich zwar den Datenschutz sicherzustellen, ist jedoch nicht als Dritter iSd Art. 4 Nr. 10 DS-GVO anzusehen. Er kann sich vom Datenschutzbeauftragten beraten lassen und nach überwiegender Meinung der Literatur und Rechtsprechung auch von ihm kontrolliert werden.[47] Unter Beachtung des Strukturprinzips der Unabhängigkeit in der Betriebsverfassung hat der Betriebsrat intern eigenständig über Maßnahmen zu beschließen (BR-internes Datenschutzkonzept), um einem Missbrauch der Daten innerhalb seines gesetzlichen Verantwortungsbereichs zu begegnen.[48]

Nach § 87 Abs. 1 Nr. 1 BetrVG ist das kollektive betriebliche Ordnungsverhalten der Arbeitnehmer mitbestimmungspflichtig, das unmittelbare Arbeitsverhalten hingegen nicht. Gegenstand des Mitbestimmungsrechts ist das betriebliche Zusammenleben und kollektive Zusammenwirken der Beschäftigten.[49] Die Entscheidung, ob, wann und wie die vertraglich vereinbarte Arbeit zu leisten ist und wie deren Erbringung kontrolliert wird, fällt nicht unter den Mitbestimmungstatbestand.[50] Mitbestimmungsfrei kann der Arbeitgeber etwa die private Nutzung dienstlich gestellter ITK verbieten.[51] Gleiches gilt für die Vorgaben zur Nutzung von ChatGPT und vergleichbaren Tools iRd Arbeitsverpflichtung.[52] Dagegen unterliegt die Herausgabe einer Arbeitsanweisung zur Meldung von potenziellen Datenschutzverletzungen nach der DS-GVO und die Verpflichtung, während der Bearbeitung des Sachverhalts kurzfristig erreichbar zu sein, der Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 1 BetrVG.[53] Aus der Mitbestimmung über das Ordnungsverhalten ergeben sich keine umfassenden, erzwingbaren Mitbestimmungsrechte des Betriebsrats hinsichtlich datenschutzrechtlicher Pflichten des Arbeitgebers, wie das LAG Hessen zutreffend feststellt hat.[54]

In der Praxis hat sich der Abschluss einer IT-Rahmenvereinbarung bewährt. Sie gibt die generellen Leitplanken vor, während konkrete Anwendungen über ein standardisiertes Aufnahmeverfahren, häufig mittels Steckbriefen bzw. in Anlagen, geregelt werden. Diese definieren u.a.:

- Funktionsumfang und Zweck,
- Datenverarbeitung,

35 Vgl. EuGH ZD 2025, 640; BGH ZD 2024, 90.
36 BAG ZD 2021, 706 mAnm Tiedemann; Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 80 Rn. 7a.
37 BAG v. 17.3.1987 – 1 ABR 59/85.
38 BAG ZD 2023, 761 mAnm Heberlein.
39 LAG Hessen ZD 2025, 532; ArbG Hamburg ZD 2024, 354 Rn. 34; vgl. zu § 90 BetrVG Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 90 Rn. 48.
40 BVerfG v. 15.12.1983 – 1 BvR 209/83.
41 BAG v. 25.4.2017 – 1 ABR 46/15.
42 BAG ZD 2019, 320 mAnm Stück.
43 ErfK/Rolfs, 25. Aufl. 2025, SGB IX § 167 Rn. 7; BAG v. 19.11.2019 – 1 ABR 36/18.
44 ErfK/Franzen, 25. Aufl. 2025, BDSG § 26 Rn. 48.
45 Paal/Pauly, DS-GVO BDSG/Gräber/Nolden, BDSG § 26 Rn 49; Kort NZA 2018, 1101; Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 79a Rn. 35.
46 ArbG Bonn ZD 2025, 176.
47 Stück ZD 2019, 255; Kühling/Buchner, DS-GVO BDSG/Bergt/Herbort, 4. Aufl. 2024, DS-GVO Art. 38 Rn. 18; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Drewes, 2. Aufl. 2025, DS-GVO Art. 38 Rn. 28; Lücke NZA 2019, 668.
48 BAG ZD 2020, 46 mAnm Tiedemann; BAG ZD 2019, 571; BAG ZD 2024, 112.
49 ArbG Hamburg ZD 2024, 354: ChatGPT.
50 BAG v. 15.4.2014 – 1 ABR 85/12.
51 LAG Hamm MMR 2006, 700.
52 Holthausen RdA 2023, 261; Kalbfus/Schöberle NZA 2023, 251; Witteler ZD 2023, 377; ArbG Hamburg ZD 2024, 354 Rn. 25 mAnm Schoss.
53 LAG Schleswig-Holstein v. 6.8.2019 – 2 TaBV 9/19.
54 LAG Hessen ZD 2025, 532.

- Rollen- und Berechtigungskonzept sowie
- Lösch- und Speicherfristen.

Damit wird sichergestellt, dass die Bewertung eines Tools nicht allein anhand abstrakter Rahmentexte erfolgt, sondern auf der Basis einer nachvollziehbaren technischen und fachlichen Beschreibung.

IV. Compliance-Aspekte

Der Arbeitgeber ist nach dem Legalitätsprinzip verpflichtet, bei Verdacht auf betriebliche Regelverstöße diese aufzuklären, abzustellen bzw. zu sanktionieren und ein wirksames Compliance-Management-System zu installieren,[55] das auch enthaftend wirkt[56]. IT-Anwendungen dienen einem bestimmten, beschriebenen Zweck, zB bei einem Zugangskontrollsystem der Prüfung der Berechtigung des Zugangs oder bei einem Zeiterfassungssystem der Erfüllung der Arbeitsschutzpflichten des Arbeitgebers nach § 3 Abs. 2 Nr. 1 ArbSchG.[57] Erlangt der Arbeitgeber jedoch, zB durch eigene Wahrnehmung, Hinweise nach dem HinSchG, Beschwerden nach § 84 BetrVG, § 13 AGG oder Hinweise von Kunden, Lieferanten, Behörden etc auf mögliche Straftaten oder schwere Vertragsverletzungen, zB einen Arbeitszeit- oder Leistungsabrechnungsbetrug oder sexuelle Belästigung (§ 184i StGB), so ist er nach dem Legalitätsprinzip (§§ 130, 30 OWiG; § 43 GmbHG; § 93 AktG) zur Aufklärung, Untersuchung sowie – bei Verifizierung – zur Aufnahme von Präventionsmaßnahmen und zur Sanktionierung verpflichtet. Dh, er muss eine Klärung herbeiführen und etwaige Beweise sichern.

Grundsätzlich gibt es de lege lata keinen Zwang zur Erstattung einer Behörden-/Strafanzeige[58] und der Arbeitgeber kann deshalb nach pflichtgemäßem Ermessen entscheiden, ob er mit seinen privatrechtlichen Mitteln selbst ermittelt oder externe Experten (zB Rechtsanwälte, Wirtschaftsprüfer, IT-Forensiker, Wirtschaftsdetektei[59]) damit beauftragt oder eine Strafanzeige erstattet und den Fort- und Ausgang des Ermittlungs- und Strafverfahrens abwartet, zumal auch strafrechtliche Entscheidungen die Arbeitsgerichte nicht binden.[60]

Rechtsgrundlage für die interne Untersuchung, die idR von Compliance/Revision und bzw. oder HR durchgeführt wird, sind:

- Bei Straftaten: § 26 Abs. 1 S. 2 BDSG; Art. 6 Abs. 1 lit. b DS-GVO – Beendigung von Beschäftigungsverhältnissen, Art. 6 Abs. 1 lit. c DS-GVO – Legalitätspflichten des Verantwortlichen nach §§ 130, 30 OWiG; § 43 GmbHG; § 93 AktG sowie Art. 6 Abs. 1 lit. f DS-GVO – Interessenabwägung nach der DS-GVO.
- Bei schweren Vertragspflichtverstößen: Nach Unanwendbarkeit des § 26 Abs. 1 S. 1 BSDG aufgrund der EuGH-Entscheidung[61] Art. 6 Abs. 1 lit. b DS-GVO – Beendigung von Beschäftigungsverhältnissen, Art. 6 Abs. 1 lit. c DS-GVO – Legalitätspflichten des Verantwortlichen nach §§ 130, 30 OWiG; § 43 GmbHG; § 93 AktG sowie Art. 6 Abs. 1 lit. f DS-GVO – Interessenabwägung nach der DS-GVO. § 26 Abs. 1 S. 2 BDSG entfaltet insoweit als Lex specialis auch keine Sperrwirkung für schwere Vertragsverletzungen.[62]

Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zur Aufdeckung setzt lediglich einen „einfachen" – keinen zwingend dringenden – Verdacht iSe Anfangsverdachts voraus, der über vage Anhaltspunkte und bloße Mutmaßungen hinausreichen muss, sodass Ermittlungen nicht ins Blaue hinein geführt werden dürfen,[63] auch nicht bei Massendatenabgleichen bzw. Screening bei Korruptionsverdacht[64]. Sollten datenschutzgemäß erhobene Zufallsfunde zur Überführung eines anderen Täters als des Verdächtigen führen, so sind auch diese verwendbar.[65]

Praxistipp: Die Anhaltspunkte sollte der ermittelnde Arbeitgeber in einem sog. Einleitungsvermerk dokumentieren, der den Untersuchungsumfang begrenzt und den Zweck der Datenerhebung erläutert,[66] und über die weiteren Ermittlungsschritte/-ergebnisse sollte er ein Ermittlungstagebuch führen.

Betriebsvereinbarungen dürfen auch nicht (mehr) generell die Datenverarbeitungen zum Zweck der Leistungs- und Verhaltenskontrolle (§ 87 Abs. 1 Nr. 6 BetrVG) ausschließen und bei einem Verstoß konstitutiv ein Sachvortrags- und Beweisverwertungsverbot statuieren.[67] Dem steht rechtlich Folgendes entgegen:

- Die Unvereinbarkeit mit der DS-GVO und dem Prozessrecht (ZPO, StPO).
- Es bestehen dafür keine gesetzlichen Mitbestimmungsrechte des Betriebsrats bzw. keine Regelungsbefugnis der Betriebsparteien oder auch der Einigungsstelle.
- Die Gerichte bzw. der Rechtsstaat dürfen dadurch in der Verfolgung und Sanktionierung doloser Täter, die keinen Schutz verdienen, nicht gebunden bzw. „an die Kette gelegt" werden.[68] Entsprechend hat auch das BVerfG im Fall „EncroChat" entschieden:[69] Der Rechtsstaat kann sich nur verwirklichen, wenn ausreichende Vorkehrungen getroffen werden, dass Straftäter iRd geltenden Gesetze verfolgt, abgeurteilt und einer gerechten Bestrafung zugeführt werden – „Datenschutz ist kein Taten-/Täterschutz". Die Fachgerichte prüfen die Beachtung des Daten-/Persönlichkeitsrechtsschutzes im jeweiligen Fall genau und entscheiden über eine Verwertung bei Datenschutzkonformität bzw. Nichtverwertung bei rechtswidriger Datenverarbeitung bzw. Exzess[70] und perpetuierender Verletzung bei gerichtlicher Berücksichtigung, die nicht erfolgen darf.

Praxistipp: Auch in einer IT-Rahmen-Betriebsvereinbarung sollte deshalb von diesen Grundsätzen nicht abgewichen und entsprechend keine Veto-/Zustimmungsverweigerungsrechte des Betriebsrats oder Sachvortrags- und Beweisverwertungsverbote in Fällen des Verdachts strafbaren Verhaltens (§ 26 Abs. 1 S. 2 BDSG) oder schwerer Vertragspflichtverstöße statuiert werden.

Eine heimliche Spindkontrolle durch den Arbeitgeber ist grundsätzlich unzulässig und kann einem Beweisverwertungsverbot unterliegen, wenn der Arbeitnehmer nicht anwesend war und nicht zugestimmt hat. Daran ändert auch die Beteiligung des Betriebsrats an der Spindkontrolle in Abwesenheit des Betroffenen nichts, sondern sie verschlimmert die Situation, weil mehr Personen Einblick erhalten.[71]

---

55 Vgl. OLG Nürnberg v. 30.3.2022 – 12 U 1520/19.
56 Hommelhoff/Hopt/Leyens, Unternehmensführung-HdB/Klahold, 2024, § 16 Rn. 104 ff.; BGH v. 9.5.2017 – 1 StR 265/16.
57 BAG v. 13.9.2022 – 1 ABR 22/21.
58 Lanzinner CCZ 2024, 276; Parigger/Helm/Stevens-Bartol, Arbeits- und Sozialstrafrecht, 2021, E, IV, 1 Rn. 88 f.; Semler/v. Schenck/Wilsing, Arbeitshandbuch für Aufsichtsratsmitglieder, 5. Aufl. 2021, § 8, IV, 1 Rn. 67 f.; Herbert/Oberrath NZA 2005, 196.
59 Zur Kostenerstattung des überführten Arbeitnehmers BAG v. 29.4.2021 – 8 AZR 276/20; LAG Köln v. 11.2.2025 – 7 Sa 635/23.
60 BAG v. 22.11.2012 – 2 AZR 732/11 Rn. 31; BAG v. 27.1.2011 – 2 AZR 825/09 Rn. 15 ff.
61 EuGH ZD 2023, 391.
62 BAG ZD 2018, 127.
63 BAG ZD 2017, 339,
64 ArbG Berlin MMR 2011, 70; Stück/Shamsaifar AuA 11/2025, 24.
65 BAG v. 22.9.2016 – 2 AZR 848/15.
66 Vgl. Fuhlrott ArbRAktuell 2020, 103; Stück CCZ 2020, 80; Fuhlrott GWR 2020, 23.
67 BAG ZD 2023, 693; LAG Hessen ZD 2025, 716 mAnm Stück; LAG Baden-Württemberg ZD 2019, 132; Fuhlrott NZA 2023, 1073.
68 BAG ZD 2023, 693: offene Videoüberwachung eines Tors zur Aufdeckung eines Arbeitszeitbetrugs; LAG Hessen ZD 2025, 716 mAnm Stück.
69 BVerfG MMR 2025, 190.
70 Zum Datenschutzexzess und eigener Verantwortlichkeit eines Beschäftigten OLG Stuttgart ZD 2025, 405; Bauer/Sura ZD 2025, 11; Kühling/Buchner, DS-GVO BDSG/Bergt, 4. Aufl. 2024, DS-GVO Art. 83 Rn. 22; Leibold/Kinzinger ZD-Aktuell 2025, 01268.
71 BAG ZD 2014, 260 mAnm Wybitul.

Praxistipp: Heimliche Kontrollmaßnahmen sind deshalb immer mit dem Datenschutzbeauftragten abzustimmen, zu dokumentieren und sind Ausnahmen bzw. Ultima Ratio.[72] Grundsätzlich sind Überwachungsmaßnahmen angekündigt und offen durchzuführen, weil sonst bei Datenschutzwidrigkeit bzw. Exzess nachteilige Rechtsfolgen drohen können, wie zB Entschädigungsansprüche (Art. 82 DS-GVO), behördliche Bußgelder (Art. 83 DS-GVO), dass der Exzesstäter selbst Verantwortlicher ist[73] oder ein Sachvortrags-/Beweismittelverwertungsverbot, wenn bei gerichtlicher Nutzung die Persönlichkeitsrechte des Betroffenen unangemessen und perpetuierend verletzt würden.

V. Datenschutzrechtliche Aspekte

Die DS-GVO bildet eine verbindliche Grundlage und kann durch Betriebsvereinbarungen ergänzt werden, indem diese einen zuverlässigen und eigenen Rechts-/Erlaubnisgrund für eine Verarbeitung personenbezogener Daten nach Art. 88 DS-GVO; § 26 Abs. 4 BDSG darstellen.[74] Diese Sichtweise ist durch ein neues EuGH-Urteil relativiert worden, in dem der EuGH Folgendes festgestellt hat:

- Eine Betriebsvereinbarung muss sich voll an den Grundsätzen der Art. 5, 6, 9 DS-GVO messen lassen.
- Sie kann und darf von der DS-GVO nicht „nach unten" abweichen.
- Die Beachtung wird von den Gerichten umfänglich kontrolliert, es gibt also keine datenschutzrechtliche Privilegierung der Betriebsparteien oder kontrollfreie Räume.[75]

Als Folge dieser Rechtsprechung empfiehlt es sich, in der Betriebsvereinbarung bzw. in datenschutzrechtlichen Dokumentationen primär auf die DS-GVO zurückzugreifen und nur ergänzend auf § 26 Abs. 3, Abs. 4 BDSG. Als Rückgriff iRd DS-GVO kommen insbesondere in Betracht:

- Art. 6 Abs. 1 lit. b DS-GVO: erforderlich zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses (§ 26 Abs. 1 S. 1 BDSG ist nach der EuGH-Rechtsprechung unanwendbar und damit unbeachtlich geworden).[76]
- Art. 6 Abs. 1 lit. c DS-GVO: Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen, wozu auch die Umsetzung einer normativ wirkenden Betriebsvereinbarung nach § 77 Abs. 1, Abs. 4 BetrVG; Art. 88 DS-GVO, Erwägungsgrund 155 DS-GVO gehört.[77]
- Art. 6 Abs. 1 lit. f DS-GVO: allgemeine Interessenabwägung.

In jeder Betriebsvereinbarung sind inhaltlich vor allem

- der Verarbeitungszweck,
- die Verarbeitungsdauer,
- Löschungsregelungen und
- die Zugriffsrechte auf die Beschäftigtendaten

zu regeln. In Rahmenbetriebsvereinbarungen sollten Gegenstände aufgenommen werden, die unabhängig vom konkreten Verarbeitungszweck immer gleich auszugestalten sind, wie zB die Betroffenenrechte oder Angaben zu technischen Datenschutzmaßnahmen bzw. den datenschützenden Voreinstellungen der IT-Systeme.[78]

De lege lata kennt das deutsche Datenschutzrecht kein Konzernprivileg: Unternehmen desselben Konzerns gelten datenschutzrechtlich als Dritte iSd Art. 4 Nr. 10 DS-GVO.[79] Dies führt bei den heutigen Unternehmens- und Organisationsstrukturen zu erheblichen Herausforderungen. § 30 des Referentenentwurfs v. 8.10.2024 zum Beschäftigtendatengesetz, der ein solches Privileg innerhalb der DS-GVO vorsah, wurde nicht umgesetzt. Folglich bedarf weiterhin jeder Datentransfer innerhalb des Konzerns einer eigenen Rechts-/Erlaubnisgrundlage.[80] Für Drittstaatskonzerngesellschaften in Non-EU- bzw. Non-DS-GVO-Ländern, zB USA oder Indien, ist ebenfalls kein Sonderprivileg vorgesehen. Deshalb bestehen in diesem Zusammenhang weiterhin erhebliche Rechtsunsicherheiten hinsichtlich der Zulässigkeit eines Datentransfers, die nach Art. 44 ff. DS-GVO sorgfältig geprüft und umgesetzt werden müssen, Erwägungsgrund 48 S. 2 DS-GVO.[81] Der Koalitionsvertrag 2025 sieht explizit kein neues Beschäftigtendaten(schutz)gesetz vor.[82]

Selbst bei einem festgestellten Datenschutzverstoß hält die Rechtsprechung von EuGH und BAG Maß und Mitte und gewährt keinen hohen Schadensersatz.[83] Es bedarf der Darlegung und des Nachweises eines konkreten Schadens, ein bloßes Unwohlsein oder die reine Befürchtung eines Datenmissbrauchs reicht nicht aus.[84] Gleichwohl gilt der Grundsatz: „Kleinvieh macht auch Mist", dh eine Vielzahl kleiner Entschädigungsbeträge können sich zu einer stattlichen Summe addieren, ggf. zzgl. Rechtsverfolgungs-/Rechtsverteidigungs- sowie Gerichtskosten. In einem Scraping-Vorfall bei Facebook führten Verstöße zu Schadensersatzansprüchen der Betroffenen in einer Größenordnung von 100 EUR.[85] In seiner Workday-Entscheidung hat das BAG eine Entschädigung von 200 EUR zugebilligt.[86] Darüber hinaus sind DS-GVO-Ansprüche abtretbar[87] und Verbraucherschutzverbände klagebefugt.[88] Einen Unterlassungsanspruch gewährt Art. 82 DS-GVO (neben Art. 17 DS-GVO Löschung) nicht, dh zivilrechtliche Unterlassungsansprüche auf Grundlage von § 1004 Abs. 1 BGB iVm § 823 Abs. 1 BGB werden verdrängt.[89]

VI. Umsetzung in der Praxis

Die IT-Rahmenvereinbarung fasst die grundsätzlichen, allgemeinen Regelungen zusammen und gibt die übergeordnete Struktur vor, die für alle IT-Anwendungen gilt. Die jeweiligen Anlagen bzw. Steckbriefe beschreiben die einzelnen Anwendungen dann konkret und spezifisch. Dabei sollten zum Zeitpunkt der Einführung die Spezifika möglichst genau dokumentiert und der Status zur Einführung festgehalten werden. Da IT-Anwendungen regelmäßigen Updates und Releases unterliegen, empfiehlt es sich in der Praxis, einen Fachausschuss aus betreibendem Fachbereich, CIO, Datenschutz und Betriebsrat (§ 28 BetrVG) zu bilden. Dieser prüft, beurteilt und entscheidet über die Neuerungen und Änderungen, um festzustellen, ob diese noch durch den IT-Rahmen und die Steckbriefe bzw. die Anlage abgedeckt sind oder ob wesentliche Änderungen eine Neufassung bzw. Aktualisierung erforderlich machen.

---

72 BAG ZD 2017, 344 Rn. 44: heimliche Videoüberwachung.
73 OLG Stuttgart ZD 2025, 405 mAnm Dieterle; Ambrock ZD 2020, 492.
74 Stück ZD 2019, 256; Kühling/Buchner, DS-GVO BDSG/Maschmann, 4. Aufl. 2024, BDSG § 26 Rn. 65; Fitting, BetrVG, 32. Aufl. 2024, BetrVG § 79a Rn. 33 f.
75 EuGH ZD 2025, 205 mAnm Monreal – Workday; BAG ZD 2025, 714 – Workday.
76 EuGH ZD 2023, 391.
77 Kühling/Buchner, DS-GVO BDSG/Buchner/Petri, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 85; Gola/Heckmann, DS-GVO BDSG/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 46; Taeger/Gabel, DSGVO – BDSG – TTDSG/Taeger, 4. Aufl. 2022, DS-GVO Art. 6 Rn. 84; Wybitul/Sörup/Pötters ZD 2015, 560.
78 Körner NZA 2019, 1395; Wurzberger ZD 2017, 258; ErfK/Franzen, 25. Aufl. 2025, BDSG § 26 Rn. 48.
79 LAG Hamm ZD 2022, 295; Kühling/Buchner, DS-GVO BDSG/Maschmann, 4. Aufl. 2024, DS-GVO Art. 88 Rn. 52; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Schantz, 2. Aufl. 2025, DS-GVO Art. 6 Abs. 1 Rn. 118.
80 Stück CCZ 2024, 331; Fuhlrott ArbRAktuell 2024, 512.
81 Vgl. Auer-Reinsdorff/Conrad, IT- und DatenschutzR-HdB/Dovas/Grapentin, 3. Aufl. 2019, § 35 Rn. 20 ff.; Kühling/Buchner, DS-GVO BDSG/Maschmann, 4. Aufl. 2024, DS-GVO Art. 88 Rn. 54.
82 Vgl. Fuhlrott ArbRAktuell 2025, 155.
83 EuGH ZD 2024, 334.
84 BAG ZD 2025, 415; BAG ZD 2025, 530.
85 BGH ZD 2025, 162.
86 BAG ZD 2025, 714.
87 OLG Hamm v. 24.7.2024 – 11 U 69/23.
88 EuGH ZD 2022, 384; BGH ZD 2020, 589.
89 EuGH ZD 2025, 640 mAnm Mekat/Wellmann – Quirin Privatbank; krit. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 70 Rn. 12.

Tests von IT-Systemen bzw. Software[90], die regelmäßig vor der Livestellung durchgeführt werden, sollten idealerweise mit Dummy-Daten ohne Personenbezug erfolgen, da bei der Verwendung von personenbezogenen Echtdaten DS-GVO, BDSG und BetrVG uneingeschränkt gelten und verbindlich zu beachten sind.[91] Außerdem sprechen Informationssicherheitsgründe potenziell dagegen. Alternativ kann vor Abschluss der Betriebsvereinbarung eine Duldungsvereinbarung mit dem Betriebsrat getroffen werden, die Zeitraum und Details der Tests konkret regelt. Ggf. kann dem Betriebsrat auch ein Testzugang eingerichtet und nach Testabschluss wieder entzogen werden.[92]

VII. Muster Betriebsvereinbarung

Zur sprachlichen Vereinfachung und besseren Lesbarkeit sind bei der Bezeichnung von Personen und Personengruppen stets Personen jeden Geschlechts gemeint.

Zwischen
Arbeitgeber X GmbH
und
Gesamtbetriebsrat (GBR) der X GmbH

wird folgende Gesamtbetriebsvereinbarung (GBV) nach § 87 Abs. 1 Nr. 6 BetrVG; Art. 6 Abs. 1 lit. c DS-GVO geschlossen:

§ 1 Geltungsbereich
Diese Gesamtbetriebsvereinbarung gilt

(1) persönlich für Arbeitnehmer der X GmbH, für gestellte und zugewiesene Arbeitnehmer, Beamte, sowie für Leiharbeitnehmer mit Ausnahme der leitenden Angestellten gem. § 5 Abs. 3 BetrVG (nachfolgend Beschäftigte);

(2) räumlich für das Unternehmen der X GmbH;

(3) sachlich für die Einführung und den Betrieb von mitbestimmungspflichtigen technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen iSd § 87 Abs. 1 Nr. 6 BetrVG. Dies sind datenverarbeitende Systeme, die individualisierte oder individualisierbare Verhaltens- oder Leistungsdaten selbst erheben und aufzeichnen, unabhängig davon, ob der Arbeitgeber die erfassten und festgehaltenen Verhaltens- oder Leistungsdaten auch auswerten oder zu Reaktionen auf festgestellte Verhaltens- oder Leistungsweisen verwenden will.

§ 2 Zweck der Gesamtbetriebsvereinbarung, Begriffe
Zweck der vorliegenden Gesamtbetriebsvereinbarung ist die Regelung des Beteiligungsverfahrens bei der Einführung neuer mitbestimmungspflichtiger technischer Einrichtungen, insbesondere IT-Verfahren, auf Ebene des Gesamtbetriebsrats gem. § 87 Abs. 1 Nr. 6 BetrVG – sei es originäre Zuständigkeit (§ 50 Abs. 1 BetrVG) oder Delegation (§ 50 Abs. 2 BetrVG) – sowie die Regelung von Rahmenbedingungen für den Betrieb dieser technischen Einrichtungen. Da der Hauptanwendungsfall in der Einführung und dem Betrieb von IT-Verfahren liegt, wird im Folgenden der Begriff IT-Verfahren synonym mit dem Begriff der technischen Einrichtung iSv § 87 Abs. 1 Nr. 6 BetrVG verwendet. Für technische Einrichtungen iSd § 87 Abs. 1 Nr. 6 BetrVG, die keine IT-Verfahren sind, gelten die Regelungen entsprechend.

§ 3 Beteiligungsverfahren
(1) Vor der Einführung und dem Betrieb eines einheitlich im Unternehmen oder in mehreren Regionen/Betrieben zu nutzenden IT-Verfahrens ist dem GBR eine Beschreibung des IT-Verfahrens zu übermitteln.

(2) In der Verfahrensbeschreibung (Ein Muster der Verfahrensbeschreibung ist als Anlage beigefügt) sind grundsätzlich folgende Inhalte darzustellen:

a) Kurze Verfahrensbeschreibung und Verfahrenszweck;

b) Nutzbare Funktionen des IT-Verfahrens;

c) Auflistung der zu verarbeitenden Kategorien personenbezogener Daten;

d) Aufbewahrungsdauer/Löschungsfristen für personenbezogene Daten;

e) Automatisierte Schnittstellen (Datenimport und -export) zu anderen IT-Verfahren und zu ggf. vorhandenen Dritten, über die zum Zeitpunkt der Einreichung personenbezogene Daten ausgetauscht werden;

f) Zum Zeitpunkt der Einreichung im System vergebene privilegierte Rollen und Rechte;

g) Auswertungen/Reports aus personenbezogenen Daten;

h) Owner (technischer Eigentümer) der technischen Einrichtung und Betreiber und

i) Zeitplanung der Implementierung und ggf. beabsichtigtes Schulungskonzept.

(3) Nach Zustimmung des GBR zur Einführung des IT-Verfahrens auf Grundlage der Verfahrensbeschreibung wird die Verfahrensbeschreibung als Anlage zu dieser Gesamtbetriebsvereinbarung genommen und kann das Verfahren auf Grundlage der Verfahrensbeschreibung und unter Beachtung der Bestimmungen dieser Gesamtbetriebsvereinbarung eingeführt und betrieben werden.

(4) Die Veröffentlichung der Anlagen iSd Absatz 3 erfolgt in gleicher Weise wie die Veröffentlichung dieser Gesamtbetriebsvereinbarung. Von der Veröffentlichung der Verfahrensbeschreibung kann ganz oder teilweise abgesehen werden, soweit dies zur Wahrung von Geschäftsgeheimnissen oder der IT-Sicherheit erforderlich ist. Soll von einer Veröffentlichung ganz oder teilweise abgesehen werden, ist hierüber Einvernehmen mit dem GBR zu erzielen.

(5) Der GBR bildet einen IT-Ausschuss zur Wahrnehmung von Beteiligungsrechten im Zusammenhang mit der Einführung und dem Betrieb von IT-Verfahren und überträgt diesem die Beratungs-, Verhandlungs- und Entscheidungs- bzw. Abschlussbefugnis. Der IT-Ausschuss nimmt die Rechte und Pflichten nach dieser Gesamtbetriebsvereinbarung für den GBR wahr.

§ 4 Leistungs- und Verhaltenskontrollen
(1) Leistungs- und Verhaltenskontrollen sind jeweils grundsätzlich nur iRd bestimmungsgemäßen Einsatzes der IT-Verfahren oder unter den Voraussetzungen des § 26 Abs. 1 S. 2 BDSG zulässig.

(2) Ausnahmsweise dürfen zur Aufdeckung von Straftaten und/oder schwerwiegenden Verletzungen vertraglicher Pflichten personenbezogene Daten von Beschäftigten dann verarbeitet werden, wenn zu dokumentierende tatsächliche einfache Anhaltspunkte den Verdacht begründen, dass der betroffene Beschäftigte im Beschäftigungsverhältnis eine Straftat und/oder schwere Vertragspflichtverletzung begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

90 Burghoff/Scholz ZD 2025, 551.
91 BAG ZD 2025, 714 – Workday.
92 LAG Berlin Brandenburg ZD 2013, 239 mAnm Stück.

(3) Die Datenverarbeitung bzw. Aufklärung nach § 4 Abs. 2 obliegt Compliance und/oder HR/Labour Law der X GmbH oder von diesen beauftragten internen und/oder externen Experten (zB spezialisierte Rechtsanwälte, Wirtschaftsprüfer, IT-Forensiker oÄ). Dabei ist der Datenschutzbeauftragte der X GmbH vorher zu beteiligen. Soweit es die Zwecke nicht gefährdet (zB Verdunkelungsgefahr, Vernichtung/Veränderung von Beweismitteln, Zeugenbeeinflussung), soll der Betroffene beteiligt werden.

(4) Der zuständige Betriebsrat und die Schwerbehindertenvertretung sind zwecks Ausübung ihrer gesetzlichen Beteiligungsrechte (insbesondere § 80 Abs. 1 Nr. 1 BetrVG iVm BDSG, DS-GVO; § 178 Abs. 2 SGB IX) zu informieren. Der Betroffene hat das Recht, sich zu einer Auswertung seiner Daten oder einer persönlichen Befragung bzw. Anhörung von einem Vertreter des für ihn zuständigen Betriebsrats oder der Schwerbehindertenvertretung begleiten zu lassen.

§ 5 Aufbewahrungsdauer/Löschung von personenbezogenen Daten

Personenbezogene Daten werden gem. Art. 17 DS-GVO unverzüglich gelöscht, wenn sie insbesondere für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Die Benutzerstammsätze werden regelmäßig überprüft und nach Ausscheiden der Beschäftigten gelöscht, sofern eine weitere Aufbewahrung nicht aufgrund gesetzlicher Verpflichtung oder aus Beweisgründen erforderlich ist.

§ 6 Kontrollrechte des Betriebsrats

(1) Der GBR ist nach § 80 Abs. 1 Nr. 1, Abs. 2 BetrVG berechtigt, die bestimmungsgemäße Nutzung der IT-Verfahren zu überprüfen. Hierzu kann der GBR bzw. ein von ihm beauftragtes Mitglied im erforderlichen Umfang und iRd gesetzlichen Vorschriften Einblick in das Verfahren nehmen.

(2) Betriebsratsmitglieder unterliegen den Bestimmungen des BetrVG in Bezug auf den Schutz personenbezogener Daten und die Wahrung von Geschäftsgeheimnissen. Der GBR gewährleistet den Schutz der ihm iRd Ausübung seiner Kontrollrechte zugänglich gemachten Daten/Inhalte und ist insoweit nach dieser Vereinbarung zur Verschwiegenheit verpflichtet, wenn nicht bereits ausdrückliche gesetzliche Schweigepflichten bestehen (zB §§ 79, 99 Abs. 1 S. 3, 102 Abs. 2 S. 5, 120 Abs. 2 BetrVG).

§ 7 Datenschutz

(1) Bei Verarbeitung (s. Art. 4 Nr. 2 DS-GVO) personenbezogener Daten sind die externen Vorschriften (DS-GVO, BDSG und weitere datenschutzrelevante Rechtsvorschriften) und X-internen Regelungen zum Datenschutz (Datenschutz- und IS-Richtlinien) anzuwenden.

(2) Die Verantwortung für den Datenschutz bei der Verarbeitung personenbezogener Daten trägt der Arbeitgeber und obliegt ihm als Verantwortlicher (Art. 4 Nr. 7 DS-GVO; § 79a BetrVG).

(3) Die Verarbeitung personenbezogener Daten muss gem. Art. 5 DS-GVO insbesondere den Grundsätzen der Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit entsprechen.

(4) Es gelten darüber hinaus die Vereinbarungen zum Datenschutz in der Rahmen-Gesamtbetriebsvereinbarung zur Umsetzung der DS-GVO bei der X GmbH.

§ 8 Änderungen von IT-Verfahren

(1) Bei Änderungen von IT-Verfahren können die Anlagen iSd § 3 Abs. 2 fortgeschrieben und aktualisiert werden.

(2) Soweit weitere personenbezogene Daten verarbeitet oder zusätzliche Funktionalitäten eingerichtet werden sollen, die eine weitergehende Leistungs- oder Verhaltenskontrolle ermöglichen, bedarf dies der vorherigen Zustimmung des GBR. In diesem Falle ist die fortgeschriebene Anlage dem GBR erneut zur Zustimmung gem. § 3 vorzulegen. § 3 Abs. 3–5 gilt entsprechend.

§ 9 Pilotierung von IT-Verfahren

(1) Bei der Einführung von IT-Verfahren sind häufig Entwicklungs- und Testphasen erforderlich, die einen Pilotbetrieb des Verfahrens erfordern, auch mit personenbezogenen Echtdaten.

(2) Um eine effektive und reibungslose Anwendungsentwicklung zu ermöglichen, kann ein IT-Verfahren iRe Pilotierung auch vor Durchführung des Beteiligungsverfahrens gem. § 3 eingeführt werden. Dem GBR ist ein solcher Pilotbetrieb eines IT-Verfahrens anzuzeigen.

(3) Ein Pilotbetrieb mit personenbezogenen Echtdaten ist ohne gesonderte Zustimmung des GBR nur bis zu einer maximalen Dauer von 6 Monaten zulässig.

(4) Während eines Pilotbetriebs mit personenbezogenen Echtdaten sind Leistungs- und Verhaltenskontrollen von Beschäftigten generell ausgeschlossen, wenn solche nicht zwingend für die Erprobung des IT-Verfahrens erforderlich sind und der GBR hierzu seine ausdrückliche Zustimmung gegeben hat.

§ 10 Nutzung von Social Features in IT-Verfahren der X GmbH

(1) Einige IT-Verfahren der X GmbH verfügen über sog. Social Features: Funktionen, die dem Austausch und der Interaktion mit anderen Nutzern des Verfahrens dienen. Zu den Social Features zählen u.a. die Funktionen Liken (Beiträge mit „Gefällt mir" bewerten), Kommentieren, Teilen, Erwähnen (@Mentioning) und Folgen sowie auch Newsfeeds, Microblogging, Messengerdienste, Foren und Wikis.

(2) Sofern ein IT-Verfahren der X GmbH über Social Features verfügt, ist es dem Nutzer freigestellt, diese Funktionen zu verwenden.

(3) Bei der Nutzung von Social Features in IT-Verfahren werden idR Identifikationsdaten des Nutzers (meist Vorname und Name) sowie ggf. Datums- und Uhrzeitangaben übertragen und innerhalb der Funktion dargestellt. Details sind in den jeweiligen Verfahrensbeschreibungen zu dokumentieren. Mit der freiwilligen Nutzung der Social Features erklärt sich der Nutzer einverstanden, dass seine personenbezogenen Daten in diesem Zusammenhang verarbeitet und für andere Nutzer des IT-Verfahrens sichtbar dargestellt werden. Hier gelten die allgemeinen Benutzerrechte der Betroffenen wie zB Social Features von IT-Verfahren der X GmbH.

(4) Der Nutzer darf nur Inhalte einstellen, die rechtskonform sind (zB keine ehrverletzenden, rassistischen, diskriminierenden oder berechtige Rechte Dritter verletzenden Beiträge). Der die Inhalte einstellende Nutzer trägt dafür die Verantwortung. Der Betreiber des IT-Verfahrens ist berechtigt, die Löschung von rechtswidrigen Inhalten ohne vorherige Ankündigung oder Anhörung vorzunehmen bzw. zu veranlassen.

§ 11 Tools und IT-Verfahren ohne besondere Auswertungsmöglichkeiten

(1) Tools und IT-Verfahren, die nur der technischen Dokumentation, Konfiguration, Systemanalyse (Verfügbarkeit, Performance, Auslastung) oder Systemsicherheit dienen und per-

sonenbezogene Daten lediglich zur Authentifizierung/Authentisierung oder iRv Logfiles bzw. Konfigurationsänderungen verarbeiten, können im Rahmen dieser Gesamtbetriebsvereinbarung ohne gesonderte Verfahrensbeschreibung betrieben werden. Eine detailliertere Protokollierung von Aktivitäten privilegierter Nutzer aus Sicherheitsgründen steht dem nicht entgegen.

(2) Bei Verfahren, die gem. § 11 Abs. 1 ohne gesonderte Verfahrensbeschreibung betrieben werden, ist eine Leistungs- und Verhaltenskontrolle entsprechend § 4 dieser GBV generell ausgeschlossen. Sollte im Ausnahmefall eine Kontrolle erforderlich werden (zB zur Ermittlung der Systemsicherheit), ist hierzu eine gesonderte Zustimmung des GBR einzuholen.

§ 12 Beschlussverfahren Steckbrief
(1) Tools und IT-Verfahren, die

a) keine besonderen Kategorien personenbezogener Daten iSd Art. 9 DS-GVO und

b) keine datenschutzrechtliche Rechtsgrundlage zur Verarbeitung personenbezogener Daten durch den GBR benötigen, und

c) die keine Leistungs- und Verhaltenskontrolle beabsichtigen/intendieren sollen,

können als Steckbrief für einen vereinfachten Beschluss durch den IT-Ausschuss/den GBR eingebracht werden.

(2) Die Inhalte des Steckbriefs ergeben sich aus Anlage X.

(3) Sollte der GBR trotz erfüllter Kriterien des Absatz 1 weitere Informationen benötigen, um seinen Aufgaben iRd Mitbestimmung des § 87 Abs. 1 Nr. 6 BetrVG nachzukommen, so kann er zu dem betreffenden IT-Verfahren weitere Informationen oder die Vorlage einer regulären Anlage zur GBV IT-Rahmen anfordern.

(4) Der GBR lädt, soweit er dies für erforderlich hält, einen Vertreter der Fachseite und/oder der technischen Bereitstellung und Administration zum fraglichen IT-Verfahren in die jeweilige Sitzung ein, der für Fragen zum IT-Verfahren zur Verfügung steht oder, soweit angefragt, das IT-Verfahren vorstellt.

§ 13 Schlussbestimmungen
(5) Diese Gesamtbetriebsvereinbarung tritt mit Unterzeichnung in Kraft und löst die Gesamtbetriebsvereinbarung IT-Rahmen vom [Datum] ab. Die Anlagen A–Z zu den früheren GBV IT-Rahmen vom [Datum] gelten unverändert fort bis zu einer Aufhebung, Ersetzung oder Ablösung.

(6) Die Gesamtbetriebsvereinbarung ist kündbar mit einer Frist von drei Monaten zum Monatsende.

(7) Für die Nachwirkung gelten die gesetzlichen Bestimmungen.

Ort, Datum, Unterschriften

Anlage: Muster Verfahrensbeschreibung/Steckbrief

Anlage xx zur GBV-IT Rahmen

Beschreibung zum IT-Verfahren „[Name des IT-Verfahrens]"

1. Nutzbare Funktionen des IT-Verfahrens
Text …

2. Automatisierte Schnittstellen (Datenimport und -export) zu anderen IT-Verfahren und zu ggf. vorhandenen Dritten, über die zum Zeitpunkt der Einreichung personenbezogene Daten ausgetauscht werden
Text/Visio aus InfoSichhK

3. Zum Zeitpunkt der Einreichung im System vergebene privilegierte Rollen und Rechte
Text/Tabelle

4. Auswertungen/Reports aus personenbezogenen Daten
Text …

5. Owner der technischen Einrichtung (technischer Eigentümer), fachlicher Eigentümer und Betreiber
Text …

6. Zeitplanung und Schulungskonzept (soweit vorgesehen)
Text …

Schnell gelesen …

- Die Implementierung und Anwendung von IT-Tools, die geeignet sind, die Leistung oder das Verhalten von Beschäftigten zu überwachen, ist regelmäßig mitbestimmt nach § 87 Abs. 1 Nr. 6 BetrVG, bedarf also einer Betriebsvereinbarung.
- Die Einführung und Nutzung digitaler IT-Systeme erfordert ein sorgfältig abgestimmtes Zusammenspiel zwischen Compliance-Anforderungen, Datenschutz, individualarbeitsrechtlichen Grundlagen und der Mitbestimmung.
- Der Betriebsrat hat kein allgemeines, umfassendes Mitbestimmungsrecht betreffend Datenschutz. Datenschutzverantwortlicher ist der Arbeitgeber.
- Rahmenbetriebsvereinbarungen, klare Bewertungsverfahren und präzise formulierte Steckbriefe helfen dabei, die Interessen von Arbeitgeber und Beschäftigten in einen verlässlichen, rechtssicheren und transparenten Ausgleich zu bringen.
- Eine IT-Betriebsvereinbarung muss das Datenschutzniveau der DS-GVO achten und darf dieses nicht nach unten absenken.
- Datenschutz ist kein Tatenschutz für betriebliche Straftaten oder schwere Vertragspflichtverletzungen.

RA Volker Stück
ist Lead Expert Arbeitsrecht und Mitbestimmung bei der BWI GmbH in Bonn.

Martin Jung
ist CIO Adviser IT Security, Datenschutz und Mitbestimmung bei der BWI GmbH in Bonn.

Franziska Klein
ist Senior Privacy Expert bei der BWI GmbH in Stetten a.k.M.

Der Beitrag stellt die persönliche Auffassung der Autoren dar.

LION DIRKERS / TOBIAS ROTHKEGEL

Automatisierung von Entscheidungsprozessen nach Art. 22 DS-GVO

Profiling
Auskunfteien
Zahlungsausfallrisiko
eCommerce
Online-Shopping

Praxisbeispiele: Scoring, E-Recruiting und bonitätsgeleitete Zahlartensteuerung im Online-Handel

■ Die Automatisierung von Prozessen spart Ressourcen und erlaubt die Berücksichtigung großer Datenmengen bei der Entscheidungsfindung. Sobald personenbezogene Daten Grundlage automatisierter Entscheidungen werden, die rechtliche oder auf andere Weise erhebliche Auswirkungen auf Betroffene haben, setzt die DS-GVO der Automatisierung jedoch deutliche Schranken und verpflichtet zur Umsetzung besonderer Betroffenenrechte und Transparenzanforderungen. Der Beitrag erörtert, ab wann die Vorgaben zur automatisierten Entscheidungsfindung iSd DS-GVO greifen, und untersucht dazu die Tatbestandsmerkmale von Art. 22 Abs. 1 DS-GVO anhand der praxisrelevanten Beispiele Scoring, E-Recruiting und Zahlartensteuerung. In diesem Rahmen ordnet der Beitrag das für die Auslegung von Art. 22 Abs. 1 DS-GVO zentrale SCHUFA-Scoring-Urteil des EuGH kritisch ein.

■ Process automation saves resources and allows large amounts of data to be considered in decision-making. However, as soon as personal data becomes the basis for automated decisions which have legal or other significant implications for data subjects, the GDPR imposes clear restrictions on automation and requires the implementation of special data subject rights and transparency requirements. This article discusses when the requirements for automated decision-making within the meaning of the GDPR apply and examines the constituent elements of Art. 22 para. 1 GDPR using practical examples such as scoring, e-recruiting and payment method selection. In this context, the article critically assesses the ECJ's SCHUFA scoring ruling, which is central to the interpretation of Art. 22 para. 1 GDPR.
Lesedauer: 24 Minuten

I. Ausgangslage

Eine automatisierte Entscheidungsfindung, die auf personenbezogenen Daten beruht, wird dann von Art. 22 DS-GVO beschränkt, wenn ihr Resultat eine rechtliche oder besondere tatsächliche Tragweite für Betroffene hat. In derartigen Situationen dürfen Entscheidungen nur vollautomatisiert getroffen werden, wenn sie zum Abschluss oder zur Erfüllung eines Vertrags notwendig sind, eine taugliche gesetzliche Erlaubnis besteht oder eine ausdrückliche Einwilligung Betroffener vorliegt, Art. 22 Abs. 2 DS-GVO. Zugleich müssen Verantwortliche in der Folge sicherstellen, dass Betroffene die automatisierte Entscheidung durch einen Menschen unter Berücksichtigung ihres Standpunkts überprüfen lassen können (Art. 22 Abs. 3 DS-GVO) und dass verständliche Informationen über die involvierte Logik der Entscheidungsfindung für Betroffene bereitstehen (Art. 13 Abs. 2 lit. g, 14 Abs. 2 lit. f DS-GVO) und auf Anfrage beauskunftet werden können (Art. 15 Abs. 1 lit. h DS-GVO).

Während der Regelungszweck, dass Menschen in existenziellen Fragen nicht zu Objekten unverständlicher Algorithmen werden dürfen, nachvollziehbar ist, stellt sich in Anbetracht des teils erheblichen Umsetzungsaufwands[1] dennoch die Frage, in welchen Situationen Art. 22 DS-GVO eigentlich greifen soll. Der EuGH hat zu Art. 22 DS-GVO bisher wenig entschieden und lediglich klargestellt, dass Art. 22 DS-GVO drei kumulative Voraussetzungen aufstellt:

- das Vorliegen einer Entscheidung,
- dass diese ausschließlich auf einer automatisierten Verarbeitung (einschließlich Profiling) beruht und
- dass sie der betroffenen Person gegenüber eine rechtliche Wirkung entfaltet oder diese in ähnlicher Weise erheblich beeinträchtigt.[2]

Die Subsumtion praktischer Sachverhalte unter diese Voraussetzungen führt jedoch im Regelfall zu zahlreichen Unklarheiten: Wer trifft die relevante Entscheidung beim Scoring? Welchen Grad muss eine menschliche Überprüfung erreichen, damit Entscheidungen nicht als vollautomatisiert gelten? Und ab wann hat eine Entscheidung eigentlich rechtliche Wirkung oder beeinträchtigt Betroffene in ähnlicher Weise erheblich? Dieser Beitrag fasst zusammen, was bisher zur Auslegung von Art. 22 Abs. 1 DS-GVO aus Rechtsprechung und Behördenausführungen bekannt ist, und beleuchtet hierauf aufbauend die einzelnen Tatbestandsmerkmale der Norm anhand der praxisnahen Beispiele Scoring, E-Recruiting und Zahlartensteuerung.

Weiteres Licht könnte ein Vorabentscheidungsverfahren des ÖOGH bringen, der dem EuGH Fragen zur Anwendung von Art. 22 DS-GVO bei der automatisierten und bonitätsgeleiteten Auswahl von Zahlarten im Online-Versandhandel (im Folgenden: Zahlartensteuerung) vorgelegt hat.[3]

II. (Bonitäts-)Scores: Wer entscheidet beim Scoring worüber?

Das Tatbestandsmerkmal Entscheidung iSv Art. 22 Abs. 1 DS-GVO wird in der DS-GVO nicht definiert und aus dem Wortlaut der Norm ergibt sich lediglich, dass Entscheidungen rechtliche und tatsächliche Auswirkungen haben können. Maßgeblich für das Vorliegen einer Entscheidung im Sinne dieser Norm ist daher ihre Wirkung und nicht ihre Form. Eine Entscheidung ist vor diesem Hintergrund jedes verbindliche Ergebnis eines

1 Prüfung und Schaffung einer Rechtsgrundlage, Implementierung der Betroffenenrechte aus Art. 22 Abs. 3 DS-GVO und Umsetzung der Transparenzanforderungen; zu Art. 15 Abs. 1 lit. h DS-GVO hat der EuGH bereits entschieden, dass die Bereitstellung aussagekräftiger Informationen nicht zur Offenlegung der verwendeten Algorithmen verpflichtet (EuGH ZD 2025, 261 Rn. 60 mAnm Radtke – Dun & Bradstreet Austria). Gerade bei der Nutzung komplexer Algorithmen zur Entscheidungsfindung kann jedoch auch die geforderte Information über konkret verwendete personenbezogene Daten und wie diese im Einzelfall bei der Entscheidungsfindung berücksichtigt wurden herausfordernd sein, vgl. EuGH ZD 2025, 261 Rn. 61 mAnm Radtke – Dun & Bradstreet Austria.

2 EuGH ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.

3 ÖOGH ZD 2026, 210 – in diesem Heft.

Auswahlprozesses, das für Betroffene rechtliche oder tatsächliche Folgen hat.

Weitere Anforderungen nennt die Norm dabei insoweit nicht, sodass die Annahme einer Entscheidung im Rahmen automatisierter Prozesse mit irgendeiner Wirkung für Betroffene grundsätzlich niedrigschwellig ist. So hält der EuGH auch eine Einbeziehung von vorgelagerten Prozessen in den Anwendungsbereich für möglich, sofern diese eine Endentscheidung vorbestimmen, auch wenn diese ggf. durch einen anderen Verantwortlichen getroffen wird.[4] Zudem scheinen nach dem Wortlaut und der bisherigen Instanzenrechtsprechung auch einfache Wenn-Dann-Entscheidungen nicht von Art. 22 Abs. 1 DS-GVO ausgenommen zu sein.

1. Scoring – Bereits eine Entscheidung iSv Art. 22 DS-GVO?

Eine Frage zum Merkmal der Entscheidung, die der EuGH im SCHUFA-Scoring-Urteil beantwortet hat, bezieht sich auf den Urheber der Entscheidung bzw. die (Un-)Mittelbarkeit ihrer Auswirkungen: Während eigentlich Kreditinstitute unter Heranziehung des SCHUFA-Scores (oder anderer Bonitätsscores) entscheiden, ob und zu welchen Konditionen ihre Kunden Kredite erhalten, hat der EuGH es für möglich befunden, dass bereits die Berechnung des Scores durch die Auskunftei eine relevante Entscheidung iSv Art. 22 DS-GVO darstellen kann, wenn der Score „eine maßgebliche Rolle bei der Gewährung des Kredits spielt".[5] Die maßgebliche Rolle des SCHUFA-Scores hielt der EuGH dabei aufgrund der Feststellung des vorlegenden Gerichts – ein unzureichender Score führe „in nahezu allen Fällen" zur Ablehnung des Kreditantrags – für gegeben.[6]

Der EuGH sieht damit bereits in der Berechnung und Zuordnung eines solchen Scores zu einer natürlichen Person eine tatbestandmäßige Entscheidung.

Voraussetzung hierfür ist, dass die vorbereitende Handlung (in Form der Berechnung des Scores) präjudizielle Wirkung für die spätere, unmittelbar wirkende Entscheidung (in Form der Kreditantragsablehnung) hat. Hieraus ergeben sich zwei Erkenntnisse:

- Auch Vorentscheidungen ohne unmittelbare Auswirkung können als Entscheidung iSd Norm gelten, dies jedenfalls wenn sie eine Endentscheidung mit rechtlicher oder erheblicher tatsächlicher Wirkung faktisch vorbestimmen;
- solche Vorentscheidungen unterfallen selbst dann dem Anwendungsbereich von Art. 22 DS-GVO, wenn die relevante Endentscheidung von einem anderen Verantwortlichen getroffen wird.

Der dahinterstehende Rechtsschutzgedanke ist in Dreieckskonstellationen, in denen Träger der Vorentscheidung und Träger der Endentscheidung personenverschieden sind, nachvollziehbar. Denn die anwendenden Kreditinstitute können nicht ohne Weiteres aussagekräftige Informationen über das Zustandekommen des externen Bonitätsscores nach Art. 15 Abs. 1 lit. h DS-GVO geben und die den Score berechnenden Auskunfteien wurden bis zu diesem Urteil nicht als Urheber einer Entscheidung iSv Art. 22 DS-GVO angesehen. Ob diese Rechtsprechung hingegen zu einer vorhersehbaren und rechtssicheren Anwendung von Art. 22 DS-GVO beiträgt, ist jedenfalls in Dreieckskonstellationen zweifelhaft. Denn ob ein Bonitätswert das Zustandekommen eines Folgegeschäfts praktisch determiniert, hängt nun mal von der Verwendung des Scores ab. Wie Scores von Kunden praktisch eingesetzt werden, liegt aber außerhalb der Sphäre der Auskunfteien und kann schwerlich generalisiert werden. Demgemäß sollte eine Übertragbarkeit des Urteils auf andere (vermeintlich vergleichbare) Konstellationen nicht ohne Weiteres angenommen werden. So betont auch der Gerichtshof, dass sich die Vorlagefrage (und somit auch deren weitere Beantwortung) ausdrücklich (nur) auf die automatisierte Erstellung eines auf personenbezogene Daten zu einer Person gestützten Wahrscheinlichkeitswerts hinsichtlich deren Fähigkeit, künftig einen Kredit zu bedienen, bezieht.[7] Auch sollte hierbei der exponierte Stellenwert des SCHUFA-Scores in der deutschen Kreditwirtschaft zwingend berücksichtigt werden. So stand (nach den Sachverhaltsfeststellungen des vorlegenden Gerichts im konkreten Fall) fest, dass im Fall eines von einem Verbraucher an eine Bank gerichteten Kreditantrags ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen dazu führe, dass die Bank die Gewährung des beantragten Kredits ablehnt.[8]

Sofern man in der Erstellung eines Bonitätswerts eine relevante Entscheidung iSv Art. 22 Abs. 1 DS-GVO sieht, ergibt sich zudem für Auskunfteien die Herausforderung, eine Rechtsgrundlage für ihr Scoring nach Art. 22 Abs. 2 DS-GVO zu finden. Denn mangels direkter Beziehung zu den betroffenen Endkunden ist die Einholung einer ausdrücklichen Einwilligung praktisch schwierig umsetzbar und die Vertragserfüllung mangels Vertrag oft nicht möglich. Auch fehlt gegenwärtig ein entsprechender Erlaubnistatbestand im Unions- oder deutschen Recht (vgl. Art. 22 Abs. 2 lit. b DS-GVO).[9]

Der deutsche Gesetzgeber plant durch eine Novellierung des § 31 BDSG Abhilfe zu schaffen, indem neben der Verwendung von Scorewerten zukünftig auch deren Erstellung unter bestimmten Voraussetzungen erlaubt werden soll. Auskunfteien stünde damit eine Rechtsgrundlage iSv Art. 22 Abs. 2 lit. b DS-GVO zur Seite. Die in der 20. Legislaturperiode eingebrachte Gesetzesnovelle, die § 31 BDSG hierfür durch einen neuen § 37a im BDSG ersetzen wollte,[10] wurde nicht mehr verabschiedet. Obgleich die BfDI empfohlen hat die Reform in der 21. Legislaturperiode erneut aufzugreifen,[11] scheinen jedenfalls ausweislich des Koalitionsvertrags[12] gegenwärtig keine entsprechenden Reformbestrebungen seitens der aktuellen Regierung zu existieren.

Die deutsche Instanzenrechtsprechung behilft sich zT damit, festzustellen, dass streitgegenständliche Bontitätsscores nicht in nahezu allen Fällen die nachfolgende Kreditentscheidung determinieren und Art. 22 DS-GVO auf die Scorewert-Erstellung nicht anwendbar sei.[13] Andere Gerichte halten zumindest die Erstellung des SCHUFA-Scores in Folge des EuGH-Urteils nun ohne Weiteres für eine Entscheidung iSv Art. 22 DS-GVO mit der Folge, dass diese erstmal nicht mehr vollautomatisiert erstellt werden dürften.[14] Auch das VG Wiesbaden, das dem EuGH die Fragen im SCHUFA-Scoring-Verfahren vorgelegt hatte, hat mittlerweile – wenig überraschend – geurteilt, dass die Erstellung und Weitergabe des Scorewerts durch die SCHUFA die betroffene

4 EuGH ZD 2024, 157 Rn. 47 f. mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
5 EuGH ZD 2024, 157 Rn. 50 mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
6 EuGH ZD 2024, 157 Rn. 48 mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
7 EuGH ZD 2024, 157 Rn. 47 mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
8 EuGH ZD 2024, 157 Rn. 48 mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
9 EuGH ZD 2024, 157 Rn. 71 f. mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
10 BT-Drs. 20/10859, 10 f.
11 BfDI, Datenschutzpolitische Agenda für die 21. Wahlperiode des Deutschen Bundestages, Dezember 2024, S. 16.
12 Vgl. Koalitionsvertrag von CDU, SPD und CSU zur 21. Legislaturperiode, 2025, S. 70.
13 Vgl. OLG Stuttgart Hinweisbeschl. v. 18.3.2025 – 9 U 20/25 Rn. 27 ff.
14 Vgl. LG Leipzig Urt. v. 29.5.2024 – 7 O 2658/23 Rn. 35.

Klägerin iSv Art. 22 Abs. 1 DS-GVO in ähnlicher Weise erheblich beeinträchtige und der Anwendungsbereich der Norm damit eröffnet sei.[15] Nach Auffassung der Kammer genüge hierfür, dass eine Entscheidung geeignet sei, „eine Vorgriffswirkung auf die Begründung, Änderung oder Aufhebung einer rechtlichen Position der betroffenen Person zu haben"[16], was beim SCHUFA-Score hinsichtlich der Kreditvergabe allgemein der Fall sei und erst recht bei Scores der SCHUFA, die individuell für Kreditinstitute erstellt würden.[17]

Auch wenn das EuGH-Urteil im SCHUFA-Scoring-Verfahren aus den o.g. Gründen nicht verallgemeinerungsfähig ist, bietet es doch wertvolle Hinweise für einerseits die Rechtserheblichkeit der Berechnung anderer Scorewerte sowie andererseits deren rechtskonforme Ausgestaltung. Sofern Unternehmen interne Scores bilden und diese bei Bedarf heranziehen, um Entscheidungen mit besonderer Tragweite zu treffen, kann auch hier bereits die Score-Bildung als Entscheidung iSv Art. 22 Abs. 1 DS-GVO gelten, wenn die später zu treffende Entscheidung maßgeblich von diesem Score abhängt. Denkbar ist dies zB bei Beförderungsentscheidungen, die von einem automatisch gebildeten Performance-Score auf Basis verschiedener Leistungskennzahlen determiniert werden. Sofern absehbar ist, dass ein Score negative Auswirkungen für Betroffene haben wird, muss konsequenterweise bereits die Score-Bildung mit Art. 22 DS-GVO konform sein. Durch den Umstand, dass auch etwaige einer finalen Entscheidung vorausgehende Zwischenschritte (für sich genommen) ggf. von Art. 22 DS-GVO erfasst sein können, sollten alle relevanten Etappen innerhalb eines Entscheidungsprozesses entsprechend bewertet werden.

2. Komplexität von automatisierten Entscheidungen?

Art. 22 Abs. 1 DS-GVO sieht hinsichtlich der Qualität einer solchen Entscheidung darüber hinaus keine weiteren Anforderungen vor. Während man bei automatisierter Entscheidungsfindung inklusive Profiling zunächst an komplexe Prozesse denkt, bei denen Algorithmen auf Basis großer Datenmengen ein Ergebnis errechnen oder prognostizieren, kann eine automatisierte Entscheidungsfindung aber theoretisch bereits in simplen Wenn-Dann-Entscheidungen vorliegen. Wenn zB bei einer biometrischen Einlasskontrolle die biometrischen Merkmale des Gesichts ausgewertet und mit den in einer Datenbank hinterlegten Gesichtsprofilen abgeglichen werden, ist das eine Verarbeitung personenbezogener Daten, die automatisch passiert und darüber entscheidet, ob eine Person das Gebäude betreten kann oder ihr der Eintritt verwehrt wird.

Eine Anwendung von Art. 22 DS-GVO scheint in einem solchen Kontext wenig sinnvoll, da die sehr einfache Entscheidungslogik für jeden verständlich ist und nicht einleuchtet, warum Verantwortliche nun einen Rechtfertigungsgrund gegenüber Unberechtigten benötigen, die erfolglos versuchen sich Zutritt zu verschaffen. Denn hier wäre ein Mensch bei entsprechender Entscheidung über den Zutritt aufgrund der gleichen menschlich vorherbestimmten Logik (Berechtigung ja/nein?) sinnvollerweise zum gleichen Ergebnis gekommen. Vergleichbare Fragen stellen sich auch beim Einsatz (komplexerer) Filterungsfunktionen. In der Literatur wird vor diesem Hintergrund zT überzeugenderweise eine teleologische Reduktion (bzw. entsprechende Auslegung) des Anwendungsbereichs von Art. 22 Abs. 1 DS-GVO dahingehend gefordert, dass einfache Wenn-Dann-Entscheidungen nicht darunterfallen sollen.[18]

In der aufsichtsbehördlichen Praxis und Rechtsprechung wird dies zT anders gesehen. So geht zB der Tätigkeitsbericht der Sächsischen Datenschutz- und Transparenzbeauftragten (SDTB) von 2021 auf Seite 90 davon aus, dass auch biometrische Einlasskontrollen durch Art. 22 Abs. 1 DS-GVO reguliert sind, und auch das VG Bremen geht beim automatisierten Erlass von Abfallgebührenbescheiden aufgrund einer Gebührenverordnung grundsätzlich von der Anwendbarkeit von Art. 22 DS-GVO aus.[19]

III. Tool-Einsatz in Recruitment-Prozessen

Art. 22 Abs. 1 DS-GVO ist nur einschlägig, sofern eine Entscheidung ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruht. Nach dem Unionsgesetzgeber setzt dies voraus, dass eine Entscheidung „ohne jegliches menschliche Eingreifen" getroffen wird.[20] Die Frage ist also: Wie viel menschliches Zutun ist erforderlich, damit eine Entscheidung nicht als ausschließlich automatisiert gilt?

Hinsichtlich der Qualität menschlichen Eingreifens betont der Europäische Datenschutzausschuss (EDSA), dass eine Person tatsächlich Einfluss auf die Entscheidung haben muss und zu deren Änderung „befugt und befähigt" sein muss.[21] In den Entscheidungsprozess involvierte Personen müssen fachlich in der Lage sein, eine Entscheidung in der konkreten Materie treffen bzw. beurteilen zu können, und organisatorisch die Autorität besitzen, solch eine Entscheidung zu ändern. Sofern eine automatisierte Entscheidung nicht sowieso durch einen Menschen abgeändert wird, muss diese also durch einen Menschen mit der im konkreten Fall geforderten Ernsthaftigkeit geprüft werden.

Hinsichtlich der Quantität menschlichen Eingreifens ist noch nicht abschließend geklärt, ob bei systematisch und massenhaft getroffenen Entscheidungen jede einzelne Entscheidung geprüft werden muss oder eine stichprobenartige Prüfung oder eine Kontrolle von Ausreißern genügen kann, damit sämtliche Entscheidungen eines Systems nicht als vollautomatisiert gelten. Reine Stichproben ändern nach überwiegender Meinung in der Literatur nichts am vollautomatisierten Charakter massenhaft getroffener Entscheidungen.[22] Dies ergibt insofern Sinn, als der Schutz von Art. 22 DS-GVO vor einer (fehlerhaften) Systementscheidung bei lediglich Stichprobenkontrollen auf wenige, zufällig ausgewählte Betroffene reduziert würde und damit der Schutzzweck der Norm weitgehend ins Leere liefe. So sieht es auch das VG Bremen, das eine Stichprobenkontrolle einzelner Abfallgebührenbescheide nicht für ausreichend hält, um hinsichtlich des automatisierten Erlasses von Abfallgebührenbescheiden insgesamt von einer menschlich getroffenen Entscheidung auszugehen.[23]

Anders wird zT die systematische Überprüfung von Entscheidungen gesehen, die unplausibel oder unerwartet sind.[24] Dem

15 VG Wiesbaden Urt. v. 19.11.2025 – 6 K 788/20.WI Rn. 178 = ZD 2026, 232 (gekürzt) mAnm Schild.
16 VG Wiesbaden Urt. v. 19.11.2025 – 6 K 788/20.WI Rn. 179 = ZD 2026, 232 (gekürzt) mAnm Schild.
17 VG Wiesbaden Urt. v. 19.11.2025 – 6 K 788/20.WI Rn. 192 = ZD 2026, 232 (gekürzt) mAnm Schild.
18 Vgl. BeckOK DatenschutzR/von Lewinski, 54. Ed. 1.11.2025, DS-GVO Art. 22 Rn. 12; Kühling/Buchner, DS-GVO BDSG/Buchner, 4. Aufl. 2024, DS-GVO Art. 22 Rn. 18; Gola/Heckmann, DS-GVO BDSG/Schulz, 3. Aufl. 2022, DS-GVO Art. 22 Rn. 19.
19 VG Bremen ZD 2026, 179 Rn. 24.
20 Vgl. Erwägungsgrund 71 S. 1 aE DS-GVO.
21 Art. 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018, S. 22.
22 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 22 Rn. 30; Kühling/Buchner, DS-GVO BDSG/Buchner, 4. Aufl. 2024, DS-GVO Art. 22 Rn. 15; Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 22 Rn. 19.
23 VG Bremen ZD 2026, 179 Rn. 23.
24 BeckOK DatenschutzR/von Lewinski, 53. Ed. 1.8.2025, DS-GVO Art. 22 Rn. 25.1; Kühling/Buchner, DS-GVO BDSG/Buchner, 4. Aufl. 2024, DS-GVO Art. 22 Rn. 15.

ist zuzustimmen, sofern die systematische Überprüfung gewährleistet, dass nicht geprüfte, plausible bzw. erwartete Entscheidungen im Einklang mit der Entscheidungslogik stehen und dementsprechend eine menschliche Überprüfung mit Sicherheit nicht zu einer Abänderung der Entscheidung führen würde. Denn in einem solchen Fall würde die Anwendung von Art. 22 DS-GVO nicht zu zusätzlichem Schutz, sondern allein zu zusätzlichem Aufwand führen.

Im Recruiting-Bereich werden vermehrt automatisierte Entscheidungssysteme eingesetzt, um aus Bewerberdatenbanken eine Vorauswahl geeigneter Kandidaten zu bestimmen, die dann im Bewerbungsverfahren weiter berücksichtigt werden (sog. short-listing). Dies führt gem. Art. 22 DS-GVO grundsätzlich zu drei rechtlich zu unterscheidenden Personengruppen:

- Bewerber, die iRd Vorauswahl bereits eliminiert werden,
- Bewerber, die vorausgewählt werden, aber die Stelle schließlich nicht erhalten sowie
- Bewerber, die vorausgewählt werden und die Stelle erhalten.

Wenngleich eine finale Einstellungsentscheidung regelmäßig auf Grundlage von Gesprächen durch eine Person getroffen wird, liegt bereits in dieser Vorauswahl eine ausschließlich automatisierte Entscheidung anhand der Verarbeitung personenbezogener Daten, die Art. 22 DS-GVO unterfallen kann. Kandidaten teilen iRd Bewerbung Lebensläufe und weitere Informationen, diese werden von entsprechender Software ausgewertet und relevante Attribute je Person abgespeichert. Abhängig von der zu besetzenden Stelle kann die Software anschließend Bewerber mit passenden Attributen vorschlagen und berücksichtigt dabei u.a. Fähigkeiten, Abschlüsse, praktische Erfahrungen und Wohnort.

In Bezug auf vorausgewählte Personen, die die Stelle erhalten, liegt keine Entscheidung vor, die diese Personen beeinträchtigt. Da die Entscheidung grundsätzlich zugunsten der vorausgewählten Personen geht, ist Art. 22 DS-GVO insoweit nicht anwendbar. Bei Personen, die auf die Shortlist kommen, aber letztlich die Stelle nicht erhalten, muss im Einzelfall geprüft werden, wie die Entscheidung getroffen wurde. Prüfen Recruiter die automatisiert erstellte Shortlist händisch, liegt bei Ablehnung der Bewerbung keine automatisierte Entscheidung vor. Verlassen sich Recruiter hingegen auch bei der Shortlist unkritisch auf eine Empfehlung der eingesetzten Software, wird im rechtlichen Sinne weiterhin eine automatisierte Entscheidung vorliegen. Vor diesem Hintergrund sollte beim Einsatz derartiger Tools besonderes Augenmerk auf eine entsprechende Prozessgestaltung sowie entsprechende Anweisung bzw. Training der Recruiter gelegt werden.

Anders verhält es sich jedenfalls mit Personen, die schon gar nicht auf die Shortlist gekommen sind. Hier liegt eine beeinträchtigende Entscheidung vor, die auch ausschließlich automatisiert getroffen wurde. Aufgrund der regelmäßig komplexen Bewertung der Jobeignung durch entsprechende Software, ist auch eine systematische Überprüfung unplausibler Ergebnisse praktisch schwer denkbar, um aus dem Anwendungsbereich von Art. 22 DS-GVO herauszufallen. Es muss sodann geprüft werden, ob angesichts der Umstände des Einzelfalls eine wirksame Einwilligung von Bewerbern eingeholt werden kann oder die Verarbeitung zum Abschluss eines Vertrags erforderlich ist.

IV. Zahlartensteuerung im Online-Handel

Schließlich sollen aber nur solche Entscheidungen von Art. 22 Abs. 1 DS-GVO erfasst sein, die entweder eine rechtliche Wirkung für Betroffene entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen.

Mangels Definition dieser Tatbestandsalternativen bleibt hier viel Raum für Auslegung und lediglich die in Erwägungsgrund 71 S. 1 DS-GVO genannten Beispiele der automatischen „Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren[s] ohne jegliches menschliche Eingreifen" lassen erkennen, dass der Unionsgesetzgeber Entscheidungen vor Augen hatte, die eine grundlegende Bedeutung für die Lebensführung Betroffener haben. Auch der EDSA und der Generalanwalt im SCHUFA-Scoring-Verfahren gehen grundsätzlich davon aus, dass Art. 22 Abs. 1 DS-GVO nur Entscheidungen mit „schwerwiegenden Auswirkungen" erfasst.[25] Wann diese Schwelle im Einzelfall überschritten ist, ist in der Praxis hingegen oftmals stark umstritten, wie man exemplarisch am Beispiel der Zahlartensteuerung sehen kann.

1. Rechtliche Wirkung

Nach dem Wortlaut der Norm und dem allgemeinen sprachlichen Verständnis von „rechtlicher Wirkung" liegt es nahe, eine solche anzunehmen, wenn Rechte der betroffenen Person durch die automatisierte Entscheidung unmittelbar betroffen sind, weil sie zB begründet, aufgehoben oder inhaltlich verändert werden.[26] In diesem Sinne setzt auch der EDSA für eine rechtliche Wirkung iSd Norm voraus, dass die Entscheidung die Rechte einer Person oder ihren rechtlichen Status betrifft oder Rechte aus einem Vertrag betroffen sind.[27]

Bei der im Online-Handel üblichen Zahlartensteuerung werden Kunden vor Abschluss der Bestellung aufgrund einer automatisierten Berechnung der Zahlungsausfallwahrscheinlichkeit uU nicht alle grundsätzlich verfügbaren Zahlarten angeboten, sondern nur solche, bei denen der Versandhändler kein finanzielles Risiko eingeht. Die Zahlungsausfallwahrscheinlichkeit wird entweder anhand eigener Informationen insbesondere etwa zum historischen Zahlungsverhalten von Kunden berechnet (interne Bonitätsprüfung) und/oder anhand der Bonitätsscores externer Auskunfteien (externe Bonitätsprüfung). Altkunden mit offenen Rechnungen oder Neukunden, die einen schlechten oder keinen externen Bonitätsscore haben, wird in der Folge regelmäßig der Kauf auf Rechnung nicht als Zahlart angeboten, da der Versandhändler hier in Vorleistung geht. Gleichzeitig ist es Kunden in einem Fall, in dem bestimmte Zahlarten nicht angeboten werden, immer noch möglich den Bestellprozess mit einer anderen Zahlart abzuschließen, die für den Versandhändler kein finanzielles Risiko birgt (etwa Vorkasse per Banküberweisung). Regelmäßig behalten sich Versandhändler in ihren AGB vor, bestimmte Zahlarten im Einzelfall nicht anzubieten und stellen klar, dass kein Anspruch auf die Inanspruchnahme einer bestimmten Zahlart besteht.

Vor diesem Hintergrund ist eine rechtliche Wirkung der Zahlartensteuerung abzulehnen. Auf der einen Seite wird Kunden nicht der Vertragsabschluss als solcher verwehrt, sondern lediglich die Nutzung einer bestimmten Zahlart, um die Gegenleistung zu erbringen. Dabei ist schon zweifelhaft, ob die Ablehnung eines Vertragsabschlusses überhaupt eine rechtliche Wirkung entfaltet oder nicht vielmehr eine tatsächliche Beeinträchtigung darstellt. Dafür spricht, dass in diesem Fall nicht in ein bestehendes Recht eingegriffen wird (abgesehen von Sachverhalten mit Kontrahierungszwang) und die Formulierung von Erwägungsgrund 71 S. 1 DS-GVO suggeriert, dass die Ablehnung

25 Art. 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018, S. 23; GA Pikamäe SA v. 16.3.2023 – C-634/21 Rn. 34 – SCHUFA Holding AG.

26 Vgl. Paal/Pauly, DS-GVO BDSG/Martini, 3. Aufl. 2021, DS-GVO Art. 22 Rn. 26.

27 Art. 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018, S. 23.

eines Online-Kreditantrags oder einer Online-Bewerbung Beispiele für eine erhebliche Beeinträchtigung iSd Norm sind. Auf der anderen Seite wird Kunden bei entsprechender Klarstellung in den AGB auch nicht das Recht genommen eine bestimmte Zahlart zu nutzen.

So sieht es auch der ÖOGH, der kürzlich zur Frage der Zahlartensteuerung im Versandhandel eine Vorlage an den EuGH beschlossen hat und im Vorlagebeschluss die Ansicht vertritt, dass „die bloße Verwehrung bestimmter Vertragskonditionen – und insbesondere der Abschluss von Verträgen nur unter Gewährung bestimmter (für den Händler kein kreditorisches Risiko aufweisender) Bezahlverfahren – keine rechtliche Wirkung für die Kunden entfaltet, weil eine solche Entscheidung weder eine Rechtsposition des Kunden noch ein Rechtsverhältnis zu ihm begründet"[28].

2. Ähnlich erhebliche Beeinträchtigung

Entscheidend ist daher, ob Betroffene durch Verweigerung bestimmter Zahlarten erheblich beeinträchtigt sind. Zur Auslegung des nicht definierten Tatbestandsmerkmals sind Wortlaut, Systematik und Sinn und Zweck der Norm entsprechend zu würdigen und zwar gem. Erwägungsgrund 71 DS-GVO.[29] In Anbetracht des Wortlauts „erheblich beeinträchtigt" (der jedenfalls auch in der englischen und französischen Sprachfassung mit „significantly affects" bzw. „l'affectant de manière significative" semantisch äquivalent ist) kann nicht bereits bei jeder negativ fühlbaren Entscheidung von einer relevanten Beeinträchtigung iSd Art. 22 Abs. 1 DS-GVO ausgegangen werden, sondern erst wenn diese von besonderer Tragweite für die Lebensführung ist. Die in Erwägungsgrund 71 S. 1 DS-GVO genannten Beispiele unterstreichen diese Auslegung. Denn vom Erfolg im Bewerbungsverfahren hängt idR die Schaffung bzw. der Erhalt der Lebensgrundlage ab und die eigene Kreditwürdigkeit entscheidet oft darüber, ob man für die Lebensführung wesentliche Gegenstände finanzieren kann, wie eine Immobilie oder ein Auto. Daneben nennt der EDSA als grundsätzlich erfasste Beispiele Entscheidungen über den Zugang zu Gesundheitsleistungen oder Bildung.[30]

Systematisch impliziert die Gegenüberstellung zur Tatbestandsalternative der rechtlichen Wirkung lediglich, dass nur Beeinträchtigungen tatsächlicher Art erfasst sind. Die Bezugnahme zur Tatbestandsalternative mittels der Worte „in ähnlicher Weise" kann wiederum bedeuten, dass die erhebliche Beeinträchtigung entweder mit einer rechtlichen Wirkung vergleichbar sein muss[31] (wie zB die Ablehnung eines Vertragsabschlusses im Ergebnis mit der Kündigung eines Vertrags vergleichbar sein kann) oder dass der Unionsgesetzgeber die Prämisse hatte, dass eine rechtliche Wirkung grundsätzlich erheblich ist. Der Sinn und Zweck der Norm, die Betroffene vor unverständlichen Computerentscheidungen ohne Einwirkungsmöglichkeit schützen soll, gibt keine Anhaltspunkte dazu, ab wann solch ein Schutz eigentlich geboten ist.

Die Vergleichbarkeit mit einer rechtlichen Wirkung wäre bei der Zahlartensteuerung nur gegeben, würde dies im Ergebnis regelmäßig zu einer Verwehrung des Vertragsabschlusses führen. Dies ist denkbar, wenn Kunden lediglich eine Zahlart angeboten würde, die wenig verbreitet ist, sodass Kunden tatsächlich daran gehindert wären den Bestellvorgang abzuschließen. Bei der Belassung üblicher Zahlarten zur Zahlung, liegt eine Verwehrung des Vertragsabschlusses dagegen fern. So meint auch der ÖOGH, „dass eine erhebliche Beeinträchtigung bei bloßer Festlegung auf ein bestimmtes Zahlverfahren zu verneinen ist, solange dem Kunden – wie hier – die Möglichkeit eingeräumt wird, den Vertrag unter Verwendung anderer, zumutbarer Zahlungsarten abzuschließen".[32]

Gleichzeitig bringt das Verwehren der Zahlart Kauf auf Rechnung auch keine Nachteile mit sich, die von besonderer Tragweite für die Lebensführung sind. Zwar ermöglicht der Kauf auf Rechnung bestellte Produkte wieder zu retournieren, wenn sie einem nicht gefallen oder nicht passen, bevor der Kaufpreis fällig wird, sodass Kunden für retournierte Ware gar nicht erst den Kaufpreis überweisen müssen. Es ist jedoch nicht erkennbar, dass dieser Vorteil für die Lebensführung von Menschen von grundlegender Bedeutung ist und dessen Abwesenheit in der Folge schwerwiegende Auswirkungen mit sich bringt. Wenn man ein besonders starkes Bedürfnis danach hat, ein Produkt vor seiner Bezahlung zu begutachten, zB weil es besonders teuer ist, dann steht wohlmöglich zum einen der Kauf auf Rechnung aufgrund des erhöhten Risikos sowieso nicht zur Verfügung und zum anderen besteht oft die Möglichkeit, sich entsprechende Produkte auch in Ladengeschäften anzuschauen (zB Möbel, Fahrräder).

Der EDSA sieht als Faktoren zur Bestimmung einer erheblichen Beeinträchtigung zudem, ob das Verhalten oder die Entscheidungen von betroffenen Personen erheblich beeinträchtigt werden, eine Beeinträchtigung dauerhaft oder für einen längeren Zeitraum besteht und ob die Entscheidung zum Ausschluss oder zur Diskriminierung führt.[33] Auch unter Berücksichtigung dieser Faktoren liegt eine erhebliche Beeinträchtigung nicht nahe: Die Zahlartensteuerung bezieht sich jeweils auf einen Bestellvorgang und hat keine lange oder dauerhafte Wirkung. Das Kaufverhalten kann bei Wegfallen der Zahlart Kauf auf Rechnung punktuell beeinflusst werden, da Bestellungen ggf. genauer geprüft werden und uU weniger bestellt wird. Dies stellt aber keine erhebliche Beeinträchtigung des Verhaltens oder der Kaufentscheidung dar. Denn wenn die angebotene Zahlart darüber entscheidet, ob bzw. wie viel bestellt wird, dann war die Kaufentscheidung regelmäßig schon nicht gefestigt. Auch liegt keine relevante Diskriminierung in der Zahlartensteuerung, solange die Berechnung der Ausfallwahrscheinlichkeit nicht an Merkmale wie Rasse, ethnische Herkunft, politische Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetische Anlagen oder Gesundheitszustand sowie sexuelle Orientierung anknüpft.[34] Nicht überzeugend ist jedenfalls, dass eine bloße Andersbehandlung von Betroffenen genügt, um eine erhebliche Beeinträchtigung iSv Art. 22 DS-GVO anzunehmen. Ein solches Verständnis findet keinen Anknüpfungspunkt im Gesetz und steht zudem im Widerspruch zu den relevanten Erwägungsgründen zur DS-GVO sowie bisher ergangener EuGH-Rechtsprechung. Auch lässt sich dies nicht mit den Ausführungen des EDSA in Einklang bringen.

Die Abwesenheit von Zahlarten, bei denen der Versandhändler in Vorleistung geht, wie beim Kauf auf Rechnung oder bei der Ratenzahlung, hat natürlich den Nachteil, dass Kunden nicht in den Genuss eines Zahlungsaufschubs kommen, was je nach akuter finanzieller Situation der Betroffenen dazu führen kann, dass eine Bestellung in den nächsten Monat verschoben werden muss. Selbst wenn dies im Einzelfall ungünstig sein

28 ÖOGH ZD 2026, 210 Rn. 21 – in diesem Heft.
29 Vgl. EuGH Urt. v. 7.12.2023 – C-634/21 Rn. 41 = ZD 2024, 157 (gekürzt) mAnm Söbbing/Schwarz und mAnm Schild – SCHUFA Holding.
30 Art. 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018, S. 22.
31 So zB ausdrücklich VG Wiesbaden Urt. v. 19.11.2025 – 6 K 788/20.WI Rn. 179 = ZD 2026, 232 (gekürzt) mAnm Schild.
32 ÖOGH ZD 2026, 210 Rn. 22 – in diesem Heft.
33 Art. 29-Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018, S. 23.
34 Vgl. Erwägungsgrund 71 S. 6 DS-GVO.

kann, kann man nicht davon ausgehen, dass die Zahlartensteuerung deswegen allgemein schwerwiegende Auswirkungen für Betroffene hat – zumal Zahlarten mit einem finanziellen Risiko in der Praxis auch nur dann angeboten werden, wenn Versandhändler das damit einhergehende Risiko einschätzen können.

Ob der EuGH das auch so sehen wird, steht auf einem anderen Blatt. Jedenfalls besteht Hoffnung, dass die Vorlage des ÖOGH auch über die Frage der Zahlartensteuerung hinaus weitere Klärung über die Auslegung von Art. 22 DS-GVO bringen wird.

V. Fazit

Es zeigt sich, dass die Bewertung, wann die Vorgaben zur automatisierten Entscheidungsfindung iSv Art. 22 DS-GVO zu beachten sind, herausfordernd sein kann, da die Tatbestandsvoraussetzungen von Art. 22 Abs. 1 DS-GVO nach wie vor mit zahlreichen ungeklärten Fragen verbunden sind.

Zusammengefasst sollten Verantwortliche dabei jedenfalls folgende Aspekte berücksichtigen:

- Der Anwendungsbereich von Art. 22 DS-GVO kann grundsätzlich bei jedem Ergebnis eines auf Basis personenbezogener Daten automatisiert geführten Auswahlprozesses eröffnet sein, das rechtliche oder tatsächlich erhebliche Auswirkungen für Betroffene hat.
- Auch können bereits einer eigentlichen Entscheidung vorgelagerte Schritte erfasst sein, wie etwa die Zuweisung eines Scores oder die Zuordnung zu einer Gruppe, sofern vorgelagerte Schritte eine spätere Entscheidung faktisch vorbestimmen. Bei der Frage nach der faktischen Vorbestimmung durch „Entscheidungen" Dritter ist dabei ein strenger Maßstab anzulegen. Insbesondere verbietet sich eine vorschnelle Übertragung des SCHUFA-Scoring-Urteils des EuGH angesichts der besonderen Stellung der SCHUFA in der deutschen Kreditwirtschaft und der Prämisse der Vorlagefrage, ein unzureichender SCHUFA-Score führe „in nahezu allen Fällen" zur Ablehnung des Kreditantrags.
- Eine besondere Komplexität der Entscheidungsfindung wird vom Wortlaut des Art. 22 Abs. 1 DS-GVO nicht gefordert und zT auch von Aufsichtsbehörden und der Instanzenrechtsprechung nicht als Voraussetzung für dessen Anwendbarkeit erachtet. Obgleich gute Argumente für die Position sprechen, dass einfache Wenn-Dann-Entscheidungen nicht von der Ratio des Art. 22 DS-GVO erfasst sind, ist die Annahme dieser Position risikobehaftet. Zur Vermeidung unsachgemäßer Ergebnisse, sollte zunächst geprüft werden, ob Auswirkungen überhaupt die Schwelle der rechtlichen Wirkung oder ähnlich erheblichen Beeinträchtigung erreichen oder ob die Implementierung menschlicher Kontrolle in den Entscheidungsprozess praktisch möglich ist.
- Um auszuschließen, dass eine Entscheidung ausschließlich automatisiert erfolgt, ist im Entscheidungsprozess vorzusehen, dass ein Mensch befugt und befähigt ist, eine maschinell vorbereitete Entscheidung (bzw. Entscheidungsempfehlung) zu überprüfen und bei Bedarf abzuändern. Hier bestehen durchaus relevante Gestaltungsspielräume, um eine rechtskonforme Implementierung zu ermöglichen. Die Durchführung von Stichprobenkontrollen genügt dabei im Regelfall nicht, um auch alle nicht überprüften Entscheidungsvorgänge aus dem Anwendungsbereich von Art. 22 DS-GVO herausfallen zu lassen. Anders kann dies hingegen bei der (zwingend vorgesehenen) Nachprüfung von Ausreißerfällen bzw. unplausiblen oder sonstigen auffälligen Entscheidungsergebnissen aussehen.
- Eine Entscheidung hat lediglich dann rechtliche Wirkung, wenn hierdurch die (vertraglichen) Rechte oder der rechtliche Status eines Betroffenen begründet, geändert oder aufgehoben werden. Schwieriger zu bewerten ist, wann eine sonstige erhebliche Beeinträchtigung vorliegt. Wann diese Schwelle erreicht ist, ist dabei durchaus umstritten. Die DS-GVO nennt dabei jedenfalls die automatische Ablehnung eines Kredits oder einer Stellenbewerbung als erfasste Konstellationen. Erforderlich ist jedenfalls eine hinreichende Tragweite, etwa durch eine wesentliche Beeinflussung des Verhaltens oder Entscheidungsfindung des Betroffenen, eine Dauerhaftigkeit bzw. jedenfalls längere Dauer oder gar ausschließende oder diskriminierende Auswirkungen der Entscheidung.
- In komplexeren Entscheidungsprozessen kann es erforderlich sein, die hiervon betroffenen natürlichen Personen in verschiedene Kohorten einzuteilen, da diese im Lichte von Art. 22 DS-GVO anders zu bewerten (und sodann anders zu behandeln) sein können. Dies gilt entsprechend für einzelne Auswahl- bzw. Verarbeitungsschritte innerhalb der Reihe, da diese für sich betrachtet einzeln von Art. 22 DS-GVO erfasst sein können.

Schnell gelesen ...

- Während eine Umsetzung der mit Art. 22 DS-GVO verbundenen Betroffenenrechte, Transparenz- und Rechtmäßigkeitsanforderungen einen erheblichen Aufwand erfordern kann, ist mangels präzisierender Rechtsprechung oft nicht eindeutig, wann Art. 22 Abs. 1 DS-GVO anwendbar ist.
- Der EuGH hat klargestellt, dass auch vorbereitende Schritte als Entscheidung iSv Art. 22 Abs. 1 DS-GVO erfasst sein können, sofern diese eine spätere Entscheidung mit unmittelbarer Auswirkung praktisch determinieren.
- Entscheidungsprozesse gelten nur dann nicht als vollautomatisiert, wenn ein Mensch die Letztentscheidung trifft bzw. sich die automatisierte Entscheidung nach ernsthafter Prüfung aneignet.
- Art. 22 Abs. 1 DS-GVO erfasst richtigerweise nur Entscheidungen mit besonderer Tragweite, die schwerwiegende tatsächliche oder rechtliche Auswirkungen für Betroffene haben. Die automatisierte Verwehrung risikobasierter Zahlarten im Online-Handel gehört nicht dazu.

Lion Dirkers, LL.M. (KCL), Maître en droit (Paris 2),
ist Rechtsanwalt und Senior Associate im Hamburger Büro von Osborne Clarke.

Dr. Tobias Rothkegel
ist Rechtsanwalt und Partner im Hamburger Büro von Osborne Clarke.

SANDRA HUSI-STÄMPFLI

Privacy by Design als Instrument der Datenethik

Vom rechtlichen Prinzip zur gelebten Verantwortung

Wertorientierte Datenarchitektur
Ethics by Design
Fairness by Design
Governance

■ Der Beitrag untersucht, wie der Grundsatz des Privacy by Design als verbindendes Element zwischen Datenschutzrecht und Datenethik fungiert. Privacy by Design verpflichtet dazu, Datenschutz und ethische Werte wie Transparenz, Fairness und Autonomie bereits in der technischen und organisatorischen Gestaltung digitaler Systeme zu verankern. Am Beispiel von Gesundheits-Apps und Schulplattformen zeigt der Beitrag, wie rechtliche Anforderungen der DS-GVO und der KI-VO bzw. im Schweizer Rechtskontext des Datenschutzgesetzes konkrete ethische Verantwortung operationalisieren können. Privacy by Design erweist sich dabei nicht nur als Compliance-Instrument, sondern als Ausdruck institutioneller Integrität: Es übersetzt die rechtliche Pflicht zur Rechenschaft in eine Kultur digitaler Verantwortung – und macht Ethik im Code praktisch erfahrbar.

■ This article examines how the principle of Privacy by Design acts as a connecting element between data protection law and data ethics. Privacy by Design requires data protection and ethical values such as transparency, fairness and autonomy to be embedded in the technical and organisational design of digital systems. Using the example of health apps and school platforms, the article shows how legal requirements of the GDPR and the German AI Regulation (AI-Act), or in the Swiss legal context of the Data Protection Act, can operationalise concrete ethical responsibility. In this context, Privacy by Design proves to be not only a compliance tool, but also an expression of institutional integrity: it translates the legal accountability obligation into a culture of digital responsibility – and makes ethics in code a practical experience.
Lesedauer: 20 Minuten

I. Einleitung

Die digitale Transformation unserer Gesellschaft macht sich nicht nur in offenkundigen Phänomenen wie Smartwatches, zunehmend „intelligenten" Haushaltsgeräten und Fahrzeugen oder dem niederschwelligen Austausch mit ChatGPT bemerkbar. Auch administrative Abläufe sowie Produktions- und Entscheidungsfindungsprozesse verändern sich und profitieren von den neuen Technologien.

In diesem Kontext lassen gerade auf datenbasierten Systemen beruhende automatisierte, dh KI-unterstützte Entscheidungsfindungen mit uU nur marginalem menschlichen Zutun den Ruf nach einer ethischen Rahmung lauter werden: Im Zentrum steht längst nicht mehr nur die Rechtmäßigkeit eines Entscheids über Bildungschancen, Versicherungsprämien oder Maßnahmen der Strafverfolgung, sondern auch die Frage, was letztendlich gerecht, dh ethisch vertretbar, ist.

Der Beitrag zeigt auf, wie die gesetzgebenden Organe sowohl in der EU als auch in der Schweiz mit dem Prinzip von Privacy by Design ein datenschutzrechtliches Instrument geschaffen haben, das ebendiese ethischen Überlegungen aufgreifen und in die Konzeption von datenbasierten Systemen und Applikationen einführen soll.

II. Überblick Ethik und Recht

Die Ethik als Teilbereich der Philosophie beschäftigt sich mit der Frage, was „richtiges" und „gutes" Handeln ist: Sie bietet einen Kompass, der auf Werten wie Gerechtigkeit, Ehrlichkeit und Respekt beruht.[1] Diese Werte können sich kontextabhängig und dynamisch verändern und variieren teilweise auch über mehrere Gemeinschaften hinweg. So grundlegend diese Werte sein mögen, verbindlich oder rechtlich durchsetzbar sind sie, für sich allein genommen, nicht.

Anders verhält es sich hingegen mit der zweiten Disziplin, die das gesellschaftliche Zusammenleben regelt, dem Recht. Es definiert, welches Verhalten innerhalb einer Gesellschaft erlaubt, verboten oder geboten ist – unabhängig von den persönlichen Überzeugungen einzelner Mitglieder. Damit gewährleistet das Recht die Aufrechterhaltung von Ordnung und Gerechtigkeit in der jeweiligen Gesellschaft und vermag diese aufgrund der institutionalisierten Verbindlichkeit und der damit einhergehenden Sanktionen auch durchzusetzen.[2] Verglichen mit den moralischen[3] Werten einer Gesellschaft ist das Recht „starr". Es ist zwar ebenfalls wandelbar, da in den Rechtsetzungsprozess jedoch idR verschiedene staatliche Institutionen eingebunden werden, bedarf eine Anpassung an neue Gegebenheiten deutlich mehr Zeit als die Veränderung der gesellschaftlichen Wahrnehmung einer bestimmten Situation.

Die zumindest materiellen Grenzen zwischen Ethik und Recht sind damit offenkundig fließend, die beiden Disziplinen stehen in einem wechselseitigen Verhältnis zueinander: Rechtsnormen basieren regelmäßig auf den ethischen Überzeugungen der jeweiligen Gesellschaft.

III. Datenethische Gerechtigkeit in der digitalisierten Gesellschaft

Die Datenethik als wissenschaftliche Teildisziplin der Ethik umfasst den Umgang mit Daten, insbesondere deren Erhebung, Bearbeitung, Nutzung und Weitergabe. Die „Daten" im Kontext der Datenethik beschränken sich dabei nicht nur auf Personendaten, sondern schließen den Umgang mit nicht-personenbezogenen Daten (zB Verkehrs-, Umwelt- oder Energiedaten) mit ein, unabhängig davon, ob diese strukturiert oder unstrukturiert sind.[4] Begründen lässt sich dies mit dem Umstand, dass auch aggregierte oder anonymisierte Daten in ihrer Kombination und

1 Hübner, Einführung in die philosophische Ethik, 4. Aufl. 2024, S. 17.
2 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025.
3 Ethik und Moral sind nicht zu verwechseln, s. dazu zB Schmidt, Ethik in der IT-Sicherheit, 2. Aufl. 2023, Kap. 2 Ziff. 2.5, das Buch ist abrufbar unter: https://pressbooks.pub/itethik/chapter/begriffliche-grundlagen-im-kontext-der-ethik/; prägnant dazu auch Rosenthal: „Unter dem Begriff der Moral sind Vorgaben für ein angebrachtes Verhalten zu verstehen. Ethik hingegen bezeichnet die philosophische Disziplin, mit der unterschiedliche Moralvorstellungen analysiert werden", Rosenthal, Datenethik – ein praktischer Zugang aus Sicht der Compliance, abrufbar unter: https://www.rosenthal.ch/downloads/RRCO-Rosenthal-Datenethik.pdf.
4 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, Rn. 14 f.

bei der Verwendung in algorithmischen Systemen zu Verzerrungen und damit zB zu diskriminierenden Vorhersagen und Bewertungen führen können. Auch die Konzentration großer Datenmengen (unabhängig davon, ob diese einen Personenbezug aufweisen oder nicht) auf wenigen Plattformen wirft grundlegende ethische Fragen zu Themen wie der digitalen Souveränität oder der missbräuchlichen Ausnutzung der Marktmacht auf.[5]

Damit wird deutlich: Aus datenethischer Sicht entscheidend ist nicht die Art der Daten, sondern die Konsequenz deren Nutzung sowohl für Individuen als auch für die Gesellschaft als Gesamtes. Gerechtigkeit als gesellschaftliches bzw. datenethisches Konzept verlangt in der digitalisierten Gesellschaft daher nach Prinzipien wie Transparenz, Fairness, Autonomie und Gemeinwohlorientierung.[6] Gestaltungspflichten sollen mit anderen Worten nicht nur formal und gestützt auf das geltende Recht, sondern auch werteorientiert umgesetzt werden: Nur, weil etwas grundsätzlich erlaubt ist, bedeutet das nicht, dass es auch gerecht sein und zwingend umgesetzt werden muss.

Als Kern der Datenethik schaffen Transparenz und Erklärbarkeit dabei in einem ersten Schritt die notwendigen Voraussetzungen zur Wahrung der Autonomie der betroffenen Personen[7]: Nur wenn eine Datenbearbeitung transparent und nachvollziehbar ist, können die betroffenen Personen ihre informationelle Selbstbestimmung wahrnehmen[8] und ihre ethischen Ansprüche wahren, nur wenn Verantwortlichkeiten klar (dh transparent)[9] sind, können Datenbearbeitungsvorgänge nachvollzogen werden.

Transparenz und Nachvollziehbarkeit sind aber letztendlich auch der Grundstein für faire und am Gemeinwohl[10] orientierte Datenbearbeitungen: Die Möglichkeit, dass Datenbearbeitungen hinterfragt und einer öffentlichen Kontrolle unterworfen werden, zwingt die datenbearbeitenden Stellen, sich am datenethischen Gemeinwohl zu orientieren und damit die Autonomie von Individuen und der Gesellschaft im Kontext von Datenbearbeitungsvorgängen zu wahren. Der Einsatz datenbasierter Systeme darf nicht zu einer schleichenden Einschränkung der informationellen Selbstbestimmung und damit der Entscheidungsfreiheit und Autonomie von Individuen führen.[11]

IV. Privacy by Design als ethische Architektur

Mit Art. 25 DS-GVO[12] hat die EU den Grundstein für eine frühzeitige Berücksichtigung des Datenschutzes in IT-Projekten gelegt, der Schweizer Gesetzgeber hat mit Art. 7 Abs. 1 Schweiz. DSG[13] eine analoge Bestimmung geschaffen und ist dem Vorbild der EU im Jahr 2023 gefolgt: Privacy by Design bzw. Datenschutz durch Technikgestaltung verlangt, dass Datenschutz bereits bei der Entwicklung von Systemen und Prozessen mitgedacht wird.[14] Konkret soll der Schutz von Personendaten nicht erst durch nachträgliche Maßnahmen wie Audits oder Benutzereinstellungen[15] gewährleistet werden: Insbesondere Transparenz, Nachvollziehbarkeit und Verhältnismäßigkeit der Datenbearbeitungen sind durch eine vorausschauende Auswahl von Systemen und Applikationen sowie gezielte technische und organisatorische Maßnahmen (TOMs), die es zu implementieren gilt, sicherzustellen.[16] Die Leitlinien 4/2019 des Europäischen Datenschutzausschusses (EDSA) zu Art. 25 DS-GVO[17] präzisieren sodann, dass Privacy by Design kein einmaliges Projektziel, sondern ein fortlaufender Prozess ist: Datenschutz muss in alle Phasen des Systemlebenszyklus integriert werden.

Privacy by Design ist damit deutlich mehr als die Aufforderung, die (Datenschutz-)Rechtskonformität bereits in der Projektphase sicherzustellen. Im Kern ist Privacy by Design eine Architekturpflicht, die die Risiken für die Privatsphäre minimieren und gleichzeitig die Kontrolle der betroffenen Personen stärken soll – mit anderer Brille betrachtet also ein Ansatz, der Ethics by Design[18] verlangt.

So kann etwa das Prinzip der Datenminimierung nicht nur als technische Pflicht interpretiert werden, sondern durchaus auch als Ausdruck des ethischen Werts der Selbstbegrenzung:[19] Vertritt eine Organisation – der öffentlichen Verwaltung oder Privatwirtschaft – die Überzeugung, dass sie nur jene Informationen erfasst und bearbeitet, die tatsächlich für ihre Aufgabenerfüllung bzw. ihren Geschäftszweck notwendig sind, oder lebt sie nach dem Maximalprinzip? Wie großzügig legt sie (gesetzliche) Ermessensspielräume hinsichtlich der Datenbearbeitungsmöglichkeiten aus und wie fundiert rechtfertigt sie die Menge der bearbeiteten Daten?

Das Prinzip der Transparenz transformiert wiederum juristische Dokumentationspflichten in eine ethische Verpflichtung zur Nachvollziehbarkeit und damit auch in das möglichst transparente Design eines Systems. Informationsasymmetrien sind zu vermeiden, Transparenz ist nicht als Selbstzweck zu verstehen, sondern als Merkmal einer datenethisch verantwortungsbewussten Grundhaltung gegenüber den Betroffenen.

Besonders deutlich wird dies im KI-Kontext: So hat die von der EU-Kommission im Jahr 2018 eingesetzte Hochrangige Expertengruppe für Künstliche Intelligenz im Jahr 2019 sieben Anforderungen für vertrauenswürdige und ethische KI[20] definiert:

- menschliche Handlungsfähigkeit,
- technische Robustheit,
- Datenschutz und Governance,
- Transparenz,
- Fairness,
- gesellschaftliches Wohlergehen und
- Rechenschaftspflicht.[21]

5 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, Rn. 15.

6 Bührmann/Schmidt, Gerechte digitalisierte Gesellschaften brauchen Zugang und Befähigung, 37. CSR-Magazin, 6.10.2021, abrufbar unter: https://csr-news.net/2021/10/06/gerechte-digitalisierte-gesellschaften-brauchen-zugang-und-befaehigung/.

7 Deutscher Ethikrat, Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz – Stellungnahme v. 20.3.2023, abrufbar unter: https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf, dort Querschnittsthema 10, S. 376 ff.

8 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, Rn. 18 ff.

9 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, Rn. 22 ff.

10 Budelacci, Mensch, Maschine, Identität – Ethik der künstlichen Intelligenz, 2022, S. 53.

11 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, 36.

12 VO (EU) 2016/679 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (DS-GVO), ABl L 119 v. 4.5.2016, 1 ff.

13 Schweiz. Bundesgesetz v. 25.9.2020 über den Datenschutz (Datenschutzgesetz, SR 235.1).

14 Praxiskommentar DSGVO/Freund/Schöning, 2023, Art. 25 Rn. 17.

15 Dazu der Grundsatz von Privacy by Default, Schweiz. DSG Art. 7 Abs. 3; Husi-Stämpfli/Morand, Datenschutzrecht litera B., 2. Aufl. 2024, Rn. 220 ff.; Praxiskommentar DSGVO/Freund/Schöning, 2023, Art. 25 Rn. 28 ff.

16 Erwägungsgrund 78 DS-GVO, Privacy by Design.

17 https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.

18 EU-Kommission, Ethics By Design and Ethics of Use Approaches for Artificial Intelligence, 2021, abrufbar unter: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf.

19 Husi-Stämpfli/Thanabalan, Datenethik in der öffentlichen Verwaltung, Jusletter 29.9.2025, Rn. 18 ff.

20 Ethik-Leitlinien für eine vertrauenswürdige KI, 2019, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425.

21 Expertengruppe für KI, Ethik-Leitlinien für eine vertrauenswürdige KI, 2019, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425, S. 17 ff.

Die im Frühjahr 2024 verabschiedete KI-VO der EU[22] baut auf diesen Prinzipien auf[23] und verpflichtet schließlich mit Art. 9–14 KI-VO die Anbieter sog. Hochrisiko-KI-Systeme zu einem umfassenden Risikomanagement, zur Qualität der Datensätze, zu Transparenz gegenüber Nutzerinnen und Nutzern, zu menschlicher Aufsicht und zu technischen Sicherheitsmaßnahmen.

Die Stärke von Privacy by Design liegt somit darin, dass es zentrale Werte der Datenethik operationalisierbar macht: Rechenschaft, Fairness, Nichtschädigung und Autonomie. Während Ethik häufig abstrakt und schwer argumentierbar bleibt, zwingt die datenschutzrechtliche Systemgestaltung zur konkreten Umsetzung: Welche Daten werden erhoben? Wer hat Zugriff? Wie kann eine betroffene Person Eingriffsmöglichkeiten behalten? Diese Fragen sind nicht nur compliance-relevant, sondern moralisch bedeutsam, wie die nachfolgenden beiden Beispiele illustrieren.

1. Beispiel Gesundheits-Apps: Fairness, Fürsorge und Gemeinwohlorientierung

Die Digitalisierung des Gesundheitsbereichs verspricht immense Chancen: KI in der Diagnostik und im Operationssaal, smarte Hilfsmittel, die Seniorinnen und Senioren ein möglichst langes und selbstbestimmtes Leben in den eigenen vier Wänden ermöglichen sollen, und Applikationen, die Vitaldaten zur Bewegungsanalyse nutzen oder Medikamentenerinnerungen absetzen. Gerade im Gesundheitsbereich zeigt sich das Spannungsfeld zwischen technischer Innovation, rechtlicher Regulierung und ethischer Verantwortung besonders deutlich.

Die datenschutzrechtlichen Prinzipien von Rechtmäßigkeit, Verhältnismäßigkeit und Zweckbindung allein vermögen es jedoch nicht, der Datenethik im Gesundheitswesen Genüge zu tun. Eine App, die Vitaldaten analysiert, Empfehlungen zur Bewegung oder Ernährung ausspricht oder Gesundheitsrisiken prognostiziert, muss nicht nur rechtmäßig funktionieren, sondern auch gerechte, nachvollziehbare und fürsorgliche Resultate hervorbringen. Die Datenethik verlangt, dass Systeme nicht nur korrekt, sondern auch gerecht arbeiten. Hier rücken datenethische Werte wie Fairness, Fürsorge und Gemeinwohlorientierung in den Vordergrund – Prinzipien, die das Datenschutzrecht in seiner normativen Struktur nur am Rande kennt, die aber für gesellschaftliche Akzeptanz zentral sind.

Fairness by Design bedeutet in diesem Kontext, dass algorithmische Modelle so konzipiert und überwacht werden, dass sie keine systematischen Verzerrungen erzeugen. Werden zB Bewegungsdaten in einer Gesundheits-App ausgewertet, darf daraus keine indirekte Diskriminierung einzelner Nutzerinnen und Nutzer oder ganzer Gruppen resultieren, etwa, indem die App Trainingsziele oder Risikoprofile nach Alter, Geschlecht oder sozioökonomischem Hintergrund verzerrt berechnet oder aber implizite Normen körperlicher Leistungsfähigkeit reproduziert.

Fairness beginnt dabei bereits bei der Datenerhebung: Trainingsdatensätze müssen repräsentativ sein und die Vielfalt der Nutzenden widerspiegeln. Werden Gesundheitsdaten nur von jungen, gesunden, technologisch affinen Personen erhoben, reproduzieren sich strukturelle Biases automatisch im System. Es gilt aber auch, die Algorithmen im weiteren Verlauf des Betriebs regelmäßig zu überprüfen und auf unbeabsichtigte Verzerrungen zu testen. Solche Überprüfungen können über Bias-Audits, unabhängige Validierungsstudien oder automatisierte Kontrollmechanismen erfolgen. Die KI-VO greift dies explizit auf: Art. 10 KI-VO verpflichtet Anbieter von Hochrisiko-KI-Systemen zu Maßnahmen für Datenqualität und Datenrepräsentativität; Art. 15 KI-VO verlangt Transparenz und Nachvollziehbarkeit. Für Gesundheits-Apps bedeutet das konkret, dass Entscheidungen technisch erklärbar und medizinisch überprüfbar sein müssen – ein Grundsatz, der datenschutzrechtliche bzw. -ethische Nachvollziehbarkeit mit medizinethischer Verantwortung verbindet.

Aus datenethischer Perspektive steht zudem das Prinzip der Fürsorge im Vordergrund. Technologien, die im Alltag mit sensitiven Gesundheitsinformationen umgehen, müssen so gestaltet sein, dass sie Menschen nicht verunsichern oder bevormunden, sondern unterstützen. Umgesetzt werden kann dies etwa durch motivierende Hinweise bzw. positive Verstärkung anstelle von Angstkommunikation. Anstatt einer vorwurfsvollen Nachricht im Sinne von „Sie bewegen sich heute weniger als gestern" ist zB der folgende Hinweis denkbar: „Sie haben die letzten Tage viel geleistet, gönnen Sie sich heute einen ruhigeren Tag, um Ihr Schrittziel morgen wieder zu erreichen". Auch adaptive Benachrichtigungen, zB indem die Applikation bei Hitzewarnungen oder schlechter Luftqualität Bewegungsempfehlungen auf kühlere Tageszeiten verschiebt und entsprechende Hinweise zu möglichen Vorsichtsmaßnahmen (Trainieren im Schatten, ausreichende Flüssigkeitsaufnahme) macht, werden dem Fürsorgeprinzip gerecht.

Ebenso wichtig ist, dass die Nutzenden den Grad der Automatisierung selbst bestimmen können: Eine ethisch verantwortungsvolle App bietet Optionen für manuelle Kontrolle, temporäres Pausieren oder Datenlöschung, anstatt Verhaltensüberwachung dauerhaft zu erzwingen. Ethik zeigt sich hier in der Haltung der Technologie: Sie dient, statt zu bevormunden. Privacy by Design als rechtliche Anforderung kann dazu beitragen, diese ethische Grundhaltung umzusetzen.

Applikationen und die darin stattfindenden individuellen Datenbearbeitungen sollen ferner auch zum Gemeinwohl beitragen: Daten sollten nicht ausschließlich zur kommerziellen Nutzung, sondern – in anonymisierter Form – auch zur Verbesserung der öffentlichen Gesundheitsversorgung bereitgestellt werden, so etwa zur Früherkennung epidemiologischer Trends oder zur Entwicklung patientenzentrierter Behandlungsansätze. Voraussetzung ist jedoch, dass die Datenverwendung transparent, nachvollziehbar und freiwillig bleibt. Privacy by Design kann hier als technisches Instrument dienen, um kollektiven Nutzen und individuellen Schutz zu vereinen: Datenräume mit abgestuften Zugriffsrechten, differenzierte Anonymisierungsmethoden oder Einwilligungsplattformen mit granularer Kontrolle sind praktische Umsetzungsbeispiele.

Auf organisatorischer Ebene bedeutet Privacy bzw. Ethics by Design schließlich, dass Entwickler, Datenschutzbeauftragte und medizinische Fachpersonen gemeinsam an der Schnittstelle von Technik und Ethik arbeiten. Dies erfordert interdisziplinäre Design-Prozesse, die medizinische Standards, Datenschutzrecht und Nutzerperspektiven zusammenführen. Bereits in der Konzeptionsphase sollten ethische Risikoanalysen durchgeführt und dokumentiert werden – zB iRv Ethical Impact Assessments, wie sie auch vom Europäischen Datenschutzbeauftragten (EDSB)[24] und der UNESCO[25] empfohlen werden.

Privacy by Design muss im Kontext von Gesundheits-Apps somit weit über den Schutz personenbezogener Daten hinausgehen.

22 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der VO (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der RL 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (KI-VO).

23 Erwägungsgrund 27 KI-VO.

24 S. ausf. dazu unter: https://www.edps.europa.eu/data-protection/our-work/ethics_en.

25 S. das Hilfsmittel der UNESCO „Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence", 2023, abrufbar unter: https://unesdoc.unesco.org/ark:/48223/pf0000386276.

Richtig umgesetzt, bildet es eine ethische Infrastruktur, die Vertrauen schafft, ohne Innovation zu hemmen. Es verbindet technischen Fortschritt mit moralischer Reflexion – und macht aus Gesundheits-Apps nicht nur digitale Werkzeuge, sondern verantwortungsvolle Partner im Dienst der Gesundheit.

2. Beispiel Schulplattformen: Datenminimierung und Fairness im Zentrum

Digitale Lernplattformen verarbeiten (sensitive) Leistungsdaten, Daten über Interaktionsmuster, Lernverhalten, Sprachkompetenzen oder sogar emotionale Reaktionen auf Lerninhalte von Schülerinnen und Schülern. Was ursprünglich als pädagogisches Hilfsmittel konzipiert war, kann so zu einem datengetriebenen Bewertungssystem werden, das tief in die Privatsphäre von Kindern eingreift.

Die KI-VO erkennt die Tragweite solcher Anwendungen daher auch ausdrücklich an: Nach Annex III Ziff. 3 KI-VO gelten Systeme, die für Bildungs- oder Berufsbildungszwecke eingesetzt werden und den Zugang zu Bildung beeinflussen können, als Hochrisiko-KI-Systeme. Entsprechend gelten die Pflichten zu Risikomanagement, Transparenz, Datenqualität und menschlicher Aufsicht, Art. 9 ff. KI-VO. Die EU-Kommission betont, dass gerade in Bildungsumgebungen algorithmische Bewertungen erhebliche Auswirkungen auf Chancengleichheit und Selbstbestimmung haben.

Die Verbindung von Datenschutzrecht und Datenethik ist im Schulkontext somit keine theoretische, sondern eine praktische Notwendigkeit: Schulen verfügen zwar idR über die notwendigen gesetzlichen Grundlagen, um Schülerinnen- und Schülerdaten zu bearbeiten, die Pflicht der Schulen geht aber weiter bzw. tiefer, denn die Datenethik fragt: Wie kann ein System gestaltet werden, das die Würde und Autonomie der Lernenden wahrt?

Ein Privacy-by-Design- bzw. Ethics-by-Design-Ansatz beginnt im Schulkontext mit strikter Datenminimierung. Lernanalysen sind so zu konzipieren, dass sie auf pseudonymisierten oder lokal gespeicherten Datensätzen beruhen, ohne zentrale Leistungsprofile zu erzeugen. Die technische Architektur sollte auf Dezentralität und Datensparsamkeit ausgelegt sein – etwa durch lokale Speicherung auf Schulservern oder Endgeräten und nicht auf Cloud-Plattformen mit kommerzieller Auswertung. In diesem Zusammenhang wird auch Privacy by Default als Schwesterprinzip zu Privacy by Design relevant: Alle nicht zwingend erforderlichen Analysen und Funktionen sind standardmäßig zu deaktivieren und sollten erst nach informierter Zustimmung (der Eltern und/oder der Kinder und Jugendlichen) aktiviert werden können.

Als zweiter Pfeiler der Datenethik stehen im Schulkontext Transparenz[26] und Erklärbarkeit im Fokus, wobei diese beiden Prinzipien auch in pädagogischer Hinsicht von Relevanz sind: Lernende müssen verstehen können, wie die Plattform zu ihren Einschätzungen kommt. Statt Black-Box-Scoring sind erklärbare Visualisierungen vorzusehen, die zeigen, welche Faktoren zu einem Ergebnis geführt haben („Dein Lernfortschritt in Grammatik basiert auf den letzten fünf Übungen in dieser Kategorie"). So wird Algorithmic Literacy[27] bzw. Privacy Literacy[28] gefördert – zentrale Elemente datenethischer Bildung. Kinder sollen im schulischen Umfeld erfahren, was Datensouveränität und informationelle Selbstbestimmung bedeutet – durch altersgerechte Einstellungen, Wahlmöglichkeiten („Wer darf meinen Fortschritt sehen?") und Simulationen von Datenfreigaben. Dieser Ansatz harmoniert mit den Zielen des Europäischen Bildungsraums[29] und der UNESCO-Empfehlung zu Ethik und KI im Bildungswesen, die fordert, dass Bildungstechnologien menschenzentriert, inklusiv und auf Vertrauen basierend gestaltet werden[30]. Schulplattformen sind damit nicht nur Lernwerkzeuge, sondern auch ethische Testfelder für gesellschaftliche Werte.

Das im o.g. Beispiel bereits umschriebene Prinzip von Fairness by Design ist darüber hinaus auch im Schulkontext von Relevanz: Die Algorithmen dürfen keine systematischen Verzerrungen erzeugen, etwa zugunsten bestimmter Sprachgruppen oder sozioökonomischer Hintergründe. KI-Modelle, die Lernfortschritte auswerten, müssen deshalb regelmäßig auf Bias überprüft und validiert werden. ZB kann ein Algorithmus, der Schreibfähigkeiten bewertet, unbewusst Kinder mit Migrationshintergrund benachteiligen, wenn Trainingsdaten überwiegend aus standardsprachlichen Texten stammen. Hier helfen die bereits unter IV.1. erwähnten Datenqualitätsprüfungen gem. Art. 10 KI-VO, um die Repräsentativität der Trainingsdaten sicherzustellen.

Schließlich ist mit der Fairness auch die Fürsorgepflicht eng verknüpft: Im Schulkontext bedeutet Fürsorge by Design, dass Systeme Lernende nicht überwachen oder bewerten, sondern unterstützen. ZB kann eine Plattform, die erkennt, dass eine Schülerin überdurchschnittlich lange für Aufgaben braucht, Hilfestellungen oder alternative Lernpfade anbieten, statt Defizite zu markieren. Dashboards, die Lernfortschritte visualisieren, sollten nicht primär auf Vergleich und Wettbewerb ausgerichtet sein („Du liegst hinter dem Klassendurchschnitt."), sondern auf Selbstreflexion und Motivation („Du hast dich in dieser Woche verbessert – weiter so!"). Die App darf keine Ranglisten erzeugen, die soziale Dynamiken verstärken, sondern sollte Feedback individuell, ermutigend und lernförderlich gestalten.

Der datenschutzrechtliche Grundsatz von Privacy by Design kann damit dazu beitragen, ein pädagogisch-ethisches Leitmotiv umzusetzen: Kinder und Jugendliche sollen lernen, digitale Systeme als Werkzeuge, nicht als Überwachungsinstanzen zu begreifen. Was im Schulalltag beginnt, wirkt sich auch auf die übrigen Lebensbereiche aus und legt einen wesentlichen Grundstein, informationell selbstbestimmte Bürgerinnen und Bürger heranwachsen zu lassen.

V. Governance und Verantwortlichkeit: Privacy by Design als ethisches Organisationsprinzip

Privacy by Design erschöpft sich nicht in technischen Anforderungen. Es ist ein Organisationsprinzip, das die Art und Weise verändert, wie Institutionen ihre datenethische Verantwortung wahrnehmen. Werte wie Transparenz, Fairness und Selbstbestimmung sind in die Strukturen des Betriebs und die jeweiligen Zuständigkeiten zu implementieren. Eine solche Verankerung erfordert klare Rollen: Der Datenschutzbeauftragte sichert rechtliche Konformität, während ein Chief Information Security Officer technische Integrität gewährleistet. Ergänzend braucht es Governance-Stellen, die ethische Fragestellungen prüfen – etwa Ethik-Boards, die systematische Bewertungen zu Fairness,

26 Fenner, Digitale Ethik, 2025, S. 299 ff.

27 Taddicken/Schumann, Algorithms and Communication/Dogruel, What is Algorithm Literacy?, A Conceptualization and Challenges Regarding its Empirical Measurement, 2021, S. 67 f.

28 Zu den verschiedenen Definitionen Wissinger, Privacy Literacy: From Theory to Practice, Communications in Information Literacy, Vol. 11, No. 2, 2017, S. 378 f.

29 Europäischer Rat, Europäischer Bildungsraum, abrufbar unter: https://www.consilium.europa.eu/de/policies/education-area/, sowie Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Aktionsplan für digitale Bildung, 18.1.2018, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-5459-2018-INIT/de/pdf, dort Ziff. 4.2, S. 8 ff.

30 UNESCO-Empfehlung zur Ethik der künstlichen Intelligenz, 2023, abrufbar unter: https://www.unesco.de/dokumente-und-hintergruende/publikationen/detail/unesco-empfehlung-zur-ethik-der-kuenstlichen-intelligenz/, dort Empfehlungen 101 ff.

Transparenz und gesellschaftlicher Wirkung durchführen.[31] In modernen Verwaltungs- und Unternehmensstrukturen gewinnen auch Digital Compliance Offices an Bedeutung, die Schnittstellen zwischen Recht, Technik und Ethik bilden und für Kohärenz sorgen.

Internationale Standards liefern dafür praxistaugliche Rahmenbedingungen. Die ISO/IEC 27701 (Privacy Information Management System) erweitert klassische Informationssicherheitsstandards um datenschutzspezifische Steuerungsmechanismen. Sie fördert die Dokumentation von Prozessen, Verantwortlichkeiten und Risikobewertungen. Die ISO/IEC 42001, die sich auf KI-Managementsysteme bezieht, legt ergänzend fest, dass Organisationen für den gesamten Lebenszyklus ihrer KI-Systeme – von der Datenbeschaffung über das Training bis zur Nutzung – Strukturen zur Gewährleistung von Transparenz, Nachvollziehbarkeit und Fairness schaffen müssen.[32] Beide Normen zeigen, dass technische Governance ohne ethische Reflexion unvollständig bleibt.

VI. Fazit: Ethik im Code – die Zukunft datenschutzkonformer Systeme

Privacy by Design steht an der Schnittstelle von Recht, Ethik und Technik. Es konkretisiert die Pflicht zur datenschutzrechtlichen Rechenschaft in Form einer gelebten Verantwortung – sowohl auf der Ebene der Systemarchitektur als auch in der Organisation. Indem es ethische Grundwerte wie Transparenz, Fairness, Fürsorge und Autonomie in rechtlich verbindliche Pflichten übersetzt, wird Privacy by Design zum normativen Bindeglied zwischen Datenschutz und digitaler Gerechtigkeit.

Rechtliche Vorgaben allein können kein Vertrauen schaffen; sie setzen lediglich den Rahmen. Erst die bewusste Entscheidung, technische und organisatorische Gestaltung im Sinne dieser Werte auszurichten, bildet die Grundlage für legitime Datenbearbeitung in einer digitalisierten Gesellschaft. Privacy by Design ist somit mehr als eine Compliance-Anforderung – es ist Ausdruck institutioneller Integrität.

Ob Gesundheits-App, Schulplattform oder andere Anwendungsfälle: Datenschutz im Designprozess mindert nicht nur das Risiko für die informationelle Selbstbestimmung der betroffenen Personen, sondern stärkt den ethischen Mehrwert der jeweiligen Anwendung. Eine datengestützte Gesellschaft, die Privacy by Design ernst nimmt, baut Vertrauen nicht durch Kontrolle, sondern durch Einsicht und Selbstbegrenzung auf. In diesem Sinne ist Privacy by Design die juristisch präziseste und zugleich praktischste Form gelebter Datenethik – Ethik im Code.

Schnell gelesen ...

- Privacy by Design verknüpft Datenschutzrecht mit Datenethik, indem es rechtliche Pflichten und ethische Werte in technische und organisatorische Gestaltung übersetzt.
- Datenschutz wird wirksam, wenn Fairness, Transparenz und Fürsorge bereits im Systementwurf verankert sind – nicht erst in der Kontrolle.
- Eine verantwortungsvolle Datenverarbeitung braucht Governance-Strukturen, die Rechenschaft, Vertrauen und ethische Integrität institutionalisieren.

Dr. iur. Sandra Husi-Stämpfli, LL.M.,
ist Datenschutzberaterin des Eidgenössischen Justiz- und Polizeidepartements EJPD in Bern sowie Leiterin Stabsbereich Digital Compliance und Governance des Generalsekretariats EJPD. Der Beitrag gibt die persönliche Meinung der Autorin wieder.

31 Praxisorientierte Umsetzungsinstrumente sind zB Privacy Impact Assessments (PIA) oder Data Protection Impact Assessments (DPIA) nach Art. 35 DS-GVO. Sie ermöglichen, Risiken für Grundrechte frühzeitig zu erkennen und gezielte Schutzmaßnahmen zu definieren. Erweiterte Varianten, sog. Ethical Impact Assessments (EIA, dazu ausf. zB unter: https://www.unesco.org/ethics-ai/en/eia), betrachten zusätzlich gesellschaftliche und kulturelle Auswirkungen datenbasierter Systeme. Beide Instrumente fördern eine Haltung proaktiver Verantwortung: Die Frage lautet nicht mehr, ob eine Anwendung rechtmäßig ist, sondern wie sie verantwortungsvoll gestaltet werden kann.

32 ISO/IEC 42001 Information Technology – Artificial intelligence – Management system, dort S. vi.

TOBIAS REKEL

KI-Einsatz bei präventiv-polizeilicher Videobeobachtung im öffentlichen Raum

Eine praxisorientierte Begutachtung zur Umsetzbarkeit am Beispiel NRW

Datenverarbeitung
Verhaltensdetektion
Compliance
Datenanalyse

■ In Nordrhein-Westfalen (NRW) erlaubt § 15a Polizeigesetz NRW (PolG NRW) die präventiv-polizeiliche Videobeobachtung an Kriminalitätsbrennpunkten. Der Beitrag prüft die Rechtmäßigkeit solcher KI-Systeme im Zusammenspiel der RL (EU) 2016/680 (JI-RL) und der zugehörigen Umsetzung im nationalen Recht, der KI-VO, § 15a PolG NRW sowie einschlägiger Grundsatzentscheidungen des BVerfG und konkretisiert die technischen und organisatorischen Anforderungen, insbesondere in Bezug auf die menschliche Aufsicht, erforderliche Kontrollmechanismen und Dokumentationserfordernisse. NRW dient als Fallstudie der automatisierten Datenanalyse, die bundesweit relevant ist.

■ In North Rhine-Westphalia (NRW), Sec. 15a of the NRW Police Act (PolG NRW) permits preventive police video surveillance at crime hotspots. This article examines the legality of such AI systems within the legal framework of Directive (EU) 2016/680 and its implementation in national law, the German AI Regulation (AI-Act), Sec. 15a of the NRW Police Act and relevant landmark decisions of the German Federal Constitutional Court (BVerfG), and specifies the technical and organisational requirements, in particular with regard to human supervision, necessary control mechanisms and documentation requirements. North Rhine-Westphalia serves as a case study of automated data analysis which is relevant nationwide.
Lesedauer: 19 Minuten

I. Einleitung

Die präventiv-polizeiliche Videobeobachtung ist fester Bestandteil einiger Innenstädte in NRW. Die Prävention und insbesondere die Bekämpfung der Gewaltkriminalität im öffentlichen Raum ist ein Dauerthema der Landesinnenpolitik.[1] Mit dem Fortschritt KI-gestützter Verhaltensdetektion entsteht die Idee, verdächtige Verhaltensmuster (Schlag- und Trittmuster) automatisiert erkennen und auf dieser Grundlage eine polizeiliche Intervention auslösen zu lassen. Technisch ist ein solcher Einsatz bereits umsetzbar und keine hypothetische Konstellation mehr.[2] Dies wird mitunter auch am Beispiel des Landes Baden-Württemberg deutlich, das bereits seit 2023 ein entsprechendes KI-System im öffentlichen Raum einsetzt.[3]

Aktuelle KI-Systeme verfolgen regelmäßig den Ansatz eines digitalen Skeletts. Hierbei werden die Positionen und Bewegungen der erfassten Körper extrahiert und durch das KI-System in Form eines digitalen Skeletts analysiert. Bei besonders auffälligen oder verdächtigen Verhaltensweisen erfolgt eine Detektion.[4]

Dieser Beitrag klärt die Leitfrage, welche Voraussetzungen für den Einsatz eines derartigen KI-Systems im Allgemeinen gelten und ob eine rechtssichere Umsetzung in NRW möglich ist. Das Landesrecht NRW (§ 15a PolG NRW) dient dabei als normativer Anknüpfungspunkt zur Beurteilung der Zulässigkeit. Die relevanten Prüfungsmaßstäbe folgen jedoch primär aus dem Unionsrecht sowie den verfassungsrechtlichen Anforderungen und sind daher nicht auf NRW beschränkt. Betrachtet wird ein Use-Case, in dem das KI-System ein überlagerndes digitales Skelett bildet und keine darüber hinausgehenden personenbezogenen Daten auswertet. Im Fall der Detektion eines verdächtigen Verhaltens soll dem videobeobachtenden Polizeibeamten die Videosequenz dann dargestellt und eine Entscheidung (verdächtig/unverdächtig) herbeigeführt werden.

Die Diskussion um den Einsatz moderner Technologien bei Strafverfolgungsbehörden ist im Allgemeinen nicht auf die Videobeobachtung beschränkt.[5] Kontrovers diskutiert werden insbesondere die automatisierte Auswertung und Zusammenführung großer Datenmengen (Palantir) sowie die automatisierte Bild- und Videoauswertung bis hin zur Gesichtserkennung im öffentlichen Raum. Der Einsatz von KI vermag die Diskussion weiter zu verschärfen und auf eine neue Ebene zu heben. Dies eben auch vor dem Hintergrund der umfassenden Leistungsfähigkeit: Nicht nur große Datenbestände oder Identitätsmerkmale, sondern auch alltägliche Bewegungs- und Interaktionsmuster können potenziell in Echtzeit automatisiert ausgewertet werden. Dem Schutz betroffener Grundrechte sowie der rechtssicheren Umsetzung kommen in diesem sensiblen Kontext besondere Bedeutung zu.

II. Zusätzlicher Eingriff: Datenerhebung und automatisierte Auswertung

Das BVerfG entschied zuletzt iRd Hessendata-Urteils, dass die Verarbeitung gespeicherter personenbezogener Daten mittels automatisierter Analyse einen Eingriff in die informationelle Selbstbestimmung darstellt.[6] Die Schwere des Eingriffs hängt einerseits von der Intensität der ursprünglichen Datenerhebung ab und wird andererseits durch die automatisierte Verarbeitung noch weiter verstärkt, da diese aufgrund spezifischer Wirkungsweisen über das Gewicht der ursprünglichen Erhebung hinausgehen kann.[7] Demnach bilden sowohl die Datenerhebung als auch die automatisierte Auswertung (mittels KI-System) je eigenständige rechtfertigungsbedürftige Eingriffe ab.[8] Hierbei dürfte die automatisierte Auswertung schwerer wiegen.[9]

Das konkrete Eingriffsgewicht der automatisierten Auswertung ergibt sich aus Art und Umfang der Daten sowie der gewählten Analysemethode. Hierbei ist insbesondere der Umstand zu beachten, dass ein KI-System Daten in einem Umfang verarbeiten kann, die eine konventionelle Auswertung (ausschließlich menschliche Videobeobachtung) gar nicht erreichen kann.[10] Dies meint die vollumfängliche und durchgehende Auswertung jeglichen registrierten Verhaltens; eben auch insoweit unverdächtiger Personen.[11]

Um personenbezogene Daten dürfte es sich iÜ selbst bei anonymisierten digitalen Skeletten noch handeln, soweit die Rückführbarkeit auf konkrete Personen möglich bleibt. Das Kriterium der personenbezogenen Daten bezieht sich nicht nur auf bestimmte, sondern eben auch bestimmbare Personen.[12] Bestimmbar ist die Person dann, wenn zusätzliche Informationen oder Verarbeitungsschritte die Zuordnung ermöglichen können.[13] Aufgrund der (zumindest kurzfristigen) Speicherung der ursprünglichen Videoaufzeichnungen (Rohaufnahmen) dürfte dies regelmäßig gegeben sein.[14] Die Videoaufzeichnungen sind zusätzliche Informationen in diesem Sinne. Die Re-Identifizierung bleibt über den konkreten Zeitpunkt sowie Ort und auch individuelle Bewegungsmuster (hier insbesondere auch körperliche Einschränkungen und Behinderungen) möglich. Im Ergebnis mindert die Verarbeitung der skelettiert dargestellten Bewegungsdaten zwar die Eingriffstiefe, lässt sie aber nicht entfallen.[15] Des Weiteren dürfte sich ein entsprechendes Eingriffsgewicht schon in der reellen Möglichkeit niederschlagen, persönliche Nachteile in Form einer Polizeikontrolle zu erfahren.

Nach Ansicht des BVerfG kann das Eingriffsgewicht der automatisierten Datenauswertung durch den Gesetzgeber mithilfe klarer Regeln zur Art und Menge der zu verarbeitenden Daten und zur Art der Analysedaten reduziert werden. Die Gesetzgeber sind adressiert, normenklare Regelungen zu treffen und wesentliche Begrenzungen der vielseitigen Big-Data-Technologien vorzunehmen.[16]

III. Allgemeine Regelungen der Datenverarbeitung

Die JI-RL[17] regelt die Verarbeitung personenbezogener Daten durch Polizei und Justiz zur Aufgabenerfüllung und ist in NRW

---

1 Vgl. exemplarisch LT-Vorl. 18/2925, 1 ff. (Maßnahmenkonzept gegen Messergewalt im öffentlichen Raum).
2 Vgl. Lang Kriminalistik 2023, 124; vgl. zum aktuellen Stand der Technik im Allgemeinen Pohlmann DuD 2025, 5.
3 Vgl. https://www.landtag-bw.de/de/aktuelles/pressemitteilungen/innenausschuss-befasst-sich-mit-erkenntnissen-aus-projekt-intelligente-videoueberwachung-in-mannheim--419604.
4 Zu Möglichkeiten und Grenzen der Technologie s. https://www.iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoueberwachung.html.
5 Vgl. exemplarisch LT-Vorl. 18/4645.
6 BVerfG ZD 2023, 338 Rn. 50 mAnm Petri; Bäuerle ZD 2025, 128.
7 BVerfGE 165, 363 Rn. 54, 66 f. = ZD 2023, 338 (gekürzt) mAnm Petri.
8 BVerfGE 165, 363 Rn. 51 = ZD 2023, 338 (gekürzt) mAnm Petri.
9 Vgl. Möstl/Bäuerle, BeckOK Polizei- und Ordnungsrecht Hessen/Bäuerle, 27. Ed. 2022, HSOG § 25a Rn. 21; vgl. Benamor BayBVl 2025, 44 (46 f.).
10 BVerfGE 165, 363 Rn. 78 = ZD 2023, 338 (gekürzt) mAnm Petri.
11 Vgl. Benamor BayBVl 2025, 44 (45).
12 Vgl. BeckOK DatenschutzR/Schild, 44. Ed. 2023, DS-GVO Art. 4 Rn. 15 f.
13 Schaffland/Wiltfang, DSGVO/BDSG/Schaffland/Holthaus, 11. Aufl. 2025, EUV 2016/679 Art. 4 Rn. 43a; vgl. EuGH ZD 2017, 24 mAnm Kühling/Klar; zusammenfassend vgl. Schröder ZD 2021, 303 mwN.
14 Vgl. exemplarisch § 15a Abs. 2 PolG NRW, der eine Speicherdauer von bis zu 14 Tagen zulässt; ähnliche Regelungen finden sich in weiteren Landespolizeigesetzen.
15 BVerfGE 165, 363 Rn. 50, 76 ff. = ZD 2023, 338 (gekürzt) mAnm Petri.
16 BVerfGE 165, 363 Rn. 104, 110 = ZD 2023, 338 (gekürzt) mAnm Petri; Benamor BayVBl 2025, 44 (46).
17 RL (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119, 89.

durch das Landesdatenschutzgesetz (DSG NRW) umgesetzt worden.[18] § 37 DSG NRW enthält die Grundsätze der Datenverarbeitung (insbesondere Zweckbindung, Datenminimierung und Datensicherheit).[19] Für das in Rede stehende KI-System ergibt sich daraus im Kern Folgendes: Die automatisierte Verarbeitung personenbezogener Daten ist strikt an dem Zweckbindungsgrundsatz auszurichten und darf grundsätzlich nur zur Kriminalprävention (Gefahrenabwehr) eingesetzt werden. Umfang und Detaillierungsgrad der Daten sind im Licht des Grundsatzes der Datenminimierung kritisch zu betrachten und auf das erforderliche Maß zu beschränken. Zur Gewährleistung der Funktionstüchtigkeit genügen Körperbewegungsdaten (sog. Pose-Tracking-Daten in Form digitaler Skelette).

Für die erforderliche Vertraulichkeit und Informationssicherheit sind geeignete technische und organisatorische Maßnahmen (TOMs) vorzusehen, insbesondere der Einsatz von Verschlüsselungstechniken für Speicher- und Übertragungsmedien sowie ein differenziertes Rollen- und Berechtigungskonzept und nachvollziehbare Zugriffs- und Veränderungsdokumentationen.

§ 46 DSG NRW enthält für das in Rede stehende KI-System zentrale Vorgaben zur Zuweisung von Entscheidungskompetenzen.[20] Nach § 46 Abs. 1 DSG NRW ist es untersagt, Entscheidungen, die für die betroffene Person eine nachteilige Rechtsfolge entfalten können, ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten zu stützen.[21] Von dem Verbot erfasst wäre damit insbesondere das Szenario, in dem ein KI-System ein verdächtiges Verhalten detektiert und ohne menschliche Kontrolle eigenständig den Anstoß für zielgerichtete polizeiliche Maßnahmen gibt. Verbotsausnahmen ergeben sich gem. § 46 Abs. 1 DSG NRW nur, wenn diese Praktik durch eine Rechtsvorschrift zugelassen wird.[22] Ein KI-System mit eigenständiger, abschließender Entscheidungskompetenz ist daher grundsätzlich unzulässig.

Hiervon ist der betrachtete Use-Case abzugrenzen: Das KI-System soll lediglich als unterstützende Detektionshilfe eingesetzt werden. Entscheidungsrelevant ist somit nicht der System-Output (Detektion des KI-Systems), sondern die darauffolgende Beurteilung des Polizeibeamten. Damit dürfte der Verbotstatbestand aus § 46 Abs. 1 DSG NRW nicht erfüllt sein.[23]

Es handelt sich damit um ein Assistenzsystem, das die Daten aufbereitet, strukturiert und den Polizeibeamten iRd Videobeobachtung unterstützt.[24]

IV. Spezifische Regelungen der KI-VO

Die KI-VO[25] verfolgt analog der DS-GVO einen risikobasierten Ansatz und unterteilt KI-Systeme in verschiedene Risikokategorien: inakzeptables Risiko (verbotenes KI-System), hohes Risiko, begrenztes Risiko und minimales Risiko.[26] In Abhängigkeit der Einordnung müssen unterschiedliche Anforderungen erfüllt werden. In Bezug auf die videobasierte Verhaltensdetektion sind insbesondere folgende Aspekte zu beachten.

1. Biometrische Fernidentifizierung

Die oft diskutierte Gesichtserkennung als biometrische Fernidentifizierung im öffentlichen Raum durch Strafverfolgungsbehörden mithilfe eines KI-Systems ist grundsätzlich verboten, Art. 5 Abs. 1 lit. h KI-VO. Einem derart ausgestalteten KI-System ist ein inakzeptables Risiko zu attribuieren.[27] Hiervon abweichende Ausnahmen kommen nur in besonderen Konstellationen in Betracht, etwa im Zusammenhang mit der Terrorabwehr, Art. 5 Abs. 1 lit. h KI-VO.[28] Eine Ausnahme liegt freilich nicht vor. Der Einsatz zu diesem Zweck im Kontext der präventiv-polizeilichen Videobeobachtung ist folglich unzulässig.

2. Einordnung als System mit hohem Risiko

Art. 5 Abs. 1 lit. d KI-VO verbietet die personenbezogene Risikobewertung.[29] Das umfasst die Risikobewertung hinsichtlich der Begehung von Straftaten allein auf Basis des Profiling oder der (ausschließlichen) Verarbeitung persönlicher Merkmale und Eigenschaften.[30] In Abgrenzung zum Use-Case liegt dies eben nicht vor. Zwar wird durch das KI-System iRd Verhaltensdetektion ein Risikowert (Schwellenwert) für die Begehung einer Straftat (zB verdächtige Schlagbewegungen, schnelles Aufeinander-zu-Bewegen) bestimmt, jedoch nicht auf Grundlage eines Profilingprozesses oder der Einbeziehung persönlicher Merkmale und Eigenschaften. Dies wäre gegeben, wenn zB personenbezogene kriminalpolizeiliche Erkenntnisse (Anzahl, Art und Ausgang vergangener Strafverfahren) oder auch persönliche Merkmale wie Geschlecht und Alter miteinbezogen würden. IRe situativen Verhaltensanalyse wird zwangsläufig auch eine individuelle Prognose erstellt. Eine Verarbeitung derartiger Informationen und Merkmale erfolgt indes nicht. Damit ist die Verbotsschwelle aus Art. 5 Abs. 1 lit. d KI-VO nicht überschritten.

Das KI-System unterliegt daher Art. 6 KI-VO iVm Anhang III Nr. 6 lit. d KI-VO.[31] Der Verordnungsgeber fasst hierunter eben solche Systeme, die durch Strafverfolgungsbehörden eingesetzt werden und eine Risikobewertung vornehmen, ohne diese auf einen Profilingprozess oder persönliche Merkmale zu stützen. Aus dieser Einordnung ergeben sich gem. Art. 8 Abs. 1 KI-VO umfangreiche Anforderungen an Anbieter und Betreiber (Polizei).[32]

3. Datenschutz und Compliance

a) Daten und Daten-Governance

Die zum Training oder zur Kalibrierung eines KI-Systems genutzten Daten müssen zweckrelevant, repräsentativ, möglichst fehlerfrei und vollständig sein,[33] Art. 10 Abs. 3 KI-VO. In Erwägungsgrund 67 S. 1 KI-VO schreibt der Verordnungsgeber zudem das Erfordernis hochwertiger Daten zu Trainingszwecken nieder, eben weil diese die spätere Leistung des KI-Systems im Wirkbetrieb maßgeblich beeinflussen können. Mittels qualitativ hochwertiger Daten kann nach Ansicht des Verordnungsgebers eine Diskriminierung verhindert werden.[34]

---

18 Zur JI-RL vgl. Golla KriPoZ 2019, 238; Weinhold/Johannes DVBl 2016, 1501.
19 HK-LDSG NRW/Paul/Weinhold, 2020, DSG NRW § 37 Rn. 12 ff.
20 Vgl. HK-LDSG NRW/Braun, 2020, DSG NRW § 46 Rn. 3.
21 Vgl. zum Recht auf menschliche Entscheidung Paal/Hüger MMR 2025, 540; HK-LDSG NRW/Braun, 2020, DSG NRW § 46 Rn. 17.
22 HK-LDSG NRW/Braun, 2020, DSG NRW § 46 Rn. 22.
23 Vgl. Paal/Hüger MMR 2025, 540 (541 f.).
24 Vgl. Paal/Hüger MMR 2025, 540 (541 f.).
25 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz – KI-VO, ABl. L, 2024/206, 1).
26 Buchalik/Gehrmann CR 2024, 145 (147 f.); Bomhard/Merkle RDi 2021, 276.
27 Buchalik/Gehrmann CR 2024, 145 (148).
28 Zur Diskussion von sog. Hintertüren für Strafverfolgungsbehörden vgl. Linardatos GPR 2022, 58 (60) (62); Veale/Zuiderveen/Borgesuius CRi 2021, 97 (101).
29 Bomhard/Pieper/Wende, KI-VO, 2025, KI-VO Art. 5 Rn. 23 ff.
30 Vgl. Peffer, Schriftenreihe der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS) V/Schönrock, 2023, 65 (66).
31 Vgl. Marnau DuD 2025, 231 (232) (234); zur Systematik von Hochrisiko-Systemen vgl. Buchalik/Gehrmann CR 2024, 145 (148 f.).
32 Vgl. Buchalik/Gehrmann CR 2024, 145 (146 f.); vgl. zum Einsatz von Hochrisiko-KI-Systemen in der öffentlichen Verwaltung im Allgemeinen Guckelberger DÖV 2025, 45.
33 Vgl. zum sog. „Garbage in, Garbage out"-Paradigma Pohlmann DuD 2025, 5 (6); vgl. Gotthardt K&R 2025, 378 (380 f.).
34 Zur Kritik an der Tauglichkeit zur Vermeidung sämtlicher Diskriminierung vgl. Ory/Weth, jurisPK-ERV I/Biallaß, 3. Aufl., Rn. 266.

Die Verhinderung unberechtigter nachteiliger Rechtsfolgen für natürliche Personen dürfte ebenso Ziel der Vorschrift sein.

Bezogen auf den Use-Case scheinen insbesondere originale Videoaufzeichnungen, die mitunter auch Streitigkeiten oder Körperverletzungen zeigen, überaus repräsentativ. Art. 10 Abs. 4 KI-VO konkretisiert dies dahingehend, dass die Trainingsdaten dem bestimmungsgemäßen Rahmen des Wirkbetriebs entsprechen sollten. Das meint, es sollen eben auch Videoaufzeichnungen größerer Menschenmengen im öffentlichen Raum genutzt werden, um das KI-System auf den Wirkbetrieb vorzubereiten. Auf diese Weise werden spätere Verzerrungen (Bias),[35] dh Fehldetektionen, vermieden, Erwägungsgrund 67 S. 5, S. 6 KI-VO.

In Art. 10 Abs. 2 KI-VO werden Ansprüche an die den Trainingsdaten zugrunde liegenden Datenverwaltungsverfahren gestellt. Das Verfahren bezieht sich u.a. auf die ursprüngliche Erhebung und Menge der Trainingsdaten sowie das Erfordernis einer Untersuchung hinsichtlich möglicher Verzerrungen und zugehöriger Verhinderungsmaßnahmen.

b) Menschliche Aufsicht als Betreiberpflicht

Art. 26 Abs. 1 und Abs. 3 KI-VO verpflichtet den Betreiber (Polizei), geeignete TOMs zur Sicherstellung einer menschlichen Aufsicht zu treffen. Das hierfür eingesetzte Personal muss über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, Art. 26 Abs. 2 KI-VO. Über Ansprüche und Kontrolle in Bezug auf die Kompetenz entscheidet der Betreiber (Polizei).[36] Mit Kompetenz sind insbesondere die Fähigkeiten gemeint, den systemseitigen Output richtig interpretieren und eigenständig bewerten zu können.[37] Dies geht einher mit der Vermeidung von sog. Automationsbias, dh eine blinde Übernahme oder bloßes Abnicken der Systementscheidung.[38] Dies würde dazu führen, dass die folgerichtig eingeschränkte Entscheidungskompetenz des KI-Systems im Wirkbetrieb eine (unrechtmäßige) Erweiterung erfahren würde. Die menschliche Aufsicht muss die Detektionen kritisch hinterfragen und in jedem Fall eine Letztentscheidung treffen. Hierzu zählt eben auch das bewusste Verwerfen einer Detektion, wenn diese falsch erscheint.

Ferner muss die menschliche Aufsicht notfalls den Betrieb stoppen können, Art. 14 Abs. 1 KI-VO. Der Betrieb des KI-Systems sollte gestoppt werden, wenn das Grundrechtsrisiko zu groß wird, zB zur Vermeidung nachteiliger Grundrechtsfolgen in Folge wiederholter oder offensichtlicher Fehldetektionen.

Zur Ermöglichung der menschlichen Plausibilitätsprüfung muss das KI-System eine Mensch-Maschine-Schnittstelle bilden, Art. 13 Abs. 1 KI-VO. Dies meint eine Art Pop-up-Fenster oder zumindest eine Signalisierung. Zur Vorbereitung der menschlichen Prüfung kann die Einschätzung des KI-Systems im Schlagwortformat hinzugereicht werden („Streit", „Körperverletzung", „Rangelei" u.a.).

c) Grundrechte-Folgenabschätzung

Art. 27 Abs. 1 KI-VO verpflichtet die Polizei zur Durchführung einer Grundrechte-Folgenabschätzung (GRFA).[39] Diese Folgenabschätzung soll hierbei den zweckbestimmten Verfahrensablauf, den geplanten Nutzungszeitraum und die Nutzungsfrequenz umfassen, die betroffenen Personengruppen bestimmen sowie spezifische Grundrechtsrisiken und die Umsetzung der Maßnahme der menschlichen Aufsicht beschreiben.[40]

Verfahrensablauf und betroffene Personen

Die Darstellung des Verfahrensablaufs sollte die Örtlichkeit der Videobeobachtung, die Anzahl, Lage und auch Art der Kameras sowie Beschränkungen in zeitlicher oder örtlicher Hinsicht (Betriebszeiten und Einsatzraum) umfassen. Ferner muss der beabsichtigte Zweck dargeboten und der Ablauf im Wirkbetrieb in chronologischer Reihenfolge dargestellt werden: Die installierten Kameras erfassen das Videomaterial und übertragen es live. Es erfolgt eine ersetzende skelettierte Darstellung der Personen und eine darauf aufbauende Auswertung der Bewegungsabläufe. Im Falle einer positiven Detektion generiert das KI-System einen Alarm oder hebt die Szene anderweitig hervor. Allenfalls wird eine menschliche Plausibilitätsprüfung (Letztentscheidung) erforderlich. Erst nach Ablauf der Überprüfung werden polizeiliche Interventionsmaßnahmen veranlasst. In Betracht kommen insbesondere das Anhalten und Ansprechen der Person sowie regelmäßig die Identitätsfeststellung oder ein Hinweis auf normgerechtes Verhalten. Von der Datenverarbeitung sind alle natürlichen Personen im überwachten Bereich betroffen.

Risiken, Minderungsmaßnahmen und Abbruchkriterien

Risiken ergeben sich aufgrund systemseitiger Fehlfunktionen. Die Gründe hierfür sind mannigfaltig. Zu nennen sind insbesondere fehlerhafte oder nicht repräsentative Trainingsdaten bzw. eine fehlerhafte Analyse. Weitere Risiken ergeben sich insbesondere bei automatischer Übernahme des Detektionsergebnisses ohne (wirkliche) menschliche Plausibilitätsprüfung (Automationsbias).[41] Die Schulung der menschlichen Aufsicht kann die Risiken mindern. Eine weitere Minderungsmaßnahme ist eine wiederkehrende Schwellenwertkalibrierung des Systems. Diese kann periodisch (nach Ablauf eines Monats) oder nach einer bestimmten Anzahl von Detektionen (zB 1.000) erfolgen. Hierzu sind operative Zielwerte festzulegen, die Rückschlüsse auf die Genauigkeit des Systems zulassen. In Betracht käme das Verhältnis zwischen falsch-positiven und richtig-positiven oder auch zwischen falsch-positiven und der Gesamtzahl der Detektionen. Liefert das KI-System übermäßig viele falsch-positive Detektionen, ist das Grundrechterisiko erhöht.[42] Dies ist bereits in der Möglichkeit der Auslösung polizeilicher Interventionsmaßnahmen auf Basis einer fehlerhaften Detektion begründet. In diesem Zusammenhang sind feste Abbruchkriterien, die zumindest die vorübergehende Außerbetriebnahme sowie eine Kalibrierung des Systems erzwingen, festzulegen. Grundrechtsschützend ist außerdem die Option, infolge gravierender falschpositiver Detektionen (zB offensichtlich friedliche Personengruppe ohne jedwede Dynamik) den Betrieb abzubrechen. Eine geschulte menschliche Aufsicht ist demnach essenziell.

d) Datenschutz-Folgenabschätzung

Art. 26 Abs. 9 KI-VO verweist auf die aus Art. 27 JI-RL folgende und in § 56 DSG NRW umgesetzte Verpflichtung zur Vornahme einer Datenschutz-Folgenabschätzung (DSFA).[43] Sie ist dann vorzunehmen, wenn insbesondere der Einsatz neuer Technologien voraussichtlich ein hohes Risiko für die Rechte betroffener Personen darstellt, § 56 Abs. 1 DSG NRW. Weite Teile der Literatur und auch die LDI NRW nehmen im Kontext polizeilicher Videobeobachtung regelmäßig ein hohes Risiko an, woraus sich die Pflicht

35 Vgl. Pohlmann DuD 2025, 5 (6).
36 Vgl. Dubovitskaya AG 2024, 877 (882).
37 Vgl. Pohlmann DuD 2025, 5 (6).
38 Vgl. Paal/Hüger MMR 2025, 540 (541 f.); vgl. Dubovitskaya AG 2024, 877 (882).
39 Ory/Weth, jurisPK-ERV I/Biallaß, 3. Aufl., Rn. 259; zur Grundrechte-Folgenabschätzung im Zusammenhang mit KI im Allgemeinen vgl. Schürmann ZD 2022, 316.
40 S. hierzu auch Erwägungsgrund 34 KI-VO.
41 Vgl. Marnau DuD 2025, 231 (234).
42 European Union Agency for Fundamental Rights (FRA), Facial recognition technology, 2020, S. 8 f., 31 ff.
43 Zur DSFA im Zusammenhang mit KI vgl. Schäfer ZD 2025, 12.

zur Vornahme einer DSFA ergibt.[44] Die Verpflichtung dürfte auch auf den Einsatz eines unterstützenden KI-Systems zutreffen.

Die DSFA sollte insbesondere den Verarbeitungszweck und die Bewertung der Verhältnismäßigkeit angeben, die verfolgten Interessen darstellen und eine Risikobewertung vornehmen sowie ferner geplante Abhilfemaßnahmen und Sicherungsvorkehrungen ausweisen, § 56 Abs. 4 DS-GVO iVm Art. 35 Abs. 7 DS-GVO.[45] IRd Prüfung der Verhältnismäßigkeit dürfte der Prüfung und Abwägung milderer Maßnahmen besondere Bedeutung zuzumessen sein. Zu nennen sind exemplarisch eine größere polizeiliche Präsenz im öffentlichen Raum oder andere kriminalpräventive Maßnahmen.

e) Protokollierung, Aufbewahrung und Controlling

Aus Art. 26 KI-VO folgt die Verpflichtung des Betreibers (Polizei), die Logs für zumindest sechs Monate aufzubewahren. Logs entstehen u.a. bei Positiv-Detektion und umfassen Informationen wie Datum, Uhrzeit, Ort, Kamera, Systemversion, Schwellenwert, Name und die (kommentargestützte) Entscheidung der menschlichen Aufsicht (Bestätigung/Verwerfung). Diese Logs sind unentbehrlich, um eine Aufsicht durch externe Stellen (Datenschutzbeauftragte und Aufsichtsbehörden) zu ermöglichen[46] und den Auskunfts- und Überprüfungsrechten der betroffenen Person aus § 47 ff. DSG NRW zu entsprechen[47].

Zur Gewährleistung einer rechtmäßigen Datenverarbeitung sind die Logs in ein engmaschiges Controlling einzubinden. In diesem Rahmen sollten insbesondere die Anzahl der benannten Betriebskennzahlen, die Gesamtanzahl der Detektionen und die Gesamtkamerastunden dokumentiert und ausgewertet werden. Ein Tätigkeitsbericht sollte eine aktuelle Fehlerquote (Falsch-Positiv), auf Plausibilität geprüfte Positiv-Detektionen in absoluten Zahlen und veranlasste polizeiliche Interventionsmaßnahmen ausweisen. Das Controlling bedient zwei elementare Funktionen: Es dient der fortlaufenden Überprüfung der Rechtmäßigkeit und Wirksamkeit des KI-Systems und kann zugleich das Vertrauen der Gesellschaft in die moderne Technologie erhöhen.[48] Die Logs sind begrifflich von den Aufzeichnungen der Videobeobachtung zu trennen. Es gelten mitunter erheblich abweichende Aufbewahrungsfristen. So lässt der Landesgesetzgeber NRW iRd präventiv-polizeilichen Videobeobachtung eine maximale Speicherdauer von 14 Tagen zu, § 15a Abs. 2 PolG NRW. Ausnahmen hiervon ergeben sich nur iRe sich anschließenden Weiterverarbeitung zu anderen Zwecken.[49]

V. Ermächtigungsgrundlage im Polizeirecht

Aus Art. 6 KI-VO iVm Anhang III Nr. 6 lit. d KI-VO folgt das Erfordernis einer konkreten Ermächtigungsgrundlage nach nationalem Recht. Die Zuständigkeit für die Gefahrenabwehr ist den Ländern zugeschrieben. Dies führt zur Betrachtung der nationalen Regelungen im Polizeirecht. Am Beispiel von NRW soll eine entsprechende Regelung diskutiert werden.

§ 15a PolG NRW ermächtigt zur offenen Videobeobachtung eines öffentlichen Platzes in NRW vorrangig durch festinstallierte oder mobile Videokameras.[50] Der Einsatz der Beobachtungstechnik ist u.a. an Kriminalitätsbrennpunkten zulässig, § 15a Abs. 1 Nr. 1 PolG NRW. Die Videobeobachtung gem. § 15a PolG NRW verfolgt präventive Ziele[51] und setzt den technischen Einsatz unter die Voraussetzung einer (zeitnahen) polizeilichen Intervention.[52] Zu klären ist, ob eine automatisierte Auswertung in diesem Zusammenhang zugelassen ist. Auf Seiten der Rechtsfolge erlaubt § 15a PolG NRW zwar die Datenerhebung durch den Einsatz technisch-optischer Mittel, setzt aber zwingend eine menschliche Beobachtung bzw. Bewertung voraus.[53] Eine abschließende Bewertung auf Grundlage einer automatisierten Verarbeitung mit nachteiliger Rechtsfolge ist nicht zulässig.[54]

Die unveränderte äußere Form der Auswertungsmaßnahme bekräftigt die Annahme ebenfalls: Ein Mensch beobachtet das Videomaterial und nimmt eine abschließende Bewertung vor. Dem KI-System wird keine eigene Entscheidungskompetenz beigemessen. Die von der Entscheidungskompetenz losgelöst stattfindende automatisierte Datenauswertung durch das KI-System spricht gewichtig gegen diese Annahme. Nach Ansicht des BVerfG muss der Gesetzgeber die wesentlichen Begrenzungen von Art und Umfang der zu verarbeitenden Daten sowie die zugelassenen Auswertungsmethoden normenklar bestimmen. Nur dann kann eine automatisierte Datenanalyse gerechtfertigt werden. Fehlen derartige Maßgaben und Befugnisse, darf die automatisierte Auswertung nicht eingesetzt werden.[55] Weder der Verweis auf eine menschliche Letztentscheidung noch eine unveränderte äußere Form oder ein behördlicher Wille genügen. Eine demnach erforderliche Regelung findet sich in § 15a PolG NRW nicht.

Der Landesgesetzgeber hat folglich den Grundrahmen für Art und Umfang der automatisierten Datenauswertung festzulegen und eine entsprechende Novellierung vorzunehmen (vgl. nachstehenden Novellierungsvorschlag).

VI. Ergebnis

Im Ergebnis bewirkt der Einsatz eines KI-Systems zur videobasierten Verhaltensdetektion im öffentlichen Raum einen doppelten Grundrechtseingriff in Form der Datenerhebung und der automatisierten Analyse. Dieser Einsatz ist iRd JI-RL und der Transformationsnormen im nationalen Recht (DSG NRW) sowie der KI-VO einzuordnen. Gemäß dem risikobasierten Ansatz der KI-VO ist dem in Rede stehenden KI-System ein hohes Risiko beizumessen, woraus wiederum strenge Anforderungen an die Auswahl der Trainingsdaten sowie den Wirkbetrieb in Form der fortlaufenden menschlichen Aufsicht oder auch der Aufbewahrung und Protokollierung von Detektionen folgen. Außerdem ist das System ausschließlich mit einer Grundrechte- und Datenschutz-Folgenabschätzung zu betreiben. Zusammengefasst ist das KI-System grundsätzlich zulässig, insofern eine biometrische Fernidentifizierung vermieden und dem KI-System keine abschließende Entscheidungskompetenz beigemessen wird. Zudem bedarf es einer expliziten Regelung im Polizeirecht des Landes. An dieser fehlt es aktuell in NRW, weswegen eine rechtssichere Implementierung der modernen Technologie (noch) nicht möglich scheint.

VII. Ausblick

Bezogen auf NRW bleibt eine Novellierung des § 15a PolG NRW abzuwarten. Ein Vorbild hierfür können die infolge des Hessen-data-Urteils geschaffenen Ermächtigungen anderer Landesgesetzgeber sein.[56]

---

44 Wysk VerwArch 2018, 109 (141) (159); HK-LDSG NRW/Franck, 2020, DSG NRW § 56 Rn. 15 ff., 18.
45 Vgl. HK-LDSG NRW/Franck, 2020, DSG NRW § 56 Rn. 25 ff.; zu den (inhaltlichen) Anforderungen s. Kühling/Buchner, DS-GVO BDSG/Jandt, 4. Aufl. 2024, DS-GVO Art. 35 Rn. 31–51.
46 Vgl. zu der Aufsichtsfunktion des LDI NRW im Zusammenhang HK-LDSG NRW/Pabst, 2020, DSG NRW § 60 Rn. 4 ff.
47 Vgl. HK-LDSG NRW/Franck, 2020, DSG NRW § 49 Rn. 16 ff., 40 ff.
48 Vgl. Lang Kriminalistik 2023, 124 (126 f.).
49 Zum Begriff der hypothetischen Datenneuerhebung BVerfG ZD 2016, 374 mAnm Petri; zur Umsetzung in NRW vgl. BeckOK PolR NRW/Arzt, 32. Ed. 2025, PolG NRW § 23 Rn. 25 ff.
50 Tegtmeyer/Vahle, PolG NRW, 13. Aufl. 2022, PolG NRW § 15a Rn. 1, 4.
51 Vgl. BVerwG ZD 2012, 438.
52 LT-Drs. 17/2351, 36; LT-Drs. 17/3865, 10.
53 Tegtmeyer/Vahle, PolG NRW, 13. Aufl. 2022, PolG NRW § 15a Rn. 4.
54 Ohnehin durch § 46 Abs. 1 DSG NRW grundsätzlich verboten.
55 BVerfG ZD 2023, 338 Rn. 50 mAnm Petri.
56 Vgl. § 44 Abs. 4 PolG Baden-Württemberg.

§ 15a Abs. 5 PolG NRW (Formulierungsvorschlag):

Die Polizei kann die nach Absatz 1 angefertigten Bildaufzeichnungen automatisiert auswerten, wenn die automatisierte Auswertung ausschließlich auf das Erkennen solcher Verhaltensmuster ausgerichtet ist, die auf die Begehung einer Straftat hindeuten und eine menschliche Letztentscheidung erfolgt. Besondere Kategorien personenbezogener Daten nach § 22a PolG NRW dürfen nicht verarbeitet werden.

Tobias Rekel
ist Polizeioberkommissar in NRW und zugleich nebenamtlicher Dozent an der Hochschule für Polizei und Öffentliche Verwaltung NRW.

Schnell gelesen ...

- Eine KI-gestützte Verhaltensdetektion iRd präventivpolizeilichen Videobeobachtung begründet einen eigenständigen, gewichtigen Eingriff neben der Datenerhebung. Auch digitale Skelette bleiben personenbezogene Daten.
- Das betrachtete System ist als Hochrisiko-KI-System einzuordnen und nur unter den Voraussetzungen der menschlichen Letztentscheidung zulässig.
- KI-VO und DSG NRW stellen hohe Ansprüche an Trainingsdaten, Daten-Governance und die menschliche Aufsicht.
- Vor Inbetriebnahme sind eine Grundrechte- und Datenschutz-Folgenabschätzung anzufertigen.
- § 15a PolG NRW ermächtigt bisher nicht zur automatisierten Datenauswertung. Nach dem Urteil des BVerfG muss die Technik expressis verbis zugelassen sein.

RECHTSPRECHUNG

EuGH: Bodycam-Aufnahmen durch Fahrkartenkontrolleure

DS-GVO Art. 13, 14
Urteil vom 18.12.2025 – C-422/24

Leitsatz der Redaktion

Die Art. 13 und 14 DS-GVO sind dahin auszulegen, dass in einer Situation, in der personenbezogene Daten mittels von Fahrkartenkontrolleuren im öffentlichen Personenverkehr getragenen Körperkameras erhoben werden, die Unterrichtung der betroffenen Personen durch Art. 13 DS-GVO geregelt wird und nicht durch Art. 14 DS-GVO.

Anm. d. Red.: Der Volltext ist abrufbar unter BeckRS 2025, 34965. Vgl. hierzu auch EuGH ZD 2015, 77 mAnm Lachenmann – Ryneš; EuGH ZD 2025, 388; EuGH MMR 2025, 353; EuGH ZD 2024, 510 mAnm Hense; EuGH ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz – Dun & Bradstreet Austria und Jaksch/Hoffmann ZD 2022, 605.

Sachverhalt

SL erbringt öffentliche Personenverkehrsdienste in Stockholm (Schweden). Das Unternehmen hat seine Fahrkartenkontrolleure mit Körperkameras ausgestattet, die eingesetzt werden, um Fahrgäste zu filmen, die bei der Fahrkartenkontrolle über keinen gültigen Fahrschein verfügen und denen mithin eine Strafgebühr auferlegt wird. Der Einsatz dieser Kameras hat die Verhinderung und Dokumentation von Drohungen und Gewalt gegen die Kontrolleure sowie die Feststellung der Identität von Fahrgästen, die eine Strafgebühr zahlen müssen, zum Ziel.

Körperkamera
Personenbezogene Daten
Unmittelbare Datenerhebung
Hinweisschild
Öffentlicher Personenverkehr

Im Rahmen ihrer Aufsichtstätigkeit überprüfte die Datenschutzaufsichtsbehörde (nachfolgend: Behörde), ob die von SL mit den Körperkameras vorgenommene Verarbeitung personenbezogener Daten in Übereinstimmung mit den Vorschriften der DS-GVO erfolgte. Im Juni 2021 erließ die Behörde eine Entscheidung, aus der hervorgeht, dass die Kontrolleure diese Kameras während ihrer gesamten Schicht tragen und dass die Kameras durchgehend Filme mit Bild und Ton aufnehmen. Die Kameras verfügen über einen sog. Ringspeicher, was bedeutet, dass automatisch nach einer bestimmten Zeit das gesamte Aufnahmematerial entfernt wird. Nach der Entfernung wird das aufgezeichnete Material gelöscht. Die Fahrkartenkontrolleure können per Knopfdruck die automatische Entfernung abbrechen und so sicherstellen, dass die Aufzeichnung nicht gelöscht wird. In diesem Fall werden auch die in der Kamera gespeicherten Information mittels der Voraufzeichnungstechnik gespeichert, mit der Informationen während der dem Knopfdruck durch den Kontrolleur vorausgehenden Minute aufgezeichnet werden. Die Fahrkartenkontrolleure sind angewiesen, in allen Situationen, in denen eine Strafgebühr erhoben wird, sowie überdies in Bedrohungssituationen die automatische Entfernung zu unterbrechen.

Über diese den Einsatz und die Funktion der Körperkameras betreffenden Feststellungen führte die Behörde in ihrer Entscheidung aus, dass SL von Dezember 2018 bis zum Zeitpunkt der Entscheidung der Behörde im Juni 2021 mit dem Einsatz der Körperkameras iRd Fahrkartenkontrollen unter Verstoß gegen mehrere Bestimmungen der DS-GVO personenbezogene Daten verarbeitet habe. SL habe es unter Missachtung von Art. 13 DS-GVO versäumt, die betroffenen Personen hinreichend zu informieren. Deshalb verhängte die Behörde gegen SL eine Geldbuße von insgesamt 16 Mio. schwedischen Kronen (SEK) (rd. 1.420.670 EUR), wobei 4 Mio. SEK (etwa 355.188 EUR) die mangelnde Unterrichtung der betroffenen Personen betrafen. Der von SL mit einer Klage gegen die Entscheidung der Behörde befasste Förvaltningsrätt i Stockholm (Verwaltungsgericht Stockholm, Schweden) wies diese Klage ab, soweit sie die wegen mangelnder Unterrichtung der betroffenen Personen gegen dieses Unternehmen verhängte Geldbuße betraf.

Daraufhin legte SL Rechtsmittel beim Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm, Schweden) ein, der sowohl das erstinstanzliche Urteil als auch die Entscheidung der Behörde aufhob, soweit dies die Verhängung der Geldbuße betraf. Unter Bezugnahme auf das Urteil des Gerichtshofs v. 11.12.

2014 – C-212/13 [= ZD 2015, 77 mAnm Lachenmann] – Ryneš, entschied dieses Gericht, dass Art. 13 DS-GVO auf den bei ihm anhängigen Rechtsstreit nicht anwendbar sei und daher die Behörde zu Unrecht gegen SL eine Geldbuße wegen Verstoßes gegen diese Vorschrift verhängt habe. Die Behörde legte gegen das Urteil des Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm) Rechtsmittel beim Högsta förvaltningsdomstol (Oberstes Verwaltungsgericht, Schweden), dem vorlegenden Gericht, ein und beantragte, dieses Urteil aufzuheben, soweit es die wegen mangelnder Unterrichtung der betroffenen Personen gegen SL verhängte Geldbuße betrifft.

Das vorlegende Gericht stellt zunächst klar, dass sich die Frage stelle, ob Art. 13 DS-GVO oder Art. 14 DS-GVO anwendbar sei, wenn personenbezogene Daten mittels einer Körperkamera erhoben würden. Die Antwort hierauf sei in zweierlei Hinsicht erforderlich. Zum einen müsse bestimmt werden, welche Informationen der betroffenen Person bereitzustellen seien, zu welchem Zeitpunkt dies zu geschehen habe und welche Ausnahmen von der Informationspflicht bestünden. Zum anderen müsse festgestellt werden, ob die Behörde berechtigt gewesen sei, gegen SL eine Geldbuße wegen Verstoßes gegen die Informationspflicht aus Art. 13 DS-GVO zu verhängen.

Aus den Gründen

27 Mit seiner Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob die Art. 13 und 14 DS-GVO dahin auszulegen sind, dass in einer Situation, in der personenbezogene Daten mittels von Fahrkartenkontrolleuren im öffentlichen Nahverkehr getragenen Körperkameras erhoben werden, die Unterrichtung der betroffenen Personen durch Art. 13 DS-GVO oder Art. 14 DS-GVO geregelt wird.

28 Für die Beantwortung dieser Frage sind gemäß stRspr des Gerichtshofs nicht nur der Wortlaut dieser Bestimmungen, sondern auch ihr Kontext und die Ziele zu berücksichtigen, die mit der Regelung, zu der sie gehören, verfolgt werden (Urt. v. 28.11. 2024 – C-169/23 [= ZD 2025, 388] Rn. 39 – Másdi).

29 Erstens ist in Bezug auf den Wortlaut der Art. 13 und 14 DS-GVO darauf hinzuweisen, dass der sachliche Anwendungsbereich von Art. 14 DS-GVO im Verhältnis zu dem von Art. 13 DS-GVO negativ definiert wird. Wie sich bereits aus den Überschriften dieser Bestimmungen ergibt, geht es in Art. 13 DS-GVO um die zur Verfügung zu stellenden Informationen in Fällen, in denen personenbezogene Daten bei der betroffenen Person erhoben werden, während Art. 14 DS-GVO diejenigen Informationen betrifft, die zur Verfügung zu stellen sind, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Urt. v. 28.11.2024 – C-169/23 [= ZD 2025, 388] Rn. 48 – Másdi).

30 Zur Unterscheidung der jeweiligen Anwendungsbereiche dieser Bestimmungen ist der Umstand, dass in verschiedenen Sprachfassungen von Art. 14 DS-GVO, namentlich in der schwedischen, der in Art. 13 dieser Verordnung verwendete Begriff „erhoben" („samlas in") nicht wieder aufgegriffen wird, nicht entscheidend.

31 Nach stRspr müssen nämlich die Bestimmungen des Unionsrechts im Licht der Fassungen in allen Sprachen der EU einheitlich ausgelegt und angewandt werden; weichen diese verschiedenen Fassungen voneinander ab, muss die fragliche Bestimmung nach der allgemeinen Systematik und dem Zweck der Regelung ausgelegt werden, zu der sie gehört (Urt. v. 13.2.2025 – C-612/23 [= MMR 2025, 353] Rn. 31 – Verbraucherzentrale Berlin (Begriff der anfänglichen Mindestvertragslaufzeit) – und die dort angeführte Rspr.).

32 Insoweit hat der Gerichtshof in Bezug auf den Gebrauch des Begriffs „Erlangung" („erhällande") in Art. 14 Abs. 5 lit. c DS-GVO, der in der schwedischen Sprachfassung auch in der Überschrift von Art. 14 DS-GVO sowie in Art. 14 Abs. 1 („erhällits") gebraucht wird, bereits klargestellt, dass dieser Begriff tatsächlich die bei einer anderen als der betroffenen Person „erhobenen" Daten sowie diejenigen Daten betrifft, die der Verantwortliche selbst iRd Erfüllung seiner Aufgabe aus solchen Daten erzeugt hat (vgl. idS Urt. v. 28.11.2024 – C-169/23 [= ZD 2025, 388] Rn. 47 – Másdi).

33 Außerdem verlangt, wie von der GAin in Nr. 28 ihrer SA ausgeführt, der Begriff der bei einer iSv Art. 13 Abs. 1 DS-GVO betroffenen Person „erhobenen" Daten keine besondere Handlung seitens der betroffenen Person, sondern nur eine Handlung des Verantwortlichen, sodass es für die Abgrenzung des Anwendungsbereichs dieser Bestimmung ggü. demjenigen von Art. 14 der Verordnung keine Rolle spielt, in welchem Maße die betroffene Person jeweils aktiv wird.

34 Hervorgehoben wird diese Erwägung auch in ... Transparenzleitlinien, denen zu entnehmen ist, dass Art. 13 DS-GVO Anwendung findet, wenn entweder die betroffene Person dem Verantwortlichen wissentlich personenbezogene Daten zur Verfügung stellt, oder wenn der Verantwortliche die Daten bei dieser Person im Wege der Beobachtung, u.a. mit Kameras, erhebt.

35 Im Anbetracht des Wortlauts von Art. 14 Abs. 2 lit. f DS-GVO ist iVm dem 61. Erwägungsgrund dieser Verordnung davon auszugehen, dass das einzig relevante Kriterium für die Abgrenzung des jeweiligen Anwendungsbereichs von Art. 13 und 14 DS-GVO in der Quelle der erhobenen personenbezogenen Daten liegt. Nach dem Wortlaut von Art. 14 Abs. 2 lit. f DS-GVO muss nämlich der Verantwortliche, wenn die Daten nicht bei der betroffenen Person erhoben wurden, der betroffenen Person mitteilen, aus welcher Quelle die personenbezogenen Daten stammen.

36 Folglich spricht die am Wortlaut der Art. 13 und 14 DS-GVO iVm dem 61. Erwägungsgrund dieser Verordnung orientierte Auslegung dafür, auf die Erhebung personenbezogener Daten mittels einer Körperkamera Art. 13 DS-GVO anzuwenden, da die Daten bei dieser Fallgestaltung nicht von einer anderen Quelle als der betroffenen Person, sondern unmittelbar von dieser selbst erlangt werden.

37 Zweitens wird eine solche Auslegung durch den Kontext bestätigt, in den sich diese Bestimmungen einfügen.

38 Insoweit ergibt sich aus Art. 5 DS-GVO, dass die Verarbeitung personenbezogener Daten in Bezug auf die von einer solchen Verarbeitung betroffenen Person u.a. konkreten Anforderungen an die Transparenz genügen muss (Urt. v. 11.7.2024 – C-757/22 [= ZD 2024, 510 mAnm Hense] Rn. 53 – Meta Platforms Ireland (Verbandsklage)).

39 Wie von der Kommission in ihren schriftlichen Erklärungen im Wesentlichen ausgeführt, verleiht Art. 13 DS-GVO, indem er vorschreibt, dass der betroffenen Person die in dieser Vorschrift genannten Informationen zum Zeitpunkt der Erhebung mitzuteilen sind, dem Recht dieser Person, unterrichtet zu werden, besonderen Ausdruck. Dagegen wurde Art. 14 DS-GVO erlassen, um auf diejenigen Situationen einzugehen, in denen der Verantwortliche keinen direkten Kontakt zur betroffenen Person hat, sondern die personenbezogenen Daten aus einer anderen Quelle erhebt, sodass die Mitteilung der Informationen im Sinne dieser Bestimmung zum Zeitpunkt ihrer Erlangung in der Praxis erschwert oder gar unmöglich wird. Die Mittelbarkeit einer solchen Erhebung rechtfertigt es daher, dass Art. 14 DS-GVO die Möglichkeit vorsieht, dass der Verantwortliche der ihn treffenden Informationspflicht erst später nachkommt.

40 Drittens sind die Art. 13 und 14 DS-GVO im Licht des mit dieser Verordnung verfolgten Ziels auszulegen, das insb. darin be-

steht, ein hohes Niveau des Schutzes der Grundfreiheiten und der Grundrechte natürlicher Personen zu gewährleisten, und zwar insb. ihres in Art. 16 AEUV gewährleisteten Rechts auf Schutz der personenbezogenen Daten, das in Art. 8 GRCh als Grundrecht verankert ist und das in Art. 7 GRCh verankerte Recht auf ein Privatleben ergänzt (Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 51 – Dun & Bradstreet Austria u.a. und die dort angeführte Rspr.).

41 Ließe man zu, dass Art. 14 DS-GVO in dem Fall Anwendung findet, dass personenbezogene Daten mittels einer Körperkamera erhoben werden, würden die betroffenen Personen nicht zum Zeitpunkt der Datenerhebung unterrichtet, obwohl sie selbst die Datenquelle sind, wodurch es dem Verantwortlichen möglich wäre, von der sofortigen Unterrichtung der betroffenen Personen abzusehen. Somit entstünde bei einer solchen Auslegung die Gefahr, dass es zu einer von der betroffenen Person unbemerkten Datenerfassung und damit zu verdeckten Überwachungspraktiken kommen könnte. Eine solche Folge wäre unvereinbar mit dem in der vorstehenden Randnummer genannten Zweck, ein hohes Niveau des Schutzes der Grundfreiheiten und der Grundrechte natürlicher Personen zu gewährleisten.

42 Allerdings steht dieser Zweck dem nicht entgegen, dass die Informationspflichten nach Art. 13 DS-GVO, wie in den Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte des Europäischen Datenschutzausschusses (EDSA) v. 29.1.2020 vorgesehen, iRe gestuften Verfahrens erfüllt werden. Gemäß diesen Leitlinien können auf einer ersten Ebene die für die betroffene Person wichtigsten Informationen auf einem Hinweisschild angezeigt werden, und auf einer zweiten Ebene können die weiteren obligatorischen Informationen dieser Person in geeigneter und vollständiger Weise an einem leicht zugänglichen Ort zur Verfügung gestellt werden.

43 Was schließlich den vom Kammarrätt i Stockholm (Oberverwaltungsgericht Stockholm, Schweden) geäußerten Zweifel in Bezug auf die Reichweite von Rn. 34 des vorstehend in Rn. 13 erwähnten Urt. v. 11.12.2014 – C-212/13 [= ZD 2015, 77 mAnm Lachenmann] – Ryneš angeht, so hat sich der Gerichtshof in jener Rn. 34 nicht zum Anwendungsbereich von Art. 11 RL 95/46 – dem Art. 14 DS-GVO entspricht – im Verhältnis zu Art. 10 der o.g. RL – dem Art. 13 DS-GVO entspricht – geäußert, sondern lediglich veranschaulicht, dass aufgrund der verschiedenen in dieser Richtlinie vorgesehenen Beschränkungen und Ausnahmen bei ihrer Anwendung berechtigte Interessen des Verantwortlichen berücksichtigt werden können.

44 Folglich lässt sich aus Rn. 34 dieses Urteils nicht ableiten, dass der Gerichtshof sich bereits zur Unterscheidung der Anwendungsbereiche von Art. 13 und 14 DS-GVO geäußert hätte.

45 Nach alledem ist auf die Vorlagefrage zu antworten, dass die Art. 13 und 14 DS-GVO dahin auszulegen sind, dass in einer Situation, in der personenbezogene Daten mittels von Fahrkartenkontrolleuren im öffentlichen Personenverkehr getragenen Körperkameras erhoben werden, die Unterrichtung der betroffenen Personen durch Art. 13 DS-GVO geregelt wird und nicht durch Art. 14 DS-GVO. ...

Anmerkung

Julia Klaren, Wiss. Mitarb., Lehrstuhl Prof. Dr. Valta, Heinrich-Heine-Universität, Düsseldorf

Mit diesem Urteil schafft der EuGH Klarheit in der schon länger bestehenden Streitigkeit hinsichtlich der Frage, wie die Informationspflichten nach Art. 13 DS-GVO von denen des Art. 14 DS-GVO abzugrenzen seien bzw. in welchem systematischen Verhältnis die beiden Normen zueinander stehen. Dass diese Frage nicht rein akademischer Natur ist, ergibt sich aus dem Wortlaut der Norm selbst. Je nach Vorschrift sind unterschiedliche Informationen zu unterschiedlichen Zeitpunkten der von der Datenerhebung betroffenen Person mitzuteilen. Darüber hinaus bestehen unterschiedliche Ausnahmen von der Informationspflicht. In der deutschen Lit. herrscht(e) bisher eher der Standpunkt vor, dass ein Fall des Art. 13 DS-GVO vorliege, wenn es sich um eine „Erhebung personenbezogener Daten mit Kenntnis oder unter Mitwirkung der betroffenen Person" (Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 4) handelt (iÜ auch BeckOK DatenschutzR/Schmidt-Wudy, 54. Ed. 1.11.2025, DS-GVO Art. 13 Rn. 30; Ebner, Weniger ist Mehr?, S. 145, 249; Jaksch/Hoffmann ZD 2022, 605 (609); Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, DS-GVO Art. 13 Rn. 13; Spindler/Schuster/Kaesling/Nink, 5. Aufl. 2026, DS-GVO Art. 13 Rn. 1). Nur Wenige verzichteten auf entsprechende Kriterien (Kühling/Buchner/Bäcker, 4. Aufl. 2024, DS-GVO Art. 13 Rn. 13). Eine heimliche Videoüberwachung etwa sollte demnach gemäß der deutlich weiter verbreiteten Ansicht Art. 14 DS-GVO zugeordnet werden (Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 14 Rn. 2). Dem ist der EuGH berechtigterweise entgegengetreten.

1. Hintergrund

Hintergrund der Vorlagefrage war eine Rechtsstreitigkeit zwischen einem schwedischen Unternehmen, das öffentliche Personenverkehrsdienste in Stockholm erbringt, und der schwedischen Aufsichtsbehörde. Während der Fahrkartenkontrolle wurden Köperkameras eingesetzt. Damit sollten Personen, die nicht über ein entsprechendes Ticket verfügten, gefilmt werden, um Drohungen und Gewalt zu verhindern bzw. um die Identität der Personen zu dokumentieren. Die Behörde monierte mehrere Verstöße gegen die DS-GVO. Insb. seien die betroffenen Personen nicht iSd Art. 13 DS-GVO ausreichend informiert worden. Die Folge war die Verhängung eines Bußgelds. Nach nationaler Auseinandersetzung legte das Oberste Verwaltungsgericht die Frage vor, ob Art. 13 DS-GVO oder Art. 14 DS-GVO anwendbar sei, wenn personenbezogene Daten mit einer Körperkamera erhoben werden.

2. Entscheidung des EuGH

Bei Aufnahmen, die durch im öffentlichen Personenverkehr getragene Körperkameras erstellt wurden, ist die Informationspflicht nach Art. 13 DS-GVO einschlägig (Rn. 45). Die Erfüllung kann allerdings in einem gestuften Verfahren erfolgen, indem zunächst lediglich die wichtigsten Informationen auf einem Hinweisschild angezeigt werden. Auf einer zweiten Ebene müssen dann die weiteren obligatorischen Informationen der betroffenen Person „an einem leicht zugänglichen Ort zur Verfügung gestellt werden" (Rn. 42). Obwohl das Ergebnis folgerichtig ist, werden zahlreiche weitere Argumente für ebendiese Auslegung nicht aufgeführt.

a) Argumentation des EuGH

Zur Begründung des gefundenen Ergebnisses verweist der EuGH darauf, er habe bereits klargestellt, dass mit „Erlangung" iSd Art. 14 Abs. 5 lit. c DS-GVO „... die bei einer anderen als der betroffenen Person ‚erhobenen' Daten ..." gemeint sind (Rn. 32). Mittelbar wird weiter der Wortlaut herangezogen, indem hervorgehoben wird, dass Art. 13 DS-GVO eben keine Handlung der betroffenen Person voraussetze, sondern lediglich eine Handlung des Verantwortlichen (Rn. 33). Zusätzlich verweist der EuGH auf die Transparenzleitlinien (gem. VO (EU) 2016/679 v. 29.11.2017 – in ihrer von der nach Art. 29 RL 95/46/EG v. 24.10.1995 eingesetzten Arbeitsgruppe am 11.4.2018 überarbeiteten Fassung), die ebenfalls die Datenerhebung durch Beobachtung unter die Informationspflicht nach Art. 13 DS-GVO subsumieren (Rn. 34). Systematisch findet daneben eine Anknüpfung an Art. 14 Abs. 2 lit. f DS-GVO sowie an den

Erwägungsgrund 61 DS-GVO statt, wonach der Verantwortliche – sofern er die personenbezogenen Daten nicht von der betroffenen Person erlangt hat – die Quelle mitteilen muss (Rn. 35 ff.). Ferner wird der in Art. 5 Abs. 1 lit. a DS-GVO normierte Transparenzgrundsatz in die Argumentation einbezogen (Rn. 38). Daneben nimmt der EuGH dabei auf die tatsächlichen Umstände Bezug, die eine differenzierte Betrachtungsweise legitimieren: Wenn personenbezogene Daten nicht bei der betroffenen Person selbst erhoben werden, rechtfertigt dies den späteren Informationszeitpunkt. Meistens besteht in diesem Zeitpunkt nämlich gar kein direkter Kontakt zu der betroffenen Person selbst (Rn. 39). Dem Telos wird dabei besondere Beachtung geschenkt: Sowohl Art. 13 DS-GVO als auch Art. 14 DS-GVO verfolgen mit Blick auf Art. 16 AEUV und Art. 8 GRCh sowie Art. 7 GRCh das Ziel, „… ein hohes Niveau des Schutzes der Grundfreiheiten und der Grundrechte natürlicher Personen zu gewährleisten …" (Rn. 40). Es würde diesem zuwiderlaufen, würde man Datenerhebungen wie diese unter Art. 14 DS-GVO subsumieren können, da heimliche Überwachungsmaßnahmen wegen des späteren Informationszeitpunkts für den Verantwortlichen deutlich attraktiver wären (Rn. 41).

b) Einordnung und Ergänzung

Die Argumentation des EuGH überzeugt, wie zuvor angedeutet, in weiten Teilen. Allerdings lässt er in vielerlei Hinsicht Argumentationspotenzial ungenutzt, indem er den weiteren Folgen – sofern obige Praktiken Art. 14 DS-GVO unterfallen würden – nicht genügend Beachtung schenkt. So stellt nicht nur der spätere Informationszeitpunkt eine Bedrohung für die verfolgten Ziele dar. Vielmehr weist Art. 14 DS-GVO einen deutlich umfangreicheren Ausnahmekatalog auf, wann von einer Information gänzlich abgesehen werden kann. Besonders brisant ist in diesem Kontext die Regelung nach Art. 14 Abs. 5 lit. b DS-GVO: Demnach kann von der Informationspflicht abgesehen werden, wenn „die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; …" (mit einem Beispiel Kühling/Buchner/Bäcker, 4. Aufl. 2024, DS-GVO Art. 13 Rn. 13a).

Folgt man diesem Argumentationsweg weiter, wirkt sich das in einem erheblichen Maß auf weitere Betroffenenrechte aus. Hierzu äußert sich das Urteil leider nicht. Gegenargumente, wie das Folgende, werden gar nicht aufgenommen und folglich auch nicht entkräftet: Teilweise wird, um zum Ergebnis der Anwendung des Art. 14 DS-GVO zu gelangen, auf das systematische Verhältnis mit Art. 13 DS-GVO verwiesen (zB Ebner, Weniger ist Mehr?, S. 250; Jaksch/Hoffmann ZD 2022, 605). Während der Verantwortliche iRd Informationspflicht nach Art. 13 DS-GVO nicht die Kategorien personenbezogener Daten mitteilen muss, besteht nach Art. 14 Abs. 1 lit. d DS-GVO eine derartige Pflicht. Systematisch lasse sich daraus ableiten, der Gesetzgeber sei offensichtlich davon ausgegangen, die betroffene Person kenne immer die Kategorien der verarbeiteten personenbezogenen Daten und müsse daher nicht informiert werden. Dies treffe aber nur zu, wenn die Erhebung mit Kenntnis der betroffenen Person erfolgt. Wenn man solche Verarbeitungen ohne Kenntnis unter Art. 14 DS-GVO fallen ließe, dann entstünde dadurch ein „Mehr" an Informationen, das der Transparenz vielmehr dienlich sei, da nur Art. 14 DS-GVO eine Pflicht zur Information über die Kategorien der personenbezogenen Daten vorsieht.

Dieses auf den ersten Blick schlüssige, im Ergebnis aber wenig überzeugende Argument kann entkräftet werden: Die betroffene Person ist, selbst wenn ihr nach Art. 13 DS-GVO die Kategorien der verarbeiteten personenbezogenen Daten nicht mitgeteilt werden müssen, nicht schutzlos. Sie kann in diesem Fall ein Auskunftsersuchen nach Art. 15 DS-GVO erheben. Einzig und allein würde(n) ihr die Quelle(n) der Daten nicht mitgeteilt werden. Eine Pflicht des Verantwortlichen, diese zu beauskunften, besteht nach dem Wortlaut nur, wenn diese nicht bei der betroffenen Person erhoben wurden, vgl. Art. 15 Abs. 1 lit. g DS-GVO. Dies ist das einzig verbleibende Dilemma, das aber vor dem übrigen Hintergrund als hinzunehmen gilt. Der Gesetzgeber sollte an dieser Stelle jedoch nachjustieren.

Zudem überließe man es bei einem anderen Verständnis dem Verantwortlichen, ob nun Art. 13 DS-GVO oder Art. 14 DS-GVO greift (Kühling/Buchner/Bäcker, 4. Aufl. 2024, DS-GVO Art. 13 Rn. 13a). Da aber heimliche Maßnahmen nach dem Telos der DS-GVO gerade nicht die Regel sein sollen, würde dies – den Blick erneut auf den späteren Informationszeitpunkt und die weitreichenden Ausnahmevorschriften des Art. 14 DS-GVO gerichtet – dem diametral entgegenlaufen. Hierzu hätte noch ausdrücklicher auf den Erwägungsgrund 60 S. 1 DS-GVO hingewiesen werden können: Demnach machen es „(d)ie Grundsätze einer fairen und transparenten Verarbeitung … erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird."

3. Fazit und Reformvorschlag

Die Entscheidung des EuGH ist schlüssig. Einer zwingenden Notwendigkeit für eine Klarstellung, dass es für die Informationspflicht nach Art. 13 DS-GVO nur darauf ankomme, dass die personenbezogenen Daten bei der betroffenen Person erhoben worden sind und es somit nicht maßgeblich sei, ob Letztere hiervon Kenntnis habe, bedarf es nicht. Der Wortlaut war diesbezüglich schon immer eindeutig. Da jedoch im Falle heimlicher Überwachungspraktiken ggf. die Lücke verbleibt, dass keine Information – auch nicht über ein Auskunftsersuchen nach Art. 15 DS-GVO – über die Quelle der Daten zu erfolgen hat, ist es sinnvoll, diese zu schließen. Denkbar sind an dieser Stelle zwei Ansatzpunkte: Einerseits könnte an Art. 13 DS-GVO, andererseits an Art. 15 DS-GVO angeknüpft werden.

ÖOGH: EuGH-Vorlage zur automatisierten Bonitätsprüfung

DS-GVO Art. 22
Beschluss vom 13.8.2025 – 6 Ob 15/25m (OLG Linz, LG Salzburg)

Leitsatz der Redaktion

Dem EuGH werden gem. Art. 267 AEUV folgende Fragen zur Vorabentscheidung vorgelegt:

1. Ist Art. 22 Abs. 1 DS-GVO dahin auszulegen, dass die Entscheidung eines Versandhändlers, die vom Kunden bei seiner Bestellanfrage gewünschte Zahlungsart „Teilzahlung" oder „auf offene Rechnung" abzulehnen, sich dem Kunden gegenüber aber bereit zu erklären, die Geschäftsbeziehung entweder mit der Zahlungsart „Kreditkarte" oder mit der Zahlungsart „PayPal" einzugehen, die ausschließlich auf einer automatisierten Einschätzung der Zahlungsausfallswahrscheinlichkeit eines Kunden beruht, die sich daraus ergibt, dass entweder nach einer automatischen Anfrage bei einer Auskunftei von dieser die Rückmeldung erstattet wird, dass der Kunde dort unbekannt ist, oder dass – bei einem bekannten Kunden – ein internes Bonitätsscoring zum Ergebnis gelangt, dass der Kunde über keine ausreichende Bonität verfügt, gegenüber dem Kunden „rechtliche Wirkung" entfaltet oder ihn „in ähnlicher Weise erheblich beeinträchtigt", sofern durch diese Entscheidung nicht der Auftrag an sich abgelehnt wird, sondern der Kunde nur auf die vom Versandhändler vorgegebenen Zahlungsarten eingeschränkt wird? Falls die Frage 1. bejaht wird:

2. a) **Ist Art. 22 Abs. 2 lit. a DS-GVO dahin auszulegen, dass es für die Frage, ob eine auf einer automatisierten Einschätzung der Zahlungsausfallswahrscheinlichkeit des potenziellen Kunden beruhende Entscheidung eines Versandhändlers wie in Frage 1. beschrieben, für den Abschluss eines Vertrags zwischen dem Kunden und dem Versandhändler „erforderlich" ist, darauf ankommt, dass zwischen dem Vertragszweck des mit dem Kunden abzuschließenden Vertrags und der Einschätzung der Zahlungsausfallswahrscheinlichkeit des Kunden ein unmittelbarer sachlicher Zusammenhang bestehen muss?**
2. b) **Müssen zur Bejahung der Erforderlichkeit nach Art. 22 Abs. 2 lit. a DS-GVO die erhobenen Datenkategorien entweder für sich oder in ihrer Kombination objektiv dazu geeignet sein, die Zahlungsausfallswahrscheinlichkeit einzuschätzen? Hat der Versandhändler oder der Kunde zu behaupten und zu beweisen, welche Datenkategorien zum Zweck der Einschätzung der Zahlungsausfallswahrscheinlichkeit konkret erhoben wurden und dass diese Datenkategorien entweder für sich oder in ihrer Kombination objektiv dazu geeignet sind, die Zahlungsausfallswahrscheinlichkeit einzuschätzen? Falls die Frage 1. bejaht wird:**
3. **Ist Art. 22 Abs. 2 lit. a DS-GVO dahin auszulegen, dass gerade eine Entscheidungsfindung in automatisierter Form des Verantwortlichen für den Abschluss oder die Erfüllung des Vertrags erforderlich ist? Falls die Frage 3. bejaht wird:**
3. a) **Ist Art. 22 Abs. 2 lit. a DS-GVO dahin auszulegen, dass es für die Frage, ob eine Entscheidung eines Versandhändlers wie unter Frage 1. beschrieben, für den Abschluss des Vertrags erforderlich ist, darauf ankommt, ob die automatisierte Entscheidungsfindung betreffend die Gewährung oder Ablehnung der gewünschten Zahlungsart mit vertretbarem Aufwand auch durch Menschen erfolgen kann? Welche Bedeutung haben dafür die Anzahl der beim Versandhändler einlangenden Bestellungen und die typische Erwartung der Kunden im Online-Bestellverfahren, umgehend darüber informiert zu werden, ob die von ihnen gewünschte Zahlungsart vom Versandhändler akzeptiert wird oder nicht?**

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 21621. Vgl. ferner EuGH ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke – SCHUFA.

Sachverhalt

Der Kl. ist ein klageberechtigter Verein iSd § 29 Konsumentenschutzgesetz (öKSchG). Die Bekl. ist ein österreichweit tätiges Versandhandelsunternehmen, das laufend mit Verbrauchern Verträge abschließt.

Zahlungsausfallrisiko
Profiling
Zahlungsartbeschränkung
Rechtliche Wirkung
Erforderlichkeit

In der Datenschutzinformation der Bekl. finden sich Informationen zur Bonitätsprüfung. Diese lauten auszugsweise:

„Bonitätsprüfungen: Wenn Sie im Rahmen einer Bestellung eine sogenannte unsichere Zahlungsart (Rechnungs- oder Ratenkauf) ausgewählt haben, gilt das Folgende: Die Bekl. und andere Versandhandelsunternehmen der * Gruppe räumen ihren Kunden grundsätzlich die Möglichkeit ein, Waren unter Inanspruchnahme unsicherer Zahlungsarten (z.B. Rechnungskauf, Finanzierungskauf) zu erwerben.

Wir sind in den Fällen, in denen ein Kunde auf eine unsichere Zahlungsart bestellen möchte, dazu berechtigt, im Rahmen der Bestellung erhaltene Informationen zur Berechnung einer Ausfallswahrscheinlichkeit zu nutzen (internes Scoring). Die Berechnung der Ausfallswahrscheinlichkeit mittels des internen Scorings basiert auf einem anerkannten mathematisch statistischen Verfahren. Die im Rahmen des internen Scoring genutzten Daten resultieren insbesondere aus einer Kombination der folgenden Datenkategorien (nicht abschließend): Adressdaten, Alter, gewünschte Zahlungskonditionen, Bestellweg und Sortimentsgruppen. IRd internen Scoring werden nur solche Daten genutzt, die der Kunde uns gegenüber selbst angegeben hat. Anhand der benannten Datenkategorien können auf Grund des eingesetzten mathematisch statistischen Verfahrens Rückschlüsse auf die Zahlungsausfallswahrscheinlichkeit getroffen werden. ... Im Rahmen der Prüfung, ob eine unsichere Zahlungsart (Raten-/Rechnungskauf) eingeräumt werden kann, sind wir auch dazu berechtigt, Bonitätsinformationen über Sie bei einer externen Auskunftei einzuholen. Wir arbeiten mit der folgenden Auskunftei zusammen. ...

Wir können im Rahmen der Bonitätsprüfung mittels des Einsatzes eines automatisierten Prozesses entscheiden, ob Ihnen die gewünschte unsichere Zahlungsart (Raten-/Rechnungskauf) eingeräumt wird. So kann z.B. bei der Übermittlung einer negativen Bonitätsauskunft durch eine Auskunftei oder bei der Berechnung eines nicht ausreichenden Score-Wertes im Rahmen des internen Scoring automatisiert eine Ablehnung der gewünschten Zahlungsart erfolgen. Sie können uns gegenüber das Recht geltend machen, dass wir eine manuelle Überprüfung der automatisierten Entscheidung vornehmen. Darüber hinaus haben Sie das Recht auf Darlegung des eigenen Standpunkts sowie das Recht auf Anfechtung der Entscheidung."

Bei der Bekl. langen pro Monat ca. 50.000 bis 60.000 Bestellungen ein, davon 90% online und ca. 10% telefonisch. Ca. 90% der Bestellungen entfallen auf sog. unsichere Zahlungsarten, nämlich 60% auf offene Rechnung und ca. 31% auf Teilzahlung. Der Rest verteilt sich auf die verbleibenden Möglichkeiten per Kreditkarte oder per PayPal. Der durchschnittliche Bestellwert liegt bei 650 EUR.

Im Falle eines Neukunden, der auf offene Rechnung oder Teilzahlung bestellt, erfolgt automatisch eine Anfrage bei der Auskunftei mit den vom Kunden bekannt gegebenen Daten. Wenn der Kunde dort unbekannt ist, lehnt die Bekl. eine Geschäftsbeziehung mit Teilzahlung oder auf offene Rechnung ab und verständigt den Kunden, dass er über Kreditkarte oder PayPal beliefert würde. Wenn der Kunde bekannt ist, gibt es drei Möglichkeiten, Scorings mit drei verschiedenen Farben. Wenn die Farbe rot ist, wird ebenfalls die unsichere Zahlungsart abgelehnt, bei gelb prüft ein Mitarbeiter der beklagten Partei und bei grün wird die Bestellung angenommen. Im Fall eines gelben Scorings nimmt der Mitarbeiter selbst Einsicht in die Datenbank und entscheidet, ob und ggf. unter welchen Bedingungen der Auftrag freigegeben wird.

Wenn die Farbe rot oder die bestellende Person unbekannt ist, führt dies ausschließlich zu einer Einschränkung der Zahlungsmöglichkeiten auf eine sichere Zahlungsart, in keinem Fall zu einer Ablehnung des Auftrags an sich.

Der Kl. begehrt – soweit für das Revisionsverfahren im zweiten Rechtsgang noch relevant – gestützt auf § 28a Abs. 1 öKSchG, der Bekl. aufzutragen, es im geschäftlichen Verkehr mit Verbrauchern im Zusammenhang mit Verbraucherkreditverhältnissen zu unterlassen, Bonitätsprüfungen, die über den Abschluss von Vereinbarungen über Teilzahlung oder Lieferung auf offene Rechnung entscheiden, anhand einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung, insb. aufgrund des Ergebnisses einer automatisierten Anfrage bei einer Auskunftei oder aufgrund einer automatisierten internen Bewertung der Kreditwürdigkeit des Verbrauchers vorzunehmen, dies ohne eine ausdrückliche Einwilligung des Verbrauchers dazu einzuholen und/oder ohne dem Verbraucher das Recht einzuräu-

men, seinen eigenen Standpunkt darzulegen und/oder die von der Bekl. derart getroffene Entscheidung anzufechten.

Das Erstgericht wies das Klagebegehren ab. Die Vorgangsweise der Bekl. stehe mit Art. 22 DS-GVO im Einklang.

Das Berufungsgericht bestätigte die Rechtsansicht des Erstgerichts. Der Anwendungsbereich des Art. 22 Abs. 1 DS-GVO sei bereits nicht eröffnet. Die Beschränkung auf ein bestimmtes Bezahlverfahren stelle keine erhebliche Beeinträchtigung dar, solange (wie hier) zumutbare Bezahlverfahren verfügbar blieben. Abgesehen davon sei die automatisierte Einzelfallentscheidung aber nach Art. 22 Abs. 2 lit. a DS-GVO auch für den Abschluss oder die Erfüllung des Vertrags erforderlich. Aufgrund der Vielzahl an Bestellungen sei eine Bonitätsprüfung durch natürliche Personen für die Bekl. praktisch nicht möglich. Zudem erwarteten die Kunden eine umgehende Entscheidung über die von ihnen begehrte Zahlungsart, was bei Bearbeitung durch eine natürliche Person einen unvertretbaren Aufwand zur Folge hätte. Das System der Bekl. entspreche auch Art. 22 Abs. 3 DS-GVO.

Aus den Gründen

16 Der Kl. wirft der Bekl. einen systematischen Verstoß gegen die Regelung der automatisierten Entscheidungsfindung gemäß (dem unmittelbar im innerstaatlichen Recht anwendbaren) Art. 22 DS-GVO vor. Stellt sich dieser Vorwurf als berechtigt dar, wäre die Bekl. – gestützt auf § 28a öKSchG – zu verpflichten, ihre gegen Art. 22 DS-GVO verstoßende Geschäftspraktik zu unterlassen.

17 Dazu sind folgende Prüfschritte vorzunehmen:
(1) Zunächst ist zu ermitteln, ob der Anwendungsbereich des Art. 22 Abs. 1 DS-GVO eröffnet ist. Die Anwendbarkeit der Bestimmung hängt von drei kumulativen Voraussetzungen ab, nämlich davon, dass erstens eine „Entscheidung" vorliegen, zweitens diese Entscheidung „ausschließlich auf einer automatisierten Verarbeitung, – einschließlich Profiling – (beruhen)" und drittens sie „gegenüber (der betroffenen Person) rechtliche Wirkung" entfalten oder sie „in ähnlicher Weise erheblich" beeinträchtigen muss (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 43 – SCHUFA). Sind die Voraussetzungen nicht erfüllt, wäre die Klage mangels Anspruchsgrundlage abzuweisen.
(2) Fällt die gegenständliche Datenverarbeitung dagegen unter Art. 22 Abs. 1 DS-GVO, wäre sie nur dann zulässig, wenn einer der in Art. 22 Abs. 2 DS-GVO genannten Ausnahmetatbestände verwirklicht ist. Dies ist nach lit. a leg cit insb. dann der Fall, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist.
(3) Liegt ein Fall des Art. 22 Abs. 2 lit. a oder lit. c DS-GVO vor, hat die Bekl. angemessene Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen ihrer Kunden zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens der Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

18 Die Vorlagefragen betreffen die Auslegung einzelner Begriffe der in den ersten beiden Prüfschritten anzuwendenden Bestimmungen der DS-GVO, soweit diese nicht bereits durch Rspr. des EuGH geklärt ist und aufgrund des wechselseitigen Parteivorbringens entscheidungswesentlich ist.

2. Zur Frage 1.

19 Voranzustellen ist, dass sich der Kl. im Verfahren – entgegen dem Standpunkt des Berufungsgerichts – auch darauf gestützt hat, dass die automatisierte Entscheidung der Bekl., ihren Kunden bestimmte Zahlungsarten zu verweigern, diesen ggü. „rechtliche Wirkung entfaltet". Insofern ist im Verfahren auch dieses Tatbestandsmerkmal zu prüfen.

20 Die Begriffe „rechtliche Wirkung entfaltet" und „in ähnlicher Weise erheblich beeinträchtigt" werden in der DS-GVO nicht näher definiert. Allein aus dem Wortlaut des Art. 22 Abs. 1 DS-GVO ergibt sich nicht, ob eine Entscheidung der Bekl. wie unter Frage 1. beschrieben rechtliche Wirkung entfaltet oder den Betroffenen in ähnlicher Weise erheblich beeinträchtigt. Nach Erwägungsgrund 71 DS-GVO umfasst eine Entscheidung iSd Art. 22 Abs. 1 DS-GVO zB die automatische Ablehnung eines Online-Kreditvertrags oder Online-Einstellungsverfahren ohne menschliches Eingreifen (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 45 – SCHUFA).

21 Der ÖOGH vertritt zwar die Auslegung, dass die bloße Verwehrung bestimmter Vertragskonditionen – und insb. der Abschluss von Verträgen nur unter Gewährung bestimmter (für den Händler kein kreditorisches Risiko aufweisender) Bezahlverfahren – keine rechtliche Wirkung für die Kunden entfaltet, weil eine solche Entscheidung weder eine Rechtsposition des Kunden noch ein Rechtsverhältnis zu ihm begründet (vgl. etwa Schulz in Gola/Heckmann, DS-GVO – BDSG, DS-GVO Art. 22 Rn. 24, 25; BeckOK Datenschutzrecht/von Lewinski, DS-GVO Art. 22 Rn. 35). Denkbar wäre aber auch, dass darin im Kern eine Entscheidung über die konkrete Ausgestaltung von Verträgen liegt und damit sehr wohl eine rechtliche Wirkung für den (potenziellen) Vertragspartner verbunden ist, weil über „das Ob oder Wie" eines Vertragsabschlusses oder einer Vertragsänderung entschieden wird (vgl. Veil in Gierschmann/Schlender/Stentzel/Veil, Komm., DS-GVO Art. 22 Rn. 60).

22 Zu erwägen wäre aber auch, ob die Verweigerung bestimmter Zahlungsarten die wirtschaftlichen oder persönlichen Belange der Kunden derart berührt, dass sie einer rechtlichen Wirkung gleichkommt, und sie damit zumindest in ähnlicher Weise beeinträchtigt. Der ÖOGH geht davon aus, dass eine erhebliche Beeinträchtigung bei bloßer Festlegung auf ein bestimmtes Zahlverfahren zu verneinen ist, solange dem Kunden – wie hier – die Möglichkeit eingeräumt wird, den Vertrag unter Verwendung anderer, zumutbarer Zahlungsarten abzuschließen (Schulz in Gola/Heckmann, DS-GVO – BDSG, DS-GVO Art. 22 Rn. 22, 25; Haidinger in Knyrim, DatKomm, DS-GVO Art. 22 Rn. 26/3). Im Verfahren C-634/21 – SCHUFA [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke], entschied der EuGH allerdings, dass einen Verbraucher die Ermittlung eines Wahrscheinlichkeitswerts hinsichtlich seiner Fähigkeit, künftig einen Kredit zu bedienen, wenn im Fall eines unzureichenden Wahrscheinlichkeitswerts die Bank in nahezu allen Fällen die Gewährung des von ihm beantragten Kredits ablehnt, „zumindest erheblich beeinträchtigt" (Rn. 48, 49). Inwieweit das auch für die bloße Verwehrung bestimmter Zahlungsarten gilt, wurde vom EuGH bislang – soweit überblickbar – noch nicht entschieden. Fraglich erscheint insb., ob – und wenn ja unter welchen Voraussetzungen – dies überhaupt einer Ablehnung eines Vertragsverhältnisses mit dem Kunden gleichzuhalten ist, und falls ja ob – wie der Kl. argumentiert – die Ablehnung der Teilzahlung vergleichbare Auswirkungen auf den Kunden hat wie eine Beschränkung des Zugangs zu einem Kredit iSd Entscheidung des EuGH [v. 7.12.2023 –] C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke].

23 Die Beantwortung der Vorlagefrage ist für den vorliegenden Rechtsstreit maßgeblich, weil im Fall der Verneinung sowohl einer rechtlichen Wirkung als auch einer in ähnlicher Weise erheblichen Beeinträchtigung bereits der Anwendungsbereich

des Art. 22 Abs. 1 DS-GVO nicht eröffnet wäre und die Klage schon aus diesem Grund abzuweisen wäre.

3. Zu den Fragen 2.a), 2.b), 3. und 3.a)

24 Sofern die Frage 1. bejaht wird, wäre zu prüfen, ob der Ausnahmetatbestand des Art. 22 Abs. 2 lit. a DS-GVO erfüllt ist. Die Beantwortung der Vorlagefragen 2.a), 2.b), 3. und 3.a) ist für den vorliegenden Rechtsstreit maßgeblich, weil damit der dafür heranzuziehende Auslegungsmaßstab der Ausnahmebestimmung geklärt werden soll. Ergibt die Auslegung, dass sich die Bekl. im vorliegenden Fall nicht auf diese Ausnahme berufen kann (und liegen auch die Voraussetzungen nach lit. b und lit. c nicht vor), wäre der Klage stattzugeben. Kann sich die Bekl. dagegen auf Absatz 2 lit. a berufen, wäre – iSd dritten Prüfschritts – zu prüfen, ob die Bekl. die in Art. 22 Abs. 3 DS-GVO vorgesehenen Verfahrensgarantien einhält.

25 Der Kl. hat im Verfahren behauptet, es liege kein sachlicher Zusammenhang zwischen dem Vertragszweck und der Entscheidung der Bekl., bestimmte Zahlungsarten nicht zu gewähren, vor. Fraglich ist vor diesem Hintergrund zunächst, ob – wie auch in der deutschen und in der österreichischen Lit. allgemein vertreten – für die Frage der Erforderlichkeit ein sachlicher Zusammenhang zwischen der (automatisiert erfolgten) Einschätzung der Bonität des Kunden anhand bestimmter erhobener Daten als Grundlage für die gegenständliche Entscheidung des Versandhändlers, bestimmte Zahlungsarten nicht zu gewähren, und dem konkreten Vertragszweck mit seinen Rechten und Pflichten, insb. der Entscheidungs- und Kalkulationsgrundlage des Vertragshändlers, die hier in der erwarteten Bonität des Kunden liegt, vorliegen muss (vgl. etwa Scholz in NK-Datenschutzrecht DS-GVO/BDSG, DS-GVO Art. 22 Rn. 45; Martini in Paal/Pauly, DS-GVO BDSG, DS-GVO Art. 22 Rn. 31a; Arning in Moos/Schefzig/Arning, Praxishandbuch DS-GVO, Kap. 6 Rn. 640 u.a.).

26 Sofern es darauf ankommen sollte, geht der ÖOGH davon aus, dass im vorliegenden Fall grds. ein ausreichender sachlicher Zusammenhang zwischen der automatisierten Bonitätsprüfung des Kunden und dem Vertragszweck vorliegt, weil die Entscheidung, dem Kunden bestimmte (für den Versandhändler mit einem kreditorischen Risiko verbundene) Zahlungsarten nicht zu gewähren, zur Erreichung des Vertragszwecks, den jeweiligen Kaufvertrag ohne Leistungsstörungen abzuwickeln, geeignet ist, zumal als maßgebliche Entscheidungsgrundlage für den Versandhändler, ein bestimmtes Rechtsgeschäft einzugehen, gerade die Einschätzung der Bonität des einzelnen Kunden dient. Dass die Daten des Kunden vom Versandhändler zum Zweck der Einschätzung der Zahlungsausfallswahrscheinlichkeit erhoben werden, hat der Kl. im Verfahren nicht bestritten. (Frage 2.a))

27 Der ÖOGH vertritt in seiner Auslegung des Art. 22 Abs. 2 lit a DS-GVO aber weiters die Ansicht, dass es für die Bejahung der Erforderlichkeit (auch) darauf ankommt, dass die vom Versandhändler konkret erhobenen Datenkategorien (entweder für sich genommen oder in ihrer Kombination) objektiv geeignet sein müssen, die Bonität des Kunden einzuschätzen. Ansonsten ließe sich nämlich gerade ein sachlicher Zusammenhang zwischen der auf diesen Daten beruhenden Bonitätseinschätzung durch den Versandhändler und dem Vertragszweck nicht begründen. Insofern erscheint es einerseits jedenfalls fraglich, warum es schon aufgrund der Rückmeldung der Auskunftei, dass der Kunde dort unbekannt sei, erforderlich sein soll, die vom Kunden gewünschte Zahlungsart abzulehnen. Ist die Bekl. bestrebt, ihr Ausfallsrisiko wegen zu geringer Bonität ihrer Kunden zu minimieren, wäre es nämlich naheliegend, auch bei unbekannten Kunden zunächst eine weitergehende Prüfung anhand der von den Kunden beim Bestellvorgang angegebenen Daten in Form eines weiteren Bonitäts-Scorings vorzunehmen. Andererseits blieb im bisherigen Verfahren überhaupt offen, welche konkreten Daten die Bekl. (bei bekannten Kunden) iRd durchgeführten Bonitätsscorings erhebt. Sollte es darauf ankommen, wären die getroffenen Feststellungen allenfalls nicht ausreichend.

28 Damit im Zusammenhang steht die Frage, ob der Versandhändler oder der Kunde zu behaupten und zu beweisen hat, welche Daten konkret erhoben wurden und ob diese (entweder für sich genommen oder in ihrer Kombination) geeignet sind, die Zahlungsausfallswahrscheinlichkeit des Kunden einzuschätzen. Derartiges Vorbringen hat die Bekl. im Verfahren bislang nicht erstattet. (Frage 2.b))

29 Der ÖOGH vertritt die Ansicht, dass für die Anwendbarkeit des Ausnahmetatbestands nach Art. 22 Abs. 2 lit a DS-GVO gerade eine automatisierte Entscheidung für den Vertragsabschluss oder die Vertragserfüllung erforderlich sein muss (vgl. Buchner in Kühling/Buchner, DS-GVO/BDSG, DS-GVO Art. 22 Rn. 30a). Da der Wortlaut der Bestimmung nur Bezug auf die „Entscheidung" nimmt, ist es aber auch denkbar, dass es dafür allein auf die Erforderlichkeit der Entscheidung als solcher ankommt (vgl. Martini in Paal/Pauly, DS-GVO BDSG, DS-GVO Art. 22 Rn. 31a). In letzterem Fall wären für die Anwendbarkeit des Art. 22 Abs. 2 lit. a DS-GVO keine Überlegungen dazu anzustellen, ob (und unter welchen Voraussetzungen) auch eine Verarbeitung durch den Menschen möglich wäre. (Frage 3.)

30 Weiters geht der ÖOGH davon aus, dass es – wie in der deutschen und in der österreichischen Lit. vertreten (vgl. etwa Herbst in Auernhammer, DS-GVO BDSG, DS-GVO Art. 22 Rn. 19) – für die Erforderlichkeit einer automatisierten Entscheidung über die Gewährung bestimmter Zahlungsarten bei Vertragsabschluss darauf ankommt, ob diese Entscheidungsfindung mit vertretbarem Aufwand durch Menschen erfolgen kann. Fraglich ist jedoch, ob – wie von der Bekl. vorgebracht – die Anzahl der Bestellungen und die Erwartung von Kunden im Online-Bestellverfahren, umgehend über die Möglichkeit der von ihnen gewählten Zahlungsart informiert zu werden, einen Einfluss auf diese Beurteilung haben, oder ob ein Versandhändler vielmehr – wie der Kl. meint – jedenfalls sicherzustellen hat, dass genügend Mitarbeiter zur Verfügung stehen um die eingehenden Bestellungen abwickeln zu können, sodass es keines Rückgriffs auf eine automatisierte Entscheidungsfindung bedarf. Im ersten Fall wäre davon auszugehen, dass die automatisierte Entscheidungsfindung der Bekl. erforderlich ist; im zweiten Fall nicht. …

BGH: Beitragsanpassungsinformationen als personenbezogene Daten

DS-GVO Art. 4 Nr. 1, 15 Abs. 1 und Abs. 3
Urteil vom 18.12.2025 – I ZR 115/25 (LG Leipzig, AG Borna)

Leitsatz

Informationen zum Beitragsverlauf eines privaten Krankenversicherungsvertrags (nämlich zu Zeitpunkt und Höhe des Alt- und Neubeitrags für jede stattgefundene Beitragsanpassung, zum Zeitpunkt erfolgter Tarifwechsel unter Angabe des Herkunfts- und Zieltarifs und zum Zeitpunkt erfolgter Tarifbeendigungen) stellen nur dann personenbezogene Daten iSv Art. 15 Abs. 1 DS-GVO iVm Art. 4 Nr. 1 DS-GVO dar, wenn sie mit einer bestimmten Person verknüpft sind, die Person also auf Grundlage der Informationen identifiziert ist oder (direkt oder indirekt) identifiziert werden kann (vgl. EuGH Urt. v. 19.10.2016 – C-582/14 [= ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel] Rn. 47 bis 49 – Breyer; Urt. v. 7.3.2024 – C-604/22 [= ZD 2024, 328 mAnm Halim/Marosi = MMR 2024, 390 mAnm Keppeler/Schneider] Rn. 37 bis 39 –

IAB Europe/Gegevensbeschermingsautoriteit). Dass eine Information einen Sachverhalt betrifft, der Auswirkungen auf eine bestimmte Person hat, reicht für die Annahme eines personenbezogenen Datums allein nicht aus.

Anm. d. Red.: Die Anmerkung gibt ausschließlich die persönliche Auffassung der Autoren wieder. Vgl. hierzu EuGH ZD 2018, 113; EuGH ZD 2023, 539; BVerwG ZD 2023, 296 mAnm Viehweger/Koreng; BGH ZD 2022, 326; BGH ZD 2024, 343 mAnm Viehweger; AG Chemnitz ZD 2025, 171 mAnm Hense; BGH ZD 2021, 581 mAnm Riemer; BGH ZD 2024, 392; BGH ZD 2024, 632; OLG Brandenburg ZD 2024, 460; OLG Dresden ZD 2025, 364 (Ls.); OLG Schleswig ZD 2023, 156; OLG Koblenz ZD 2024, 730; EuGH MMR 2012, 174; EuGH ZD 2015, 77 mAnm Lachenmann – Ryneš; EuGH ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel – Breyer; EuGH ZD 2024, 328 mAnm Halim/Marosi = MMR 2024, 390 mAnm Keppeler/Schneider – IAB Europe; BGH ZD 2024, 346 und OLG Rostock ZD 2024, 728.

Sachverhalt

Der Kl. ist seit September 2010 bei der Bekl. privat kranken- und pflegeversichert. In den vergangenen Jahren wurde der monatlich von ihm hierfür zu zahlende Beitrag mehrfach angepasst. Die Anpassungen wurden dem Kl. jeweils unter Übersendung eines (Nachtrags-)Versicherungsscheins und eines standardisierten Informationsschreibens zur Beitragsanpassung mitgeteilt. Dem Kl. liegen die Nachträge zum Versicherungsschein und die Begründungsschreiben nicht mehr vor. Im März 2023 forderte er die Bekl. vergeblich zur Herausgabe dieser Unterlagen auf.

Auskunftsrecht
Krankenversicherung
Identifizierbarkeit
Verknüpfung
Tarifwechsel

Die auf Auskunftserteilung und Schadensersatz gerichtete Klage hat das AG abgewiesen. Hiergegen hat der Kl. Berufung eingelegt und hilfsweise ergänzend beantragt, die Bekl. zu verurteilen, der Klägerseite eine Kopie der personenbezogenen Daten zum Beitragsverlauf des Versicherungsvertrags in den Jahren 2014, 2015, 2017, 2018, 2019, 2020, 2021 und 2023 zur Verfügung zu stellen, aus der folgende Informationen zu entnehmen sind:
a) Zeitpunkt und Höhe des Alt- und Neubeitrags für jede stattgefundene Beitragsanpassung gem. § 203 Abs. 2 VVG,
b) Zeitpunkt erfolgter Tarifwechsel unter Angabe des Herkunfts- und Zieltarifs,
c) Zeitpunkt erfolgter Tarifbeendigungen.

Das Berufungsgericht hat das Urteil des AG abgeändert und die Bekl. unter Zurückweisung der Berufung iÜ nach dem Hilfsantrag verurteilt.

Das Berufungsgericht hat angenommen, dem Kl. stehe ein Auskunftsrecht nach Art. 15 Abs. 1 und Abs. 3 DS-GVO zu, weil die mit dem Hilfsantrag begehrten Informationen personenbezogene Daten seien.

Aus den Gründen

8 B. Die Revision der Bekl. hat Erfolg. Sie führt zur Aufhebung des Berufungsurteils und Zurückverweisung der Sache an das Berufungsgericht. ...

21 V. Mit der Begründung des Berufungsgerichts kann nicht angenommen werden, dass sämtliche vom Kl. begehrten Informationen personenbezogene Daten iSv Art. 15 Abs. 1 und Abs. 3, 4 Nr. 1 DS-GVO darstellen.

22 1. Das Berufungsgericht hat im Ausgangspunkt zutreffend zugrunde gelegt, dass der Begriff der personenbezogenen Daten weit zu verstehen ist und hierunter nicht allein sensible oder private Informationen fallen. Der Begriff umfasst vielmehr potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (vgl. EuGH Urt. v. 20.12.2017 – C-434/16 [= ZD 2018, 113] Rn. 34 f. – Nowak; Urt. v. 4.5.2023 – C-487/21 [= ZD 2023, 539] Rn. 23 f. – Österreichische Datenschutzbehörde und CRIF; BGH Urt. v. 22.2.2022 – VI ZR 14/21 [= ZD 2022, 326] Rn. 11; Urt. v. 27.9.2023 – IV ZR 177/22 Rn. 47; Urt. v. 6.2.2024 – VI ZR 15/23 [= ZD 2024, 343 mAnm Viehweger], jew. mwN).

23 2. Schreiben der betroffenen Person an den Verantwortlichen sind ihrem gesamten Inhalt nach als personenbezogene Daten einzustufen, da die personenbezogene Information bereits darin besteht, dass die betroffene Person sich dem Schreiben gemäß geäußert hat. Anderes gilt allerdings für Schreiben des Verantwortlichen an die betroffene Person, wie sie auch im Streitfall in Rede stehen. Diese unterfallen dem datenschutzrechtlichen Auskunftsanspruch nur insoweit, als sie Informationen über die betroffene Person nach den o.g. Kriterien enthalten (vgl. BGH Urt. v. 15.6.2021 – VI ZR 576/19 [= ZD 2021, 581 mAnm Riemer] Rn. 25; BGH NJW 2023, 3490 Rn. 48; BGH ZD 2024, 346 Rn. 10).

24 3. Bei den zu Beitragsanpassungen einer privaten Krankenversicherung ergangenen Begründungsschreiben nebst Anlagen handelt es sich nach der Rspr. des BGH jedenfalls nicht in ihrer Gesamtheit um personenbezogene Daten des Versicherungsnehmers. Sie können allerdings einzelne personenbezogene Daten des Versicherungsnehmers enthalten (vgl. BGH NJW 2023, 3490 Rn. 49; BGH Urt. v. 8.5.2024 – IV ZR 102/23 [= ZD 2024, 632] Rn. 10; BGH WM 2024, 555 [= ZD 2024, 343 mAnm Viehweger] Rn. 8). Der auslösende Faktor einer Prämienanpassung ist nicht mit einer bestimmten Person verknüpft. Es handelt sich dabei um die Abweichung der erforderlichen von den kalkulierten Versicherungsleistungen oder Sterbewahrscheinlichkeiten in einem Tarif in einer festgelegten Mindesthöhe (§ 203 Abs. 2 VVG iVm § 155 Abs. 3 und Abs. 4 VAG); ein Bezug zu einem bestimmten Versicherungsnehmer besteht nicht (vgl. BGH RuS 2024, 633 [= ZD 2024, 632] Rn. 14).

25 4. Unter Zugrundelegung dieser Maßstäbe kann mit der vom Berufungsgericht gegebenen Begründung nicht angenommen werden, dass die vom Kl. begehrten Informationen über den Zeitpunkt und die Höhe des Alt- und Neubeitrags für jede erfolgte Beitragsanpassung, über den Zeitpunkt erfolgter Tarifbeendigungen und Tarifwechsel unter Angabe des Herkunfts- und Zieltarifs und über den Zeitpunkt erfolgter Tarifbeendigungen sämtlich personenbezogene Daten iSv Art. 15 Abs. 1 und Abs. 3, 4 Nr. 1 DS-GVO darstellen.

26 a) In der obergerichtlichen Rspr. ist umstritten, ob Informationen wie diejenigen, die Gegenstand des streitgegenständlichen Auskunftsbegehrens sind, als personenbezogene Daten anzusehen sind.

27 aa) Nach einer Ansicht, der sich das Berufungsgericht angeschlossen hat, stellen die vom Kl. begehrten Informationen personenbezogene Daten dar (vgl. OLG Rostock ZD 2024, 728; OLG Brandenburg Urt. v. 28.2.2024 – 11 U 161/23 [= ZD 2024, 460] Rn. 12; Urt. v. 3.5.2024 – 11 U 19/24 Rn. 37; OLG Frankfurt/M. Urt. v. 10.12.2024 – 18 U 63/23 Rn. 47 f.; OLG Karlsruhe Urt. v. 17.12.2024 – 12 U 183/23 Rn. 48 f.; OLG Jena MDR 2025, 457 Rn. 68 bis 70; OLG Dresden NJW-RR 2025, 609 [= ZD 2025, 364 (Ls.)] Rn. 39 bis 42).

28 (1) Zur Begründung wird ausgeführt, aus den Versicherungsscheinen und deren Nachträgen ergebe sich, mit welchem Inhalt und zu welchen Konditionen für den Versicherungsnehmer bei dem Versicherer Versicherungsschutz bestehe (vgl. OLG Rostock ZD 2024, 728). Die konkretisierte und individualisierte Beitragsanpassung sei ein Datum, das unmittelbar nur auf den einzelnen Versicherungsnehmer zugeschnitten sei bzw. nur ihn betreffe (vgl. OLG Brandenburg Urt. v. 28.2.2024 – 11 U 161/23 [= ZD

2024, 460] Rn. 12; Urt. v. 3.5.2024 – 11 U 19/24 Rn. 37; OLG Karlsruhe Urt. v. 17.12.2024 – 12 U 183/23 Rn. 49; OLG Jena MDR 2025, 457 Rn. 70). ZT wird betont, auch wenn eine Prämie oder eine Prämienerhöhung in einem bestimmten Tarif oder zu einem bestimmten Zeitpunkt per se mit dem Versicherten nichts zu tun habe, sei sie deshalb mit ihm verknüpft und habe Auswirkungen auf ihn, weil er in entsprechenden Tarifen versichert und damit konkret von den Erhöhungen betroffen sei und die Neuprämien zahlen müsse (vgl. OLG Frankfurt/M. Urt. v. 10.12.2024 – 18 U 63/23 Rn. 47).

29 (2) Entsprechendes wird auch für Informationen über Zeitpunkt und Höhe erfolgter Tarifwechsel und Tarifbeendigungen vertreten (vgl. OLG Frankfurt/M. Urt. v. 10.12.2024 – 18 U 63/23 Rn. 49; OLG Karlsruhe Urt. v. 17.12.2024 – 12 U 183/23 Rn. 50; OLG Jena MDR 2025, 457 Rn. 69; aA OLG Dresden NJW-RR 2025, 609 [= ZD 2025, 364 (Ls.)] Rn. 43). Diese Informationen seien abhängig von den persönlichen Vertragserklärungen des Versicherungsnehmers, indem sich dieser mit der Folge des Tarifwechsels oder der Tarifbeendigung ggü. dem Versicherer geäußert habe. Schreiben des Versicherungsnehmers an die Versicherung zählten aber gemäß der Rspr. des BGH grds. ihrem gesamten Inhalt nach zu den personenbezogenen Daten. Tarifwechsel und Tarifbeendigungen geschähen individuell und gerade nicht einheitlich innerhalb einer Beobachtungseinheit, sodass auch eine Bestimmbarkeit der betroffenen Person anhand dieser Daten nicht ausgeschlossen erscheine. Hierin bestehe ein Unterschied zu den auslösenden Faktoren, für die der BGH eine Eigenschaft als personenbezogene Daten verneint habe. Eine Änderung der auslösenden Faktoren müsse sich nicht zwangsläufig auf den Versicherungsnehmer auswirken, da sie nicht immer zu einer Beitragsanpassung führe (vgl. OLG Jena MDR 2025, 457 Rn. 69 f.).

30 bb) Nach der Gegenansicht sind Informationen zum Beitragsverlauf wie diejenigen, hinsichtlich derer der Kl. Auskunft begehrt, keine personenbezogenen Daten (zu den im Streitfall begehrten Informationen vgl. OLG Dresden Beschl. v. 14.11.2024 – 4 U 379/24 Rn. 8 bis 10; Urt. v. 4.2.2025 – 4 U 1627/22 Rn. 29 bis 31; Beschl. v. 18.3.2025 – 4 U 1586/22 Rn. 40 bis 42; OLG Dresden Beschl. v. 16.7.2025 – 4 U 1448/22 Rn. 40 bis 44; zu Informationen über Beitragsanpassungen vgl. OLG Schleswig MDR 2022, 1286 [= ZD 2023, 156] Rn. 41 bis 49; OLG Koblenz NJW-RR 2023, 1592 [= ZD 2024, 730] Rn. 52 bis 54; OLG Köln Urt. v. 19.7.2024 – 20 U 27/23 Rn. 28 bis 35; Urt. v. 28.1.2025 – 3 U 71/24 Rn. 3 bis 17; Urt. v. 13.6.2025 – 20 U 176/24 Rn. 14 bis 24; zu Informationen über Tarifprämien vgl. OLG München RuS 2022, 94 Rn. 50 bis 56).

31 Die Informationen zum Beitragsverlauf seien nicht mit der Person des Versicherungsnehmers verknüpft. Der Erhöhungsbetrag sei nur das Ergebnis einer unter Berücksichtigung festgelegter Parameter angestellten Preisberechnung der Versicherung für einen bestimmten Tarif und lasse keine Rückschlüsse auf die Person des Versicherungsnehmers oder dessen individuellen Versicherungsvertrag zu. Vielmehr erfolge die Berechnung für alle Versicherungsnehmer, die infolge bestimmter abstrakter Parameter in eine Beobachtungseinheit zusammengefasst würden, in gleicher Weise. Die Höhe einer Beitragsanpassung spiegele nicht den individualisierten Versicherungsschutz des Versicherungsnehmers wider, sondern gebe nur Aufschluss darüber, um welchen monatlichen Differenzbetrag sich bezogen auf eine Beobachtungseinheit der Preis für eine durch den Versicherungsvertrag bzw. den fraglichen Tarif abgedeckte Vorsorge eines Versicherungsnehmers verändert habe. Aus der Angabe, welcher Beitrag für einen bestimmten Tarif zu entrichten sei, lasse sich nicht zurückverfolgen, um welchen Versicherungsnehmer es sich handele. Aus diesen Gründen stellten auch die Zeitpunkte, ab denen Betragsanpassungen jeweils wirkten, keine personenbezogenen Daten über die Person des Versicherungsnehmers dar, sondern lediglich eine Information über den Preis des jeweils von der Anpassung betroffenen Versicherungstarifs, der sich ab einem bestimmten Datum verändert habe (vgl. OLG Köln Urt. v. 19.7.2024 – 20 U 27/23 Rn. 33 f.; Urt. v. 28.1.2025 – 3 U 71/24 Rn. 10 f.; Urt. v. 13.6.2025 – 20 U 176/24 Rn. 20 bis 23; OLG Dresden Beschl. v. 14.11.2024 – 4 U 379/24 Rn. 10; Urt. v. 4.2.2025 – 4 U 1627/22 Rn. 29 f.; Beschl. v. 18.3.2025 – 4 U 1586/22 Rn. 40 bis 42; OLG Dresden Beschl. v. 16.7.2025 – 4 U 1448/22 Rn. 41).

32 b) Die zuletzt dargestellte Ansicht trifft – ausgehend von den jeweils getroffenen Feststellungen – zu, wohingegen der zuerst dargestellten Ansicht, der sich das Berufungsgericht angeschlossen hat, ein fehlerhafter rechtlicher Maßstab zugrunde liegt.

33 aa) Wie dargelegt, muss sich eine Information, damit sie nach der Definition des Art. 4 Nr. 1 DS-GVO ein personenbezogenes Datum darstellt, auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei eine indirekte Identifizierbarkeit ausreicht. Es muss sich um eine Information „über" eine Person handeln, was der Fall ist, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (vgl. oben Rn. 22 sowie die dortigen Nachweise). Der Umstand, dass eine Information einen Sachverhalt betrifft, der Auswirkungen auf eine bestimmte Person hat, reicht daher für die Annahme eines personenbezogenen Datums allein nicht aus. Vielmehr muss die Information aufgrund einer solchen Auswirkung (oder ihres Inhalts oder Zwecks) mit einer bestimmten Person in dem Sinne verknüpft sein, dass die Person auf Grundlage der Information identifiziert ist oder (direkt oder indirekt) identifiziert werden kann (vgl. EuGH Urt. v. 24.11.2011 – C-70/10 [= MMR 2012, 174] Rn. 51 – Scarlet Extended; Urt. v. 11.11.2014 – C-212/13 [= ZD 2015, 77 mAnm Lachenmann] Rn. 22 – Ryneš; Urt. v. 19.10.2016 – C-582/14 [= ZD 2017, 24 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel] Rn. 47 bis 49 – Breyer; Urt. v. 7.3.2024 – C-604/22 [= ZD 2024, 328 mAnm Halim/Marosi = MMR 2024, 390 mAnm Keppeler/Schneider] Rn. 37 bis 39 – IAB Europe/Gegevensbeschermingsautoriteit).

34 bb) Dies hat das Berufungsgericht nicht berücksichtigt, indem es unter Anschluss an das Thüringer OLG (MDR 2025, 457 Rn. 70) und in Übereinstimmung mit der unter Rn. 27 bis 29 dargestellten obergerichtlichen Rspr. maßgeblich darauf abgestellt hat, die von der Bekl. vorgenommenen Beitragsanpassungen hätten unmittelbare Auswirkungen auf die individuell geschuldete Versicherungsprämie und damit auf das individuelle Versicherungsverhältnis. Dass die Person des Versicherungsnehmers aufgrund der Informationen über Zeitpunkt und Höhe von Beitragsanpassungen oder aufgrund der festgestellten Auswirkungen auf das Versicherungsverhältnis identifiziert oder identifizierbar würde, hat das Berufungsgericht hingegen nicht festgestellt (dies trotz der Annahme personenbezogener Daten ausdrücklich verneinend OLG Brandenburg Urt. v. 3.5.2024 – 11 U 19/24 Rn. 37). Ein Bezug (zunächst) „neutraler" Daten zu einer konkreten Person (vgl. dazu BGH NJW-RR 2022, 764 [= ZD 2022, 326] Rn. 11) wird nicht allein dadurch hergestellt, dass die betroffene Person in entsprechenden Tarifen versichert und konkret von den Erhöhungen betroffen ist (so zutreffend OLG Köln Urt. v. 13.6.2025 – 20 U 176/24 Rn. 22; aA OLG Frankfurt/M. Urt. v. 10.12.2024 – 18 U 63/23 Rn. 47; OLG Karlsruhe Urt. v. 17.12.2024 – 12 U 183/23 Rn. 49).

35 Von der zuvor (unter Rn. 30 f.) dargestellten Ansicht wird die Verknüpfung mit einer bestimmten Person daher mit Recht verneint, wenn die Angabe, welcher Beitrag für einen bestimmten Tarif zu entrichten ist, keine Rückschlüsse darauf zulässt, um

welchen Versicherungsnehmer es sich handelt, und die Höhe der Tarife und der Zeitpunkt einer Tariferhöhung oder eines Tarifwechsels lediglich Auskunft darüber geben, welcher Preis für die durch den Versicherungsvertrag verwirklichte Vorsorge zu entrichten ist (vgl. OLG Dresden Beschl. v. 18.3.2025 – 4 U 1586/22 Rn. 40; OLG Köln Urt. v. 28.1.2025 – 3 U 71/24 Rn. 10; Urt. v. 13.6.2025 – 20 U 176/24 Rn. 20 bis 22). Feststellungen dahingehend, dass die im Streitfall begehrten Informationen Aufschluss darüber geben könnten, wann eine bestimmte natürliche Person nach welchem Tarif versichert war oder wann sie in welcher Höhe Versicherungsbeiträge gezahlt hat, hat das Berufungsgericht entgegen der Behauptung der Revisionserwiderung nicht getroffen.

36 cc) Mit der Begründung des Berufungsgerichts kann auch hinsichtlich der vom Kl. begehrten Informationen zum Zeitpunkt erfolgter Tarifwechsel unter Angabe des Herkunft- und Zieltarifs und zum Zeitpunkt von Tarifbeendigungen eine Eigenschaft als personenbezogene Daten nicht bejaht werden.

37 (1) Soweit das Berufungsgericht zur Begründung seiner dahingehenden Bewertung darauf verweist, Tarifwechsel und Tarifbeendigungen seien von Vertragserklärungen des Versicherungsnehmers abhängig (vgl. auch OLG Jena MDR 2025, 457 Rn. 69), greift dies zu kurz. Zwar sind Schreiben der betroffenen Person an den Verantwortlichen nach der zuvor (unter Rn. 23) wiedergegebenen Rspr. des BGH ihrem gesamten Inhalt nach als personenbezogene Daten einzustufen, weil die personenbezogene Information bereits darin besteht, dass die betroffene Person sich dem Schreiben gemäß geäußert hat. Allein daraus lässt sich jedoch nicht schließen, dass Informationen darüber, welche (rechtlichen oder tatsächlichen) Folgen sich aus entsprechenden Schreiben ergeben (hier: die auf einer Erklärung des Versicherten beruhende Tarifänderung), ihrerseits personenbezogene Daten sind. Etwaige Tarifänderungen stellen vielmehr eine aus der Sphäre des Versicherungsunternehmens stammende Reaktion auf die Erklärungen des Versicherungsnehmers dar. Schreiben des Verantwortlichen an die betroffene Person unterfallen aber nach der zuvor (unter Rn. 23) dargestellten Rspr. dem datenschutzrechtlichen Auskunftsanspruch nur insoweit, als sie Informationen über die betroffene Person nach den hierfür maßgeblichen Kriterien enthalten.

38 (2) Die Eigenschaft der Informationen zu Tarifwechseln und Tarifbeendigungen als personenbezogene Daten kann entgegen der Ansicht des Berufungsgerichts (vgl. auch OLG Jena MDR 2025, 457 Rn. 69) auch nicht ohne Weiteres daraus geschlossen werden, dass diese individuell und nicht einheitlich innerhalb einer Beobachtungseinheit geschehen. Die aus diesem Umstand gezogene Schlussfolgerung, eine Bestimmbarkeit der betroffenen Person anhand dieser Daten erscheine „nicht ausgeschlossen", verbleibt im Unklaren und wird vom Berufungsgericht nicht näher begründet. Sie reicht daher ebenfalls für sich genommen nicht aus, um einen Personenbezug der begehrten Daten zu begründen. ...

Anmerkung

Ministerialrat Dr. Ansgar Koreng, Sächsisches Staatsministerium der Justiz / Michael Viehweger, Vizepräsident des SG Leipzig

Mit dem vorliegenden Urteil setzt der I. Zivilsenat des BGH die Linie des IV. Zivilsenats (Urt. v. 27.9.2023 – IV ZR 177/22) und des VI. Zivilsenats (ZD 2024, 343 mAnm Viehweger) im Ergebnis fort und kommt zu dem Befund, dass aus Art. 15 Abs. 1 und Abs. 3 DS-GVO kein Anspruch auf Abschriften von Unterlagen eines privaten Krankenversicherungsunternehmens folge, aus denen sich Informationen über den Zeitpunkt und die Höhe des Alt- und Neubeitrags bei Beitragsanpassungen, über den Zeitpunkt von Tarifwechseln unter Angabe des Herkunfts- und Zieltarifs sowie über den Zeitpunkt von Tarifbeendigungen ergeben.

Der I. Zivilsenat setzt sich mit verschiedenen Ansichten zu der Frage auseinander, ob es sich bei den o.g. Unterlagen in Gänze um personenbezogene Daten handelt, und schließt sich der Auffassung an, wonach diese Unterlagen zwar personenbezogene Daten enthielten, jedoch nicht durchweg solche seien. Der Gegenansicht liege ein „fehlerhafter rechtlicher Maßstab zugrunde" (Rn. 32). Die Ausführungen des Senats überzeugen indes nicht vollständig.

Zunächst pflichtet der Senat dem Berufungsgericht insofern bei, als der Begriff der personenbezogenen Daten weit zu verstehen sei und hierunter nicht allein sensible oder private Informationen fielen. Der Begriff umfasse vielmehr potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur, sofern es sich um Informationen über die in Rede stehende Person handelt. Diese Voraussetzung sei erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (Rn. 22). Hiergegen ist nichts zu erwidern; diese Maßstäbe entsprechen der stRspr des EuGH (ZD 2018, 113 Rn. 34, 35).

Folgerichtig schließt sich der Senat sodann auch der Auffassung an, wonach Schreiben der betroffenen Person an den Verantwortlichen ihrem gesamten Inhalt nach als personenbezogene Daten anzusehen sind, da die personenbezogene Information bereits darin bestehe, dass die betroffene Person sich dem Schreiben gemäß geäußert habe (Rn. 23).

Anderes gelte allerdings für Schreiben des Verantwortlichen an die betroffene Person, wie sie auch im Streitfall in Rede stehen. Diese unterfielen dem datenschutzrechtlichen Auskunftsanspruch nur insoweit, als sie Informationen über die betroffene Person nach den o.g. Kriterien enthalten (Rn. 23). Mit der Begründung des Berufungsgerichts könne nicht angenommen werden, dass die vom Kl. begehrten Informationen sämtlich personenbezogene Daten iSv Art. 15 Abs. 1 und Abs. 3, 4 Nr. 1 DS-GVO darstellten (Rn. 25). Denn das Berufungsgericht habe nicht festgestellt, dass die Person des Versicherungsnehmers aufgrund der Informationen über Zeitpunkt und Höhe von Beitragsanpassungen oder aufgrund der festgestellten Auswirkungen auf das Versicherungsverhältnis identifiziert oder identifizierbar wird (Rn. 34).

Dies erscheint zweifelhaft. Der Senat rekurriert zunächst auf Art. 4 Nr. 1 DS-GVO, wonach eine Information dann ein personenbezogenes Datum darstellt, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person bezieht, wobei eine indirekte Identifizierbarkeit ausreicht. Es müsse sich – im Anschluss an die „Nowak"-Entscheidung des EuGH ZD 2018, 113 Rn. 34 – um eine Information „über" eine Person handeln, was der Fall ist, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (Rn. 22, 33). Schon dies macht deutlich, dass die Auswirkungen auf eine konkrete Person ausreichen, einer Information Personenbezug zu verleihen.

Den Befund des Berufungsgerichts, wonach die hier geforderten Informationen Auswirkungen auf die betroffene Person haben, zieht der Senat – insoweit zutreffend – auch nicht in Zweifel (Rn. 34). Die Informationen zu Zeitpunkt und Höhe des Alt- und Neubetrags für jede stattgefundene Beitragsanpassung gem. § 203 Abs. 2 VVG, zum Zeitpunkt erfolgter Tarifwechsel unter Angabe des Herkunfts- und Zieltarifs sowie zum Zeitpunkt erfolgter Tarifbeendigungen beziehen sich auf den Versicherungsvertrag des Kl. und bestimmen dessen Inhalt sowie die Höhe der Leistungspflicht des Kl. ggü. der Bekl. (vgl. AG Chemnitz ZD 2025, 171 mAnm Hense).

Der Senat fordert allerdings (offenbar zusätzlich), dass die Information aufgrund einer solchen Auswirkung (oder ihres Inhalts oder Zwecks) mit einer bestimmten Person in dem Sinne verknüpft sein müsse, dass die Person „auf Grundlage der Information" identifiziert sei oder (direkt oder indirekt) identifiziert werden könne (Rn. 33). Dies sei weder bei der Angabe, welcher Beitrag für einen bestimmten Tarif zu entrichten ist, noch bei der Höhe der Tarife sowie dem Zeitpunkt einer Tariferhöhung oder eines Tarifwechsels der Fall (Rn. 35).

Dabei erschließt sich aus der Entscheidung heraus nicht, wie diese vermeintliche Einschränkung gemeint sein soll. Die Wendung, wonach ein Datum nur dann Personenbezug habe, wenn die Person „auf Grundlage der Information" identifiziert werden kann, könnte so verstanden werden, dass der Senat meint, die betreffende Information selbst müsse die Identifizierung – wie auch immer – ermöglichen. Das hat dann freilich – wie auch im hier vorliegenden Fall – zur Folge, dass der Verantwortliche die vom Auskunftsbegehren umfassten Informationen nur in hinreichend kleine Bestandteile zerlegen muss, um hieran anschließend zu dem in der Folge wenig überraschenden Ergebnis zu gelangen, dass die sich hieraus ergebenden Informationssplitter dann jeweils eine Identifizierung einer bestimmten Person nicht mehr ermöglichen. Eine derartige Herangehensweise ist jedoch mit der in Art. 4 Nr. 1 DS-GVO angelegten Unterscheidung zwischen einer identifizierten und einer identifizierbaren natürlichen Person schwerlich vereinbar: Zwar ist eine Person in der Tat nur dann „identifiziert", wenn die Identität der Person unmittelbar aus der Information selbst folgt – wofür oftmals selbst Vor- und Zuname nicht ausreichen. Demgegenüber ist die Person iSd Vorschrift aber bereits dann „identifizierbar", wenn die Zuordnung gelingt, sobald die Information mit weiteren Informationen verknüpft wird (Kühling/Buchner/Klar/Kühling, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 1 Rn. 18 und 19 mwN). Der EuGH lässt es für eine Identifizierbarkeit iSv Art. 4 Nr. 5 DS-GVO iVm Erwägungsgrund 26 DS-GVO in stRspr genügen, dass ein Datum durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden kann (ZD 2024, 328 Rn. 39 mAnm Halim/Marosi). Auf diese Rspr. nimmt der Senat an der entscheidenden Stelle auch selbst Bezug. Mithin ist es eben nicht Voraussetzung von Art. 4 Nr. 1 DS-GVO, dass gerade das in Frage stehende Datum für sich genommen eine Identifizierung der Person ermöglicht. Vielmehr ist ein Datum auch dann personenbezogen, wenn es iSd „Nowak"-Entscheidung (EuGH ZD 2018, 113 Rn. 34 f.) aufgrund seines Inhalts, seines Zwecks oder seiner Auswirkungen mit einer bestimmten – anderweitig identifizierbaren – Person verknüpft ist. So ermöglicht etwa die Postanschrift eines Mehrfamilienhauses für sich genommen auch nicht die Identifizierung jedes Bewohners; befindet sie sich jedoch in den Unterlagen der Hausratsversicherung eines der Bewohner, so steht völlig außer Zweifel, dass sie – für die Versicherung – ihn betreffend Personenbezug hat. So ist es auch mit jeder anderen Information, die die Versicherung in ihren dem betroffenen Versicherungsnehmer zugeordneten Unterlagen speichert und auch mit jedem in einer Korrespondenz zwischen Versicherung und Versicherungsnehmer enthaltenen Satz.

Die vom Senat in Rn. 33 als Beleg angeführten Fundstellen stützen die These des Senats, die Person müsse „auf Grundlage" der gegenständlichen Information identifizierbar sein, nicht. Sie betreffen umgekehrt Fallgruppen, in denen eine Identifizierung gerade nicht ohne zusätzliche Informationen hergestellt werden konnte: So wurden IP-Adressen im Fall „Breyer" für personenbezogen gehalten, wenn der Verantwortliche „über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen" (EuGH ZD 2017, 24 Rn. 49 mAnm Kühling/Klar = MMR 2016, 842 mAnm Moos/Rothkegel). Im Fall „IAB Europe" konstatierte er den Personenbezug von „Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten" (EuGH ZD 2024, 328 Rn. 39). Die Entscheidung „Scarlet Extended" (EuGH MMR 2012, 174 Rn. 51) gibt für die Frage gar nichts her, weil dort lediglich konstatiert wird, dass IP-Adressen die genaue Identifizierung ermöglichten und mithin personenbezogen seien, ohne dass dies näher ausgeführt würde. Das Bild einer Person hielt der EuGH im Fall „Ryneš" wohl immerhin für sich genommen für personenbezogen, „sofern es die Identifikation der betroffenen Person ermöglicht" (EuGH ZD 2015, 77 Rn. 22 mAnm Lachenmann).

Wenn der Senat aber nur auf das allgemeine Merkmal der Identifizierbarkeit abstellen wollte, erscheint es unverständlich, warum der Kl. auf Grundlage der hier relevanten Informationen nicht identifizierbar sein sollte. Es wäre zu fragen gewesen, ob dem Bekl. als Verantwortlichem Mittel zur Verfügung stehen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt auf Grundlage der Information zu identifizieren (Erwägungsgrund 26 S. 3 DS-GVO; EuGH ZD 2025, 631 Rn. 79 ff.). Der Senat stellt zwar auf das Fehlen entsprechender Feststellungen des Berufungsgerichts ab und macht dies zur Grundlage der Zurückverweisung. Zu überzeugen vermag dies jedoch nicht.

In diesem Zusammenhang erscheint es nicht konsequent, wenn der BGH zwar alle Schreiben des Versicherten an die Versicherung als in ihrer Gänze personenbezogen begreifen möchte, nicht aber die Schreiben der Versicherung an den Versicherten (Rn. 23). Erkennt man im erstgenannten Fall den Personenbezug bereits darin, dass sich der Versicherte wie aus den Schreiben ersichtlich geäußert hat, so ist nicht nachvollziehbar, weshalb im zweitgenannten Fall ein solcher Personenbezug verneint werden soll, obwohl auch hier ein dem Versicherten zuzuordnender Kommunikationsinhalt vorliegt, nämlich der Versicherung ihm gegenüber. Vergleichbares hat das BVerwG bereits für schriftliche Anmerkungen von Prüfern zu den Ausführungen des Prüflings entschieden, die (auch) personenbezogene Daten des Prüflings darstellen, weil sie die Beurteilung seiner individuellen Leistung sowie seiner Kenntnisse und Kompetenzen – wiederum mit Folgen für seine Berufschancen – dokumentieren (BVerwG ZD 2023, 296 mAnm Viehweger/Koreng; Viehweger NJW 2023, 1079 Rn. 18). Dort ging es wohlgemerkt um eine juristische Staatsprüfung, bei der sich die Identität des Prüflings aus dem Prüfervotum selbst gar nicht ergab, sondern der Bezug zum Prüfling erst durch das Justizprüfungsamt unter Zuhilfenahme von Zusatzinformationen hergestellt werden konnte. Demgegenüber können sämtliche in einem Schreiben der Versicherung an den Versicherungsnehmer enthaltenen Informationen dem Versicherungsnehmer zwanglos schon dadurch unmittelbar zugeordnet werden, dass das betreffende Schreiben eben an ihn adressiert ist. Dass dies hier wohl der Fall war, lässt sich aus den tatsächlichen Feststellungen und aus Rn. 20 folgern, wonach dem Kl. die in Frage stehenden Unterlagen jedenfalls unstreitig einmal übermittelt worden sind. Dem Verantwortlichen ist zweifellos bekannt oder jedenfalls ohne Weiteres ermittelbar, welche Beitragsanpassungen ggü. welchen Versicherungsnehmern erfolgt sind und welche Tarifwechsel sowie Tarifbeendigungen individuell stattgefunden haben.

Daneben bleibt in der Entscheidung ein in der Rspr. des BGH in der Vergangenheit bereits aufgegriffener Aspekt gänzlich außen vor: Der Kl. hat hier eine Kopie nicht von bestimmten Dokumenten, sondern von personenbezogenen Daten verlangt. Unter welchen Voraussetzungen die Bekl. zur Erfüllung des Anspruchs Ablichtungen von Dokumenten übermitteln muss, ist in

der Rspr. des EuGH geklärt. Danach kann sich, um sicherzustellen, dass die so bereitgestellten Informationen leicht verständlich sind (Art. 12 Abs. 1 DS-GVO iVm Erwägungsgrund 58 DS-GVO), „die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u.a. personenbezogene Daten enthalten, die Gegenstand der Verarbeitung sind, als unerlässlich erweisen …, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten", EuGH ZD 2023, 539 Rn. 31 f., 41, 45. Den Betroffenen soll durch die Ausübung des in dieser Bestimmung vorgesehenen Auskunftsrechts ermöglicht werden, zu überprüfen, ob sie betreffende Daten richtig sind und in zulässiger Weise verarbeitet werden (EuGH ZD 2023, 539 Rn. 34). Die zur Verfügung zu stellende Kopie der personenbezogenen Daten muss daher alle Merkmale aufweisen, die es der betroffenen Person ermöglichen, ihre Rechte aus der DS-GVO wirksam auszuüben (EuGH ZD 2023, 539 Rn. 39).

Der IV. und der VI. Zivilsenat des BGH haben in der Vergangenheit die Auffassung vertreten, es sei Sache des Betroffenen, dazu vorzutragen, „dass die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten, sodass ausnahmsweise die Übermittlung einer Kopie" der geforderten Unterlagen nötig wäre (BGH Urt. v. 27.9.2023 – IV ZR 177/22; BGH ZD 2024, 392; BGH ZD 2024, 343 mAnm Viehweger).

Mit Blick auf die Kritik, die diese Rspr. erfahren hat (vgl. etwa Anm. Hense zu AG Chemnitz ZD 2025, 171), wäre eine Auseinandersetzung des I. Zivilsenats mit dieser Problematik wünschenswert gewesen. Womöglich hätte man schon mit Blick auf die Kontextualisierungspflicht dazu kommen müssen, dass der Versicherte Anspruch auf Ablichtungen seiner vollständigen Korrespondenz mit dem Versicherer hat.

BGH: Immaterieller Schaden wegen Datenleck bei Musikstreamingdienste-anbieter

DS-GVO Art. 5 Abs. 1 lit. c, lit. e, lit. f, Abs. 2, 28 Abs. 3 S. 2 lit. g, lit. h, 32, 82 Abs. 1
Urteil vom 11.11.2025 – VI ZR 396/24 (OLG Dresden, LG Dresden)

Leitsätze

1. Der Verantwortliche hat auch im Zusammenhang mit der Beendigung einer Auftragsverarbeitung den Schutz der Rechte der betroffenen Personen zu gewährleisten. Er hat sicherzustellen, dass – vorbehaltlich etwaiger gesetzlicher Speicherpflichten – keinerlei personenbezogene Daten mehr beim Auftragsverarbeiter verbleiben, die diesem vom Verantwortlichen zwecks Auftragserfüllung überlassen wurden. Er hat daher das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass es bei Auftragsende tatsächlich zur Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragsverarbeiter kommt.

2. Verbleiben personenbezogene Daten nach Beendigung des Auftrags beim Auftragsverarbeiter, werden sie dort abgegriffen und im Darknet zum Verkauf angeboten, stellt dies einen immateriellen Schaden iSv Art. 82 Abs. 1 DS-GVO dar. Ein solcher ist nicht allein deshalb ausgeschlossen, weil die Daten schon zuvor rechtswidrig abgegriffen worden sind.

Anm. d. Red.: Vgl. hierzu EuGH ZD 2025, 87; BGH ZD 2025, 162 mAnm Horn; EuGH ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel; EuGH ZD 2024, 381 mAnm Moos/Rothkegel = MMR 2024, 552 mAnm Halim; EuGH ZD 2025, 640 mAnm Mekat/Wellmann = MMR 2025, 950 mAnm Mekat/Ligocki und EuGH ZD 2024, 209 mAnm Schneider.

Sachverhalt

Der Kl. macht gegen die Bekl. Schadensersatz- und Feststellungsansprüche wegen behaupteter Verletzung der DS-GVO geltend.

Darknet
Auftragsverarbeiter
Vertragsbeendigung
Kontrollpflicht
Datenlöschung

Die Bekl., die ihren Sitz in Frankreich hat, betreibt den Online-Musikstreamingdienst D. Externer Auftragsverarbeiter der Bekl. war bis zum Auftragsende am 1.12.2019 das Unternehmen O. Am 30.11.2019 teilte dieses der Bekl. per Mail mit, deren Webseite und die dort befindlichen Daten („your site and all the data on the site") würden am Folgetag gelöscht. Dass dies auch tatsächlich geschehen sei, erklärte das Unternehmen O. erstmalig mit E-Mail v. 22.2.2023. Zuvor war bekannt geworden, dass unbekannte Hacker seit November 2022 Daten von Nutzern des Dienstes der Bekl. im Darknet zum Verkauf anboten. Die Datensätze stammten aus dem Jahr 2019. Sie waren von dem Unternehmen O. nicht, wie mit der Bekl. vereinbart, unmittelbar nach Auftragsende gelöscht worden, sondern von Mitarbeitern des Unternehmens O. von der Produktiv- in eine Testumgebung überführt worden und anschließend entweder von Hackern erbeutet oder von Mitarbeitern des Unternehmens O. unbefugt weitergegeben worden. Die Bekl. informierte die von dem Vorfall betroffenen Personen nach dessen Bekanntwerden.

Der Kl. ist Nutzer des Dienstes der Bekl. Seine Daten sind im Kundenprofil der Bekl. gespeichert. Der bei dem streitgegenständlichen Vorfall abgegriffene Datensatz enthielt Vor-, Nachname, Geschlecht, E-Mail-Adresse und Sprache des Kl. sowie das Registrierungsdatum.

Der Kl. verlangt die Leistung von immateriellem Schadensersatz, weil die Bekl. die nach der DS-GVO gebotenen technischen und organisatorischen Schutzmaßnahmen nicht ergriffen habe. Seit der Kenntnis über das Datenleck mache er sich Sorgen über den Verbleib und einen möglichen Missbrauch seiner Daten in Gestalt von Identitätsdiebstahl, Phishing, unzulässigen Werbeanrufen und Werbemails.

Das LG hat die Klage abgewiesen. Die Berufung des Kl. hat das OLG zurückgewiesen.

Aus den Gründen

9 B. Die Revision ist begründet.

10 I. Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen hält dessen Beurteilung, dem Kl. sei kein immaterieller Schaden iSv Art. 82 Abs. 1 DS-GVO entstanden, der revisionsrechtlichen Prüfung nicht stand. …

13 3. Nach stRspr des Gerichtshofs der Europäischen Union (im Folgenden: Gerichtshof) erfordert ein Schadensersatzanspruch iSd Art. 82 Abs. 1 DS-GVO einen Verstoß gegen die DS-GVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. nur EuGH Urt. v. 4.10.2024 – C-200/23 [= ZD 2025, 87] Rn. 140; weitere Nachweise in Senat Urt. v. 18.11.2024 – VI ZR 10/24 [= ZD 2025, 162 mAnm Horn] Rn. 21). …

14 a) Rechtlich nicht zu beanstanden ist die Beurteilung des Berufungsgerichts, dass die Bekl. bei Vorliegen eines Schadens

(dazu unten b) [= Rn. 24]) haftungsrechtlich dafür einzustehen hat, dass die Daten des Kl. bei dem Unternehmen O. nach Beendigung des Auftragsverarbeitungsverhältnisses nicht gelöscht wurden, sodass sie bei dem Unternehmen O. (durch Hacking oder infolge unbefugter Weitergabe durch Mitarbeiter des Unternehmens O.) abgegriffen und anschließend im Darknet zum Verkauf angeboten werden konnten. Dabei geht es nicht lediglich um einen Verstoß des Auftragsverarbeiters O. gegen die DS-GVO, für den die Bekl. – vorbehaltlich der Möglichkeit einer Exkulpation nach Art. 82 Abs. 3 DS-GVO – gem. Art. 82 Abs. 2 S. 1 DS-GVO einzustehen hat. Vielmehr liegt darüber hinaus ein eigener Verstoß der Bekl. gegen die DS-GVO vor, der, wie vom Berufungsgericht zutreffend gesehen, darin besteht, dass sie sich bei Beendigung des Vertrags mit ihrem Auftragsverarbeiter O. mit dessen Ankündigung einer Datenlöschung begnügte und nicht die Bestätigung einer erfolgten umfassenden Datenlöschung einholte (dazu aa) [= Rn. 15]). Wegen dieser eigenen schadensursächlichen Pflichtverletzung gelingt ihr eine Exkulpation nach Art. 82 Abs. 3 DS-GVO nicht (bb) [= Rn. 23]).

15 aa) Die Bekl. hat jedenfalls ihre Pflichten aus Art. 5 Abs. 2 DS-GVO iVm Art. 5 Abs. 1 lit. c, lit. e und lit. f DS-GVO sowie aus Art. 32 Abs. 1 DS-GVO verletzt.

16 (1) Überträgt ein Verantwortlicher iSv Art. 4 Nr. 7 DS-GVO die Datenverarbeitung auf einen Auftragsverarbeiter, kann er sich dadurch von seinen datenschutzrechtlichen Pflichten nicht befreien (Gabel/Lutz in Taeger/Gabel, DSGVO-BDSG-TTDSG, 4. Aufl., Art. 28 Rn. 2). Er bleibt „Herr der Verarbeitung" und daher ggü. der betroffenen Person für die Einhaltung der datenschutzrechtlichen Vorschriften bei der Verarbeitung ihrer Daten durch den Auftragsverarbeiter als seinem „verlängerten Arm" verantwortlich (Martini in Paal/Pauly, DS-GVO BDSG, 3. Aufl., Art. 28 Rn. 2; Bergt in Kühling/Buchner, DS-GVO BDSG, 4. Aufl., Art. 82 Rn. 55). Lediglich im Falle eines sog. Aufgaben- oder Auftragsverarbeiterexzesses, bei dem der Auftragsverarbeiter unter Verstoß gegen die DS-GVO selbst die Zwecke und Mittel der Verarbeitung bestimmt (Art. 28 Abs. 10 DS-GVO), wird dieser Verantwortlicher und der ursprüngliche Verantwortliche uU aus seiner Haftung entlassen (vgl. für den Fall einer Haftung nach Art. 83 DS-GVO EuGH ZD 2024, 209 [mAnm Schneider] Rn. 85). Das gilt u.a. dann, wenn der Auftragsverarbeiter Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche zugestimmt hätte (EuGH, aaO [= ZD 2024, 209 mAnm Schneider]). Auch in diesen Fällen kommt allerdings eine Haftung des Verantwortlichen in Betracht, wenn er es versäumt, mit den Mitteln des Vertragsrechts auf ein vertragskonformes Verhalten des Auftragsverarbeiters zu drängen (vgl. Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 28 Rn. 94).

17 Der Verantwortliche hat auch im Zusammenhang mit der Auftragsbeendigung den Schutz der Rechte der betroffenen Personen zu gewährleisten. Insoweit ist von Bedeutung, dass die Übermittlung von personenbezogenen Daten seitens des Verantwortlichen an den Auftragsverarbeiter einen Eingriff in die durch Art. 7 und 8 GRCh garantierten Rechte der betroffenen Personen auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellt, der nur so lange gerechtfertigt ist, als die Voraussetzungen der Auftragsverarbeitung vorliegen. Wenn aber das Auftragsverhältnis nicht mehr besteht, gibt es keine Rechtfertigung mehr dafür, dass sich die Daten noch beim Auftragsverarbeiter befinden (BeckOK Datenschutzrecht/Spoerr, 53. Ed., 1.8.2025, DS-GVO Art. 28 Rn. 78). Es ist daher auch und gerade durch den Verantwortlichen sicherzustellen, dass – vorbehaltlich etwaiger gesetzlicher Speicherpflichten – keinerlei personenbezogene Daten mehr beim Auftragsverarbeiter verbleiben, die diesem vom Verantwortlichen zwecks Auftragserfüllung überlassen wurden (BeckOK/Spoerr, aaO, Art. 28 Rn. 79; Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl., DS-GVO Art. 28 Rn. 78; Hartung in Kühling/Buchner, aaO, Art. 28 Rn. 77). Das Zugriffsrecht des Auftragsverarbeiters auf diese Daten entfällt mit dem Auftragsende, der Zugang zu ihnen muss ihm daher ab diesem Zeitpunkt verwehrt sein (Martini, aaO, Art. 28 Rn. 50). In Art. 28 Abs. 3 S. 2 lit. g DS-GVO ist dementsprechend geregelt, dass in dem Vertrag oder anderen Rechtsinstrument, auf dessen Grundlage die Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO zu erfolgen hat, vorzusehen ist, dass der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Ferner ist gem. Art. 28 Abs. 3 S. 2 lit. h DS-GVO vorzusehen, dass der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten, also auch der Löschungs- bzw. Rückgabepflicht, zur Verfügung stellt und Überprüfungen seitens des Verantwortlichen oder eines von diesem beauftragten Prüfers ermöglicht und dazu beiträgt.

18 Der Verantwortliche darf sich allerdings grds. nicht damit begnügen, mit dem Auftragsverarbeiter einen Vertrag abzuschließen, in dem diesem die vertragliche Verpflichtung zur Löschung der Daten und zum Nachweis der Löschung bei Auftragsbeendigung auferlegt wird. Er hat vielmehr bei Beendigung des Auftragsverhältnisses das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass der Auftragsverarbeiter seine vertragliche Verpflichtung erfüllt, die personenbezogenen Daten also tatsächlich nicht länger bei ihm gespeichert bleiben, sodass er tatsächlich keinen Zugriff mehr auf diese hat. Ob sich diese Pflicht aus Art. 28 DS-GVO ergibt, weil dessen Absatz 1 und Absatz 3 S. 2 lit. h bei verständiger Auslegung der Vorschrift eine Kontrollpflicht des Verantwortlichen impliziert (vgl. Gabel/Lutz, aaO, Art. 28 Rn. 27, 31; BeckOK/Spoerr, aaO, Art. 28 Rn. 35; Martini, aaO, Art. 28 Rn. 20; Hartung, aaO, Art. 28 Rn. 60), kann dahinstehen. Denn jedenfalls ergibt sie sich aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und insb. dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO), der den Zeitraum der Speicherung betrifft und dessen Ausfluss die Löschungs- bzw. Rückgabepflicht bei Beendigung des Auftragsverhältnisses ist (Martini, aaO, Art. 28 Rn. 50; Petri in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl., DS-GVO Art. 28 Rn. 78). Für die Einhaltung dieser Grundsätze ist der Verantwortliche gem. Art. 5 Abs. 2 DS-GVO „verantwortlich". Ferner ergibt sich seine Pflicht, sicherzustellen, dass dem Auftragsverarbeiter mit Beendigung des Auftrags der Zugang zu den personenbezogenen Daten der betroffenen Personen entzogen wird, aus der aus Art. 5 Abs. 2 DS-GVO iVm Art. 5 Abs. 1 lit. f DS-GVO und Art. 32 Abs. 1 DS-GVO folgenden Pflicht, eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. So hat der Verantwortliche gem. Art. 32 Abs. 1 DS-GVO unter Berücksichtigung u.a. Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Gem. Art. 32 Abs. 2 DS-GVO sind bei der Beurteilung des angemessenen

Schutzniveaus insb. die Risiken zu berücksichtigen, die mit der Datenverarbeitung verbunden sind, u.a. durch den unbefugten Zugang zu gespeicherten Daten. Das Risiko eines unbefugten Zugriffs auf die gespeicherten Daten besteht nicht erst bei einem Cyberangriff durch außenstehende Dritte, sondern schon dann, wenn die Daten nach Beendigung des Auftragsverhältnisses beim Auftragsverarbeiter gespeichert bleiben, obwohl dessen Zugriffsrecht mit der Beendigung des Auftrags erloschen ist. Dies hat der Verantwortliche durch geeignete Maßnahmen „so weit wie möglich" zu verhindern (zu dieser Einschränkung vgl. EuGH Urt. v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel] Rn. 30). Er hat daher das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass es bei Auftragsende tatsächlich zur Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragsverarbeiter kommt. Die Beweislast für die Geeignetheit seiner insoweit getroffenen Sicherheitsmaßnahmen liegt beim Verantwortlichen (vgl. EuGH, aaO [= ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel] Rn. 52, 56).

19 Hat der Verantwortliche diese ihm selbst obliegende Pflicht verletzt und insb. nicht auf ein vertragskonformes Verhalten des Auftragsverarbeiters hinsichtlich der Datenlöschung bzw. -rückgabe bei Auftragsende gedrängt, so kann er sich seiner Verantwortung hierfür nicht schon durch den Hinweis auf einen Aufgabenexzess entziehen, den der Auftragsverarbeiter dadurch begeht, dass er die Daten vertragswidrig behält und weiterverarbeitet. Für die Folgen seines eigenen Pflichtenverstoßes hat der Verantwortliche selbst einzustehen.

20 (2) Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen ist die Bekl. ihrer unter ((1) [= Rn. 16]) dargestellten Pflicht nicht nachgekommen. Sie hatte zwar vertragliche Regelungen mit dem Unternehmen O. getroffen, um den Vorgaben des Art. 28 Abs. 3 S. 2 lit. g und lit. h DS-GVO gerecht zu werden. Insb. hatte das Unternehmen O. nach Wahl der Bekl. entweder eine vollständige Kopie aller personenbezogenen Daten des Unternehmens der Bekl. an diese zurückzugeben und alle anderen Kopien zu löschen oder alle Daten sowie deren Kopien zu löschen; die Löschung hatte innerhalb von 21 Tagen nach Auftragsende zu erfolgen. Ferner hatte es der Bekl. schriftlich zu bestätigen, dass es (und seine Unterauftragsverarbeiter) die Rückgabe- bzw. Löschungspflicht innerhalb der Frist „vollständig eingehalten haben". Es kann dahinstehen, ob die Bekl. schon dadurch, dass sie das ihr vertraglich eingeräumte Wahlrecht nicht ausgeübt hat, eine Pflichtverletzung begangen hat, die für das spätere Abgreifen der Daten (mit-)ursächlich war. Denn jedenfalls hat sie ihre Pflicht, das ihrerseits nach den Umständen des vorliegenden Falls Erforderliche dazu beizutragen, dass sichergestellt ist, dass es bei Auftragsende tatsächlich zur Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragsverarbeiter kommt, dadurch verletzt, dass sie sich mit der Ankündigung des Unternehmens O., es werde am nächsten Tag die „Site" der Bekl. und alle Daten auf der „Site" löschen, begnügt hat. So entsprach die angekündigte Tätigkeit schon nicht der vertraglich geschuldeten und datenschutzrechtlich geforderten umfassenden Löschung auch aller Datenkopien. Deshalb und weil die vertraglich geschuldete schriftliche Bestätigung ausblieb, dass die Löschungspflichten „vollständig eingehalten" wurden, die Löschung sämtlicher Daten und Datenkopien also vollzogen war, hatte die Bekl. in ihrer Verantwortung für die personenbezogenen Daten ihrer Kunden unmittelbar nach Ablauf der 21-tägigen Frist die Bestätigung einzufordern. Die vom Berufungsgericht festgestellte Nachfrage der Bekl. bei O. erst im Jahr 2023 – also mehr als drei Jahre nach Beendigung des Auftrags und erst nach Bekanntwerden des Hacking-Vorfalls – war ersichtlich verspätet und konnte letzteren nicht mehr verhindern. ...

23 bb) Revisionsrechtlich nicht zu beanstanden ist die Beurteilung des Berufungsgerichts, dass sich die Bekl. nicht nach Art. 82 Abs. 3 DS-GVO – etwa unter Berufung auf ein weisungs- oder vertragswidriges Verhalten ihres Auftragsverarbeiters oder auf einen Hacking-Angriff durch unbefugte Dritte – entlasten kann. Eine Entlastung würde voraussetzen, dass die Bekl. nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, sie also keinerlei Verschulden trifft (Boehm in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl., DS-GVO, Art. 82 Rn. 24). Da ihr ein eigener (mindestens leicht) fahrlässiger Verstoß gegen die DS-GVO vorzuwerfen ist, müsste sie nachweisen, dass es keinerlei Kausalzusammenhang zwischen diesem Verstoß und dem dem Kl. entstandenen Schaden gibt (vgl. EuGH Urt. v. 11.4.2024 – C-741/21 [= ZD 2024, 381 mAnm Moos/Rothkegel = MMR 2024, 552 mAnm Halim] Rn. 51; v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel] Rn. 72). Dies ist ihr nicht gelungen. Die Beurteilung des Berufungsgerichts, es dürfe angenommen werden, dass das Unternehmen O. auf die gebotene Nachfrage der Bekl. bzgl. des Vollzugs der Löschung reagiert und die bei ihm noch vorhandenen Daten gelöscht hätte, ist revisionsrechtlich nicht zu beanstanden. Damit war die Pflichtverletzung der Bekl. mitursächlich dafür, dass personenbezogene Daten ihrer Kunden einschließlich des Kl. trotz Beendigung des Auftrags bei dem Unternehmen O. verblieben, dort von der Produktiv- in eine Testumgebung überführt wurden, entweder von Hackern erbeutet oder von Mitarbeitern des Unternehmens O. unbefugt weitergegeben und anschließend im Darknet zum Verkauf angeboten wurden.

24 b) Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen ist dessen Beurteilung, dem Kl. sei kein immaterieller Schaden iSv Art. 82 Abs. 1 DS-GVO entstanden, rechtsfehlerhaft. Nach den Feststellungen des Berufungsgerichts waren von dem Vorfall folgende personenbezogene Daten des Kl. betroffen: Vor- und Nachname, Geschlecht, E-Mail-Adresse, Sprache sowie sein Registrierungsdatum bei der Bekl. Der Kl. hat nicht nur die Kontrolle über diese Daten dadurch verloren, dass nach Beendigung der Auftragsverarbeitung das Unternehmen O. und Dritte (Hacker) unbefugten Zugriff auf die Daten hatten. Vielmehr ist es darüber hinaus anschließend zu einer missbräuchlichen Verwendung der Daten dadurch gekommen, dass sie im Darknet zum Verkauf angeboten wurden. Spätestens damit ist dem Kl. ein immaterieller Schaden entstanden. Ferner ist ein solcher Schaden durch die entgegen der Auffassung des Berufungsgerichts als begründet anzusehende Befürchtung des Kl. eingetreten, es könne zu einer (weiteren) missbräuchlichen Verwendung der im Darknet veröffentlichten Daten durch Versendung von Spam-Mails kommen.

25 aa) Der Begriff des „immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (stRspr, vgl. nur EuGH Urt. v. 4.9.2025 – C-655/23 [= ZD 2025, 640 mAnm Mekat/Wellmann = MMR 2025, 950 mAnm Mekat/Ligocki] Rn. 55; v. 4.10.2024 – C-200/23 [= ZD 2025, 87] Rn. 139 mwN; weitere Nachweise bei Senat Urt. v. 18.11.2024 – VI ZR 10/24 [= ZD 2025, 162 mAnm Horn] Rn. 28). Dabei soll nach Erwägungsgrund 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der DS-GVO reicht nach der Rspr. des Gerichts-

hofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – iSe eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich (stRspr, vgl. EuGH Urt. v. 4.9.2025 – C-655/23, aaO [= ZD 2025, 640 mAnm Mekat/Wellmann = MMR 2025, 950 mAnm Mekat/Ligocki] Rn. 56; v. 4.10.2024 – C-200/23, aaO [= ZD 2025, 87] Rn. 140 mwN; weitere Nachweise bei Senat Urt. v. 18.11.2024 – VI ZR 10/24, aaO [= ZD 2025, 162 mAnm Horn]).

26 Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DS-GVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat oder eine „Bagatellgrenze" überschreitet (EuGH Urt. v. 4.9.2025 – C-655/23, aaO [= ZD 2025, 640 mAnm Mekat/Wellmann = MMR 2025, 950 mAnm Mekat/Ligocki] Rn. 58; v. 4.10.2024 – C-200/23, aaO [= ZD 2025, 87] Rn. 149 mwN; weitere Nachweise bei Senat Urt. v. 18.11.2024 – VI ZR 10/24, aaO [= ZD 2025, 162 mAnm Horn] Rn. 29). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DS-GVO verpflichtet ist, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die DS-GVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden iSv Art. 82 dieser VO darstellen (vgl. EuGH Urt. v. 4.10.2024 – C-200/23, aaO [= ZD 2025, 87] Rn. 142; weitere Nachweise bei Senat Urt. v. 18.11.2024 – VI ZR 10/24, aaO [= ZD 2025, 162 mAnm Horn]). ...

39 (2) Die Beurteilung des Berufungsgerichts, die vom Kl. vorgetragene Befürchtung eines Datenmissbrauchs könne nicht als begründet angesehen werden, steht nicht in Einklang mit der Rspr. des Gerichtshofs.

40 Nach seinem vom Berufungsgericht festgestellten Vortrag befürchtet der Kl. aufgrund des streitgegenständlichen Vorfalls insb. den Erhalt von Spam-Mails mit auch betrügerischem Inhalt sowie einen Identitätsdiebstahl. Werden wie hier Name und E-Mail-Adresse einer natürlichen Person im Darknet zum Verkauf angeboten, so darf es als sehr wahrscheinlich angesehen werden, dass diese Daten dazu verwendet werden, Werbemails, aber auch Mails mit betrügerischem Inhalt an diese Person zu senden. Das stellt wohl auch das Berufungsgericht nicht in Frage. Ferner besteht die konkrete Gefahr, dass unter dem Namen der betroffenen Person und scheinbar von ihrem E-Mail-Account aus Mails mit betrügerischem Inhalt an Dritte geschickt werden. Schon mit der Versendung dieser Spam-Mails an den Kl. bzw. scheinbar von ihm als Absender an Dritte würden die Daten des Kl. (nach ihrer Veröffentlichung im Darknet ein weiteres Mal) missbräuchlich verwendet, sodass die Befürchtung eben dieser – objektiv naheliegenden – Verwendung als solche einen immateriellen Schaden darstellt, sofern diese Befürchtung samt ihrer negativen Folgen nachgewiesen ist. Darauf, welches Gefahrenpotenzial mit Spam-Mails verbunden ist, welche Vorsichtsmaßnahmen insoweit ergriffen werden können und wann solche Mails zu einem materiellen Schaden führen, kommt es entgegen der Auffassung des Berufungsgerichts für die Qualifizierung der Befürchtung als begründet hier nicht an. Da die missbräuchliche Datenverwendung nur befürchtet werden, aber nicht erfolgen muss, ist ferner unerheblich, ob der Kl. gerade infolge des streitgegenständlichen Vorfalls Spam-Mails erhalten hat oder erhalten wird. Mit den weiteren Erwägungen, es handle sich bei den gehackten Daten nicht um besonders sensible Daten, Spam-Mails würden auch andere Personen erhalten, deren Daten nicht gehackt worden seien, das Unwohlsein des Kl. gehe nicht über das hinaus, was alle sich im Internet bewegenden Privatpersonen beim Erhalt ungebetener Nachrichten erduldeten, zudem habe der Kl. nach Bekanntwerden des Vorfalls seine E-Mail-Adresse nicht geändert, hat das Berufungsgericht im Ergebnis eine Erheblichkeitsschwelle für die Annahme eines Schadens angenommen, die es nach der oben aufgezeigten Rspr. des Gerichtshofs nicht gibt. Diese Überlegungen können erst bei der Ermittlung der Schadenshöhe eine Rolle spielen (vgl. Senat Urt. v. 18.11.2024 – VI ZR 10/24 [= ZD 2025, 162 mAnm Horn] Rn. 99). Dabei wird allerdings zu berücksichtigen sein, dass die Befürchtung einer missbräuchlichen Datenverwendung und die damit verbundene Sorge stärker empfunden werden kann, wenn die betroffene Person positiv weiß, dass ihre Daten im Darknet zum Verkauf angeboten wurden.

41 Schließlich entzieht der Umstand, dass die Daten des Kl. der Webseite „haveibeenpwned.com" zufolge schon vor dem streitgegenständlichen Vorfall gehackt worden sein sollen, der Befürchtung, dass sie infolge des streitgegenständlichen Vorfalls erneut – von denselben oder anderen Personen – missbräuchlich verwendet werden, nicht die Grundlage. Insb. fehlt es entgegen der Ansicht der Revisionserwiderung nicht an der Kausalität zwischen dem streitgegenständlichen Verstoß und der Befürchtung als immateriellem Schaden. ...

Anmerkung

Professor Dr. Thomas Hoeren, ITM, Universität Münster

Die Entscheidung des BGH markiert einen weiteren, konsequenten Schritt in der Fortentwicklung des unionsrechtlich geprägten Schadensbegriffs des Art. 82 DS-GVO, wirft aber zugleich erhebliche Abgrenzungs- und Steuerungsfragen auf. Der Senat bestätigt seine inzwischen gefestigte Linie, wonach der immaterielle Schaden keinen Erheblichkeitsschwellenwert kennt und bereits in der konkreten Beeinträchtigung des Persönlichkeitsrechts durch den Kontrollverlust über personenbezogene Daten liegen kann. Damit wird die frühere, in der Instanzrechtsprechung verbreitete Tendenz zu einer faktischen Bagatellschwelle endgültig aufgegeben.

Kritisch zu hinterfragen ist allerdings, wie weit der vom Gericht angenommene Kontrollverlust tatsächlich trägt. Der BGH knüpft den Schadenseintritt maßgeblich an das objektive Bekanntwerden sensibler Nutzerdaten infolge eines Datenlecks und an die daraus resultierende abstrakte Gefährdungslage. Damit verschiebt sich der Schwerpunkt von einer konkret-individuellen Beeinträchtigung hin zu einer normativ geprägten Bewertung datenschutzrechtlicher Risiken. Die Gefahr liegt darin, dass der immaterielle Schaden zunehmend funktionalisiert wird, um Durchsetzungsdefizite des Datenschutzrechts zu kompensieren. Art. 82 DS-GVO droht so, zumindest partiell, eine pönale oder generalpräventive Funktion anzunehmen, die ihm systematisch fremd ist.

Zudem bleibt unklar, wie Gerichte künftig zwischen bloßer Unannehmlichkeit und ersatzfähigem immateriellen Schaden differenzieren sollen. Der BGH verweist zwar auf die Notwendigkeit einer individuellen Darlegung, senkt die Anforderungen an diese Darlegung jedoch faktisch erheblich ab. Für datenintensive Geschäftsmodelle, insb. im Plattform- und Streamingbereich, bedeutet dies ein kaum kalkulierbares Haftungsrisiko, das sich weniger aus der Schwere des einzelnen Eingriffs als aus der schieren Zahl potenziell betroffener Nutzer speist.

Schließlich stellt sich die Frage nach der Angemessenheit der zugesprochenen Beträge im Lichte der Verhältnismäßigkeit. Wenn bereits relativ geringfügige Datenlecks zu einem Anspruch auf

immateriellen Schadensersatz führen, ohne dass konkrete Folgebeeinträchtigungen nachgewiesen werden müssen, besteht die Gefahr einer Entwertung des Schadensbegriffs selbst. Die Entscheidung überzeugt damit in ihrer unionsrechtlichen Anschlussfähigkeit, lässt aber eine klarere dogmatische Konturierung des immateriellen Schadens vermissen und verlagert zentrale Abwägungsfragen in die – bislang wenig vorhersehbare – Höhe des zugesprochenen Betrags.

OLG Brandenburg: Vorrang des Anwaltsgeheimnisses vor dem Auskunftsanspruch

DS-GVO Art. 15, 23 Abs. 1; BDSG § 29 Abs. 1 S. 2; BRAO § 43a Abs. 2
Beschluss vom 5.11.2025 – 1 U 16/25 (LG Potsdam)

Leitsatz der Redaktion

Ein Anspruch auf Auskunft nach Maßgabe von Art. 15 DS-GVO gegen einen Berufsgeheimnisträger besteht nicht, wenn sich der iRe Mandatsverhältnisses zu sichernde Geheimnisschutz als vorrangig erweist, Art. 23 Abs. 1 DS-GVO iVm § 29 Abs. 1 S. 2 BDSG, § 43a Abs. 2 BRAO.

Anm. d. Red.: Vgl. hierzu auch ZD 2019, 483; EuGH ZD 2023, 271; EuGH ZD 2023, 601 und Brink/Joos ZD 2019, 483.

Aus den Gründen

1 Die Berufung gegen das Urteil des LG Potsdam v. 9.1.2025 – 2 O 10/22 ist gem. § 522 Abs. 2 ZPO zurückzuweisen, weil nach einstimmiger Auffassung des Senats das Rechtsmittel offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rspr. eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist. ...

Verschwiegenheitspflicht
Geheimnisschutz
Mandatsgeheimnis
Offenkundige Tatsachen

3 Der Kl. steht die begehrte Auskunft nach Maßgabe von § 15 DS-GVO nicht zu, da sich der iRe Mandatsverhältnisses zu sichernde Geheimnisschutz als vorrangig erweist, Art. 23 Abs. 1 DS-GVO iVm § 29 Abs. 1 S. 2 BDSG, § 43a Abs. 2 BRAO.

4 Die begehrte Auskunft unterfällt dem Anwaltsgeheimnis. Es ist weder ersichtlich, dass es sich um offenkundige Tatsachen handeln würde, noch handelt es sich um solche Tatsachen, die ihrer Bedeutung nach keiner Geheimhaltung bedürften. Der Umstand, dass sich die Bekl. – teilweise – auf eine „Selbstveröffentlichung" der Kl. beruft, lässt nicht den Schluss zu, die Klageforderung beziehe sich auf offenbarungspflichtige offenkundige Tatsachen. Offenkundiges lässt sich nicht mehr offenbaren. Die Frage der „Selbstveröffentlichung" ist iÜ zwischen den Parteien höchst streitig und die fehlende „Selbstveröffentlichung" Grundlage des klägerischen Auskunftsbegehrens. ...

Anmerkung

Prof. Dr. Behrang Raji, Of Counsel, BKP & Partner Rechtsanwälte

1. Verfahrensgang

Der Beschluss des OLG Brandenburg beleuchtet das Spannungsverhältnis zwischen dem Auskunftsanspruch nach Art. 15 DS-GVO und dem anwaltlichen Berufsgeheimnis gem. § 43a Abs. 2 BRAO iVm § 29 Abs. 1 S. 2 BDSG. Das LG Potsdam hatte die Klage abgewiesen; das OLG Brandenburg beabsichtigt, die Berufung durch Hinweisbeschluss nach § 522 Abs. 2 ZPO zurückzuweisen. Die Kl. konnte hierzu Stellung nehmen. Prozessual wird mit einem Hinweisbeschluss die Möglichkeit der mündlichen Verhandlung und weiterer Sachverhaltsaufklärung eingeschränkt, sodass die Anforderungen an eine erfolgreiche Berufung deutlich erhöht sind.

2. Anwaltsgeheimnis und § 29 BDSG

Das Gericht unterscheidet zutreffend zwischen den beiden Alternativen des § 29 Abs. 1 S. 2 BDSG. Es erkennt, dass bei Vorliegen einer spezialgesetzlichen Geheimhaltungspflicht (hier § 43a Abs. 2 BRAO) die erste Alternative eingreift, während die zweite Alternative auf überwiegende berechtigte Interessen des Betroffenen oder von Dritten abstellt.

Das Gericht sieht im vorliegenden Fall das Auskunftsrecht aus Art. 15 DS-GVO kategorisch ausgeschlossen. Die Bekl. hatte in ihrer Berufungserwiderung ausdrücklich vorgetragen, die „insoweit erforderliche Ermessensentscheidung" durchgeführt zu haben und sich auf eine Abwägung berufen. Das Gericht geht hierauf jedoch nicht ein, sondern stellt lediglich fest, die begehrte Auskunft unterfalle dem Anwaltsgeheimnis nach § 43a Abs. 2 BRAO, sodass ein Abwägungserfordernis nach § 29 Abs. 1 S. 2 BDSG nicht erforderlich ist.

Der Wortlaut der Norm verdeutlicht jedoch mit dem Wort „soweit", dass eine Einschränkung des Art. 15 DS-GVO nur dann in Betracht kommt, wenn hierdurch Informationen offenbart würden, die nach § 43a Abs. 2 BRAO geheim gehalten werden müssten. Es muss somit – wenn auch keine Abwägung – jedenfalls eine Bewertung im Einzelfall erfolgen, ob die in Rede stehenden Informationen dem Anwendungsbereich der spezialgesetzlichen Rechtsvorschrift unterfallen und deshalb tatsächlich geheimhaltungsbedürftig sind.

Das Anwaltsgeheimnis ist grundrechtlich abgesichert (Brink/Joos ZD 2019, 483 (488)). Die besondere Schutzwürdigkeit des anwaltlichen Berufsgeheimnisses nach Art. 7 GRCh und Art. 8 Abs. 1 EMRK gründet auf der Funktion der Rechtsanwaltschaft in einer demokratischen Gesellschaft, namentlich der Verteidigung der Rechtsunterworfenen (EuGH Urt. v. 8.12.2022 – C-694/20 Rn. 28; EGMR Urt. v. 6.12.2012 – 12323/11 – Michaud/Frankreich §§ 118 und 119). § 43a Abs. 2 BRAO wird durch § 2 BORA konkretisiert und stellt klar, dass das Gebot zur Verschwiegenheit zu den tragenden Säulen des Anwaltsberufs schlechthin zählt und die unerlässliche Basis des Vertrauensverhältnisses zwischen Rechtsanwalt und Mandant ist (Weyland/Bauckmann, 11. Aufl. 2024, BRAO, § 43a Rn. 12). Aus dieser Konkretisierung folgt, dass nicht jede im beruflichen Kontext anfallende Information automatisch auskunftsunfähig ist.

Das Gericht stellt überzeugend klar, dass § 29 Abs. 2 BDSG nicht anwendbar ist, der eine Interessenabwägung nur bei Informationspflichten nach Art. 13, 14 DS-GVO vorsieht. Das Gericht begründet die Nichtanwendbarkeit mit dem Argument, § 29 Abs. 2 BDSG betreffe nach dem Wortlaut Informationspflichten des Auftraggebers, nicht des Geheimnisträgers. Zudem betreffe § 29 Abs. 2 BDSG nicht den Umgang mit Informationen im Falle von Geheimhaltungspflichten, sondern Informationspflichten des Mandanten, für die eben keine Geheimhaltungspflicht gilt.

3. Unionsrechtliche Reichweite von § 43a Abs. 2 BRAO

Art. 23 Abs. 1 lit. i DS-GVO stellt die Öffnungsklausel dar, die den Mitgliedstaaten Beschränkungen der Betroffenenrechte erlaubt. Erwägungsgrund 4 S. 2 und S. 3 DS-GVO verdeutlicht, dass dabei praktische Konkordanz zwischen dem Datenschutz und anderen Grundrechten herzustellen ist – hier zwischen dem Datenschutz des Betroffenen und dem verfassungsrecht-

lich geschützten Anwaltsgeheimnis. Art. 23 Abs. 1 S. 2 DS-GVO garantiert dabei den Wesensgehalt der Betroffenenrechte.

Der nationale Gesetzgeber muss sich innerhalb des durch Art. 23 DS-GVO vorgegebenen Rahmens bewegen. Einschränkungen des Auskunftsrechts sind insoweit nur zulässig, soweit sie zum Schutz der Rechte und Freiheiten anderer Personen erforderlich sind. Gemeint sind die Rechte des Mandanten, insb. Vertraulichkeit, effektive Verteidigung und Vertrauensschutz.

§ 43a Abs. 2 BRAO erfasst jedoch „alles, was dem Anwalt in Ausübung seines Berufs bekannt wird". Dies schließt nach dem Wortlaut auch Datenverarbeitungen ohne Mandatsbezug ein, wodurch jedoch der Wesensgehalt des Auskunftsrechts ausgehöhlt werden würde. § 43a Abs. 2 BRAO ist somit auf mandatsbezogene Informationen teleologisch zu reduzieren, wenngleich im vorliegenden Verfahren wegen des eindeutigen Mandatsbezugs kein Anlass für das Gericht bestand, diesen Aspekt zu thematisieren. Aus dem weiten Wortlaut des § 43a Abs. 2 BRAO leitet das Gericht konsequent ab, dass sich die Verschwiegenheit auch auf Wissen erstreckt, das der Anwalt durch eigene Recherche erlangt hat.

4. Offenkundigkeit als Rückausnahme

§ 43a Abs. 2 S. 3 BRAO nimmt offenkundige Tatsachen explizit vom Geheimnisschutz aus. Offenkundige Informationen, also bereits öffentlich zugängliche oder allgemein bekannte Tatsachen, müssen beauskunftet werden, da sich offenkundige Informationen nicht mehr offenbaren lassen und Nicht-Geheimhaltungsbedürftiges keines Schutzes mehr bedarf (Weyland/Bauckmann, 11. Aufl. 2024, BRAO § 43a Rn. 17). Offenkundig sind Tatsachen, die allgemein bekannt oder ohne Weiteres aus allgemein zugänglichen Quellen feststellbar sind (Zöller, ZPO/Greger 35. Aufl., § 291 Rn. 1b). Das Gericht setzt sich mit dieser Ausnahme nicht differenziert auseinander und verweist lediglich darauf, dass zwischen den Parteien Streit über die Tatsachen bestehe. Die Rückausnahme liefe jedoch leer, wenn für die Anwendung dieser Ausnahme unstreitige Tatsachen erforderlich wären. Die Offenkundigkeit ist vielmehr objektiv zu bestimmen. Entscheidend ist, ob die Informationen für jedermann ohne Weiteres zugänglich oder allgemein bekannt sind, nicht, ob eine Partei dies bestreitet.

5. Wesensgehalt des Auskunftsanspruchs

Bei dem Auskunftsrecht nach Art. 15 DS-GVO handelt es sich um ein zentrales Auskunftsrecht, das die Transparenz der Art und Weise der Verarbeitung personenbezogener Daten ggü. der betroffenen Person gewährleisten soll (EuGH ZD 2023, 271 Rn. 42; EuGH ZD 2023, 601 Rn. 59). Das grundrechtlich in Art. 8 Abs. 2 GRCh abgesicherte Recht ist insoweit ein Kernelement des europäischen Datenschutzrechts. Vor diesem Hintergrund müssen Einschränkungen verhältnismäßig sein und dürfen den Wesensgehalt des Rechts nicht antasten, Art. 23 Abs. 1 S. 2 DS-GVO. Das vorliegende Verfahren gibt Anlass zu zweifeln, ob wegen der Reichweite des § 43a Abs. 2 BRAO das „soweit" in § 29 Abs. 1 S. 2 BDSG sowie die Rückausnahme der Offenkundigkeit in § 43a Abs. 2 S. 3 BRAO als Korrektive ausreichen, um den Wesensgehalt des Auskunftsrechts zu wahren.

Im vorliegenden Verfahren war der Ausschluss des Auskunftsanspruchs nachvollziehbar, weil die Auskunft über Beweismittel und Prozessstrategie tatsächlich das Vertrauensverhältnis und die Verteidigungsposition des Mandanten gefährdet hätte. Das Gericht musste jedoch nicht entscheiden, wie weit die Rückausnahme der Offenkundigkeit reicht oder ob § 43a Abs. 2 BRAO unionsrechtlich insgesamt Bestand hat. Der Gesetzgeber sollte konkretisierend klarstellen, dass sich § 43a Abs. 2 BRAO nur auf mandatsbezogene Informationen erstreckt.

LG München I: Kein Schadensersatzanspruch für Drittland-Datentransfer

DS-GVO Art. 46, 49 Abs. 1 lit. c, 82; BGB § 242
Urteil vom 27.8.2025 – 33 O 635/25; nicht rechtskräftig

Leitsätze der Redaktion

1. Die Übermittlung personenbezogener Daten in die USA kann auf Art. 46 Abs. 1 DS-GVO gestützt werden, wenn – wie hier – davon auszugehen ist, dass auch in den USA dem Betroffenen wirksame Rechtsbehelfe zur Durchsetzung seiner Rechte zur Verfügung stehen. Neben einer zivilrechtlichen Klage gegen den Mutterkonzern (hier: Meta Platforms Inc.) des Verantwortlichen, soweit dieser aus Sicht des Betroffenen Daten unrechtmäßig verarbeitet, steht dem Betroffenen auch die Möglichkeit offen, die US-amerikanischen Datenschutzbehörden einzuschalten.
2. Das abstrakte Risiko eines Datenzugriffs von US-Behörden ist Folge der politischen Entwicklung in den USA, nicht des Speicherorts der Daten und begründet daher mangels Kausalität keinen Schaden.
3. Es erscheint mit dem Gebot von Treu und Glauben nicht zu vereinbaren, einerseits in Kenntnis des behaupteten Rechtsverstoßes den Dienst des Verantwortlichen (mit dem bekannten Datenübertrag in die USA) zu nutzen, andererseits aber diesen gerade für das Anbieten des Dienstes auf Schadensersatz in Anspruch nehmen zu wollen.

Anm. d. Red.: Vgl. hierzu auch LG Bonn ZD 2026, 106 mAnm Hoeren und EuGH ZD 2020, 511 mAnm Moos/Rothkegel = MMR 2020, 597 mAnm Hoeren – Schrems II.

Sachverhalt

Der Kl. nimmt die Bekl. u.a. auf Schadensersatz aus Verstößen gegen die DS-GVO aufgrund der Übermittlung von Daten in die USA in Anspruch.

Soziales Netzwerk
Standardvertragsklauseln
Immaterieller Schaden
Kausalität
Treu und Glauben

Die Bekl. ist eine Gesellschaft mit Sitz in Irland, ihre Konzernmuttergesellschaft, die M. Platforms Inc., hat ihren Sitz in den USA. Die Bekl. betreibt insb. die sozialen Netzwerke F. und I. in Europa, der Mutterkonzern bietet solche Dienste auch im Rest der Welt an. Bei F. handelt es sich um einen globalen Online-Dienst für Kommunikation und das Teilen von Inhalten, der es den Nutzern ermöglichen soll, mit anderen Nutzern auf der ganzen Welt auf vielfältige Weise in Kontakt zu treten und Inhalte auf verschiedene Arten zu teilen. Der Kl. unterhielt auf F. ein Nutzerprofil. Er nutzte die angebotenen Kommunikationsdienste von F. jedenfalls bis in das Jahr 2024.

Die Bekl. überträgt routinemäßig verschiedene Arten von Daten in die USA, dazu gehören EU-Benutzerdaten, die nicht ohnehin öffentlich einsehbar sind. Am 16.7.2020 erklärte der EuGH in der Rs. C-311/18 (= ZD 2020, 511 mAnm Moos/Rothkegel = MMR 2020, 597 mAnm Hoeren – Schrems II) das sog. Privacy Shield für ungültig.

Am 11.7.2023 trat mit dem EU-US Data Privacy Framework ein neues Datenschutzabkommen zwischen der EU und den USA in Kraft. Seit diesem Zeitpunkt stützt die Bekl. den Datentransfer in die USA auf dieses Abkommen. Der Kl. behauptet, die Bekl. habe seit 16.7.2020 bis 2023 jahrelang wissentlich gegen die DS-GVO verstoßen, um Profit zu machen. Sie übertrage Verhaltensdaten, Geräteinformationen und werbungsbezogene Daten in die USA. Die Bekl. mache personenbezogene Daten ihrer Nutzer Dritten, insb. den amerikanischen Ermittlungsbehörden, vorsätzlich zugänglich.

Aus den Gründen

36 Soweit die Klage zulässig ist, erweist sie sich als vollumfänglich unbegründet.

37 I. Dem Kl. steht kein Anspruch auf Zahlung eines Betrags von 3.000 EUR oder einer niedrigeren Summe nach Art. 82 DS-GVO zu.

38 1. Bereits im Ausgangspunkt steht dem Kl. kein Schadensersatzanspruch zu, weil die Übertragung der Daten des Kl. in die USA entgegen der Rechtsauffassung des Kl. auch in der Zeit vom 16.7.2020 bis zum 11.7.2023 nicht rechtswidrig war.

39 a) Die Bekl. konnte sich für den Datenübertrag auf Art. 46 Abs. 1 DS-GVO stützen. Zwischen der Bekl. und ihrem Mutterkonzern waren Standarddatenschutzklauseln vereinbart, die unter Art. 46 Abs. 2 lit. c DS-GVO fallen. Solche ausreichenden Standardvertragsklauseln stellen nach Art. 46 DS-GVO unter den dort genannten Bedingungen ausreichende Garantien des Verantwortlichen bzw. des Auftragsdatenverarbeiters dar. Es ist davon auszugehen, dass auch in den USA dem Betroffenen wirksame Rechtsbehelfe zur Durchsetzung seiner Rechte zur Verfügung stehen. Neben einer zivilrechtlichen Klage gegen den Mutterkonzern der Bekl., soweit dieser aus Sicht des Kl. Daten unrechtmäßig verarbeitete, steht dem Kl. auch die Möglichkeit offen, die US-amerikanischen Datenschutzbehörden einzuschalten.

40 b) Zuletzt konnte sich die Bekl. für die Datenübermittlung auch [auf] Art. 49 Abs. 1 lit. c DS-GVO stützen …

43 2. Darüber hinaus vermochte der Kl. ein ihm durch den Datenübertrag in die USA entstandenen Schaden auch nicht zur Überzeugung des Gerichts darzulegen …

45 In seiner informatorischen Anhörung legte der Kl. dem Gericht umfangreiche, auch körperliche, Beeinträchtigungen aufgrund seiner Kenntnis eines Datenübertrags seitens der Bekl. in die USA dar. Auf Nachfrage des Gerichts, weil es dem Gericht nur schwer nachvollziehbar erschien, dass ein Nutzer von F. vom Datenübertrag erst 2024 Kenntnis erlangt haben soll, erläuterte der Kl. seine Beeinträchtigungen weiter dahingehend, dass für ihn vor allem belastend sei die Kenntnis, dass auch Dritte in den USA Kenntnis von seiner Kommunikation erlangen könnten.

46 Für das Gericht ist im Grundsatz noch verständlich, dass sich Nutzer der Bekl. Sorgen machen wegen eines Zugriffs etwa der US-Geheimdienste oder der Grenzbehörden der USA auf ihre Posts etc. auf der Kommunikationsplattform der Bekl. Diesen Punkt vermag das Gericht dem Kl. zu glauben, der auch anschaulich seine Ängste beschrieb. Zumindest sehr ungewöhnlich erscheinen dem Gericht allerdings die geklagten auch körperlichen Beeinträchtigungen des Kl. in Kenntnis des Datenübertrags bzw. eines Zugriffs von US-Behörden hierauf. Es handelt sich nach Einschätzung des Gerichts zunächst einmal um ein abstraktes Risiko, allzumal ein konkreter Schaden (etwa gegen ihn bisher eingeleitete Maßnahmen der US-Behörden) vom Kl. nicht angegeben wurde. Hierauf gleich mit körperlichen Beschwerden wie Schlaflosigkeit zu reagieren, erscheint dem Gericht zumindest sehr ungewöhnlich.

47 Letztlich scheidet ein Schaden des Kl., die vom Kl. genannten Beeinträchtigungen für einmal als zutreffend unterstellt, aber an der fehlenden Kausalität der Datenübertragung seitens der Bekl. in die USA hierfür: Es kann zwar ohne Weiteres Medienberichten entnommen werden, dass die USA seit Amtseinführung der Trump II-Adminstration eine verschärfte Politik ggü. Einwanderern (darunter auch Einwanderern, die über legale Kanäle ins Land kommen wollen wie zB für Studien- oder Forschungsaufenthalte) ergriffen haben. Des Weiteren ist auch zutreffend, dass die US-amerikanischen Grenzbehörden nach Medienberichten ein verschärftes Vorgehen ggü. Personen, die (auch nur kurzfristig) in die USA einreisen wollen, an den Tag legen. Hier sollen nach Medienberichten auch in sozialen Medien gepostete Inhalte von Relevanz sein. Allerdings ist dieses Vorgehen unabhängig vom Datenübertrag seitens der Bekl. in die USA. Es ist schlichtweg eine Folge einer massiv geänderten Politik der USA ggü. Einwanderern und sonstigen Ausländern. Für dieses Vorgehen spielt jedoch der Datenübertrag in die USA keine Rolle. Selbst wenn die Bekl. einen solchen Datenübertrag nicht vornehmen sollte, könnten sich die US-amerikanischen Behörden die geposteten Inhalte anzeigen lassen, etwa in dem sie selber F.-Profile unterhalten oder Einwanderungs- sowie Einreisewillige dazu zwingen, ihnen den Zugang zu Profilen in den sozialen Medien zu eröffnen. Letzteres ist nach Medienberichten bereits vorgekommen und völlig unabhängig vom Speicherort der F.-Kommunikation des Kl. Das Gericht kann zwar ohne Weiteres nachfühlen, dass dies insb. für Personen, die sich zur Zeit für eine Reise in die USA bzw. einen Aufenthalt dort interessieren (wie vom Kl. angegeben) sehr unangenehm und bedrohlich ist. Dies ist aber eine Folge der politischen Entwicklung in den USA, nicht des Speicherorts der Daten. Hinzu tritt, dass – sollte der Kl. tatsächlich eine solche Vorstellung gehabt haben – es schon immer eine unrealistische Annahme war, dass Dritte auf die von der Bekl. gespeicherten Daten ihrer Nutzer nie zugreifen könnten. Ein solcher Zugriff war schon lange und auch in Deutschland nach den einschlägigen gesetzlichen Bestimmungen möglich, etwa für Staatsanwaltschaften und Gerichte iRv Strafverfolgungsmaßnahmen nach der StPO und für den Verfassungsschutz nach den für die jeweilige Behörde geltenden Vorschriften. Ähnliche Möglichkeiten bestehen, wie von den Parteien dargelegt, für die US-amerikanischen Dienste. Und auch die anderen EU-Staaten werden im Rahmen vergleichbarer Regeln wie der deutschen auf bei F. vorhandene Daten zugreifen können – rechtlich ist das unabhängig vom Speicherort. Neu ist insoweit allenfalls die Bereitschaft US-amerikanischer Behörden und Dienste, hiervon massiv Gebrauch zu machen (und hierbei bestehende gesetzliche Schranken sehr eng zu sehen bzw. die Befugnisse sehr weit) und die gewonnenen Erkenntnisse dann auch zum Zwecke politischer Differenzierung auch hinsichtlich von Äußerungen zu verwenden, die auch nach dem US-Recht ohne Weiteres zulässig wären. Auch diese geänderte Politik der US-Behörden ist aber eine Folge der allgemein geänderten politischen Verhältnisse in den USA, nicht aber des Speicherorts der Daten der Bekl.

48 3. Zuletzt besteht auch kein Schadensersatzanspruch des Kl. gegen die Bekl., weil dessen Geltendmachung gegen das Gebot von Treu und Glauben verstößt (§ 242 BGB). Der Kl. verlangt von der Bekl. Schadensersatz für eine Datenübertragung in die USA. Es ist jedoch allgemein bekannt – und war nach Überzeugung des Gerichts auch dem Kl. bekannt – dass die Bekl. einen Dienst zur weltweiten Kommunikation anbietet und Tochter eines US-amerikanischen Unternehmens ist. Schon allein, um die Dienste der Bekl. weltweit anbieten zu können, ist es offensichtlich erforderlich, Daten aus der EU in das Nicht-EU-Ausland zu übertragen. Nach Überzeugung des Gerichts war auch den Nutzern der Dienste der Bekl. für den hier gegenständlichen Zeitraum bewusst, dass ihre Daten auch in die USA übertragen werden. Über die entsprechende Datenübertragung wurde schon vor dem Privacy-Shield-Urteil des EuGH öffentlich berichtet. Spätestens aber anlässlich der Schrems-II-Entscheidung wurde öffentlich breit über den Transfer von Daten seitens der Bekl. berichtet. Auch die Frage eines Zugriffs US-amerikanischer Behörden auf Daten ist bereits infolge der Snowden-Berichterstattung allgemein bekannt. Dennoch hat der Kl. die Dienste der Bekl. benutzt. Es erscheint mit dem Gebot von Treu und Glauben nicht zu vereinbaren, einerseits in Kenntnis des behaupteten Rechts-

verstoßes den Dienst der Bekl. (mit dem bekannten Datenübertrag in die USA) zu nutzen, andererseits aber die Bekl. gerade für das Anbieten des Dienstes auf Schadensersatz in Anspruch nehmen zu wollen.

49 Aus Sicht des Gerichts zeigt die vorliegende Klage, dass es dem Kl. nicht um den Ersatz tatsächlich erlittener Schäden geht, sondern er einen ihn tatsächlich nur eingeschränkt betreffenden Vorgang (die Datenübertragung in die USA) nutzen will, um hierfür eine Geldentschädigung zu erlangen. Fühlte sich der Kl. tatsächlich so schwer beeinträchtigt durch den Datentransfer in die USA, so hätte es sich angeboten, nicht nur F. schon ursprünglich nicht zu nutzen, jedenfalls aber die Nutzung zu stoppen (letzteres gibt der Kl. auch an), sondern ebenso die Nutzung des Dienstes I., der ebenfalls von der Bekl. betrieben wird und bei dem sich mutmaßlich ein ähnliches Problem wie bei F. ergibt. Die Geltendmachung von Schadensersatz ohne tatsächlich erlittene Schäden kann ebenso wenig Sinn und Zweck eines Anspruchs aus Art. 82 DS-GVO sein wie die massenhafte Geltendmachung von Schadensersatz- und weiteren Ansprüchen durch die Prozessbevollmächtigten des Kl. durch weitgehend aus Textbausteinen bestehende Klagen, um durch diese Klagen und ggf. noch weiter zu führende Rechtsmittelverfahren ein hohes Maß an Gebühren für die Rechtsanwälte zu generieren, wobei es dabei sogar unerheblich ist, wie diese Verfahren im Ergebnis ausgehen. ...

AG Düsseldorf: Googlen eines Bewerbers im arbeitsgerichtlichen Verfahren

DS-GVO Art. 4 Nr. 2, 6 Abs. 1 S. 1 lit. f, 14, 82 Abs. 1
Urteil vom 19.8.2025 – 42 C 61/25; rechtskräftig

Leitsätze der Redaktion

1. Die Google-Recherche einer betroffenen Person stellt eine Datenverarbeitung iSd Art. 4 Nr. 2 DS-GVO dar.
2. Die betroffene Person ist unmittelbar nach Durchführung der Recherche über die Kategorien der erhobenen personenbezogenen Daten iSd Art. 14 Abs. 1 lit. d DS-GVO zu informieren.

Anm. d. Red.: Vgl. hierzu BAG ZD 2026, 226 – in diesem Heft; LAG Düsseldorf ZD 2024, 590; EuGH ZD 2023, 446 mAnm Mekat/Ligocki; EuGH ZD 2024, 208 und EuGH ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel.

Sachverhalt

Die Bekl. suchte im August 2023 einen Sachbearbeiter für die Bereiche Kreditmanagement und Forderungsmanagement. Der Kl. bewarb sich auf diese ausgeschriebene Stelle. Im Zuge eines Verfahrens vor dem AG Berlin (Az. 2 Ca 12410/23) berief sich die Bekl. u.a. auf Recherchen über den Kl., die sie im Internet vorgenommen hatte. Zuvor hatte der Kl. hierüber keine Kenntnis. In einem Schriftsatz der Bekl. waren Screenshots aus einer Internetrecherche betreffend den Kl. beigefügt. Der Kl. ist der Auffassung: Die Bekl. habe dadurch, dass sie den Kl. nicht umgehend über die erfolgte Internetrecherche informiert habe, gegen die DS-GVO verstoßen.

Internetrecherche
Datenverarbeitung
Informationspflicht
Immaterieller Schaden
Kontrollverlust

Aus den Gründen

16 Die Klage ist teilweise begründet.

17 Dem Kl. steht ggü. der Bekl. ein Zahlungsanspruch iHv 250 EUR aus Art. 82 Abs. 1 DS-GVO zu.

18 Die Internetrecherche der Bekl. stellt bereits eine Datenverarbeitung iSd Art. 4 Nr. 2 DS-GVO dar (vgl. LAG Düsseldorf Urt. v. 10.4.2024 – 12 Sa 1007/23 [= ZD 2024, 590]).

19 Das Gericht erachtet dabei die Datenerhebung als solche im konkreten Fall trotz der fehlenden Einwilligung des Kl. (Art. 6 Abs. 1 S. 1 lit. a DS-GVO) für rechtmäßig.

20 Grundlage für die Datenerhebung ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

21 Art. 6 Abs. 1 S. 1 lit. f DS-GVO erlaubt die Verarbeitung von Daten, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

22 Die Bekl. hat vorliegend den Namen des Kl. im Zusammenhang mit einem gerichtlichen Verfahren als Bekl. „gegoogelt", um Erkenntnisse über dessen Person zu erlangen.

23 Das Gericht hält eine solche Maßnahme iRe Rechtsverteidigung zumindest im vorliegenden Fall für sinnvoll und erforderlich, zumal vorliegend die Bekl. hierdurch Erkenntnisse erlangt hat, die möglicherweise für den Ausgang des Verfahrens von Bedeutung sein würden.

24 Dem stehen überwiegende Interessen des Kl. nicht entgegen. Es handelt sich bei den Erkenntnissen aus einer Google-Recherche um solche aus allgemein zugänglichen Quellen. Sofern sich dort abwertende Kommentare oder Beiträge über den Kl. befinden, führt dies nicht zu einem überwiegenden Interesse desselben.

25 Zum einen ist dem Nutzer einer entsprechenden Erkenntnisquelle vorab nicht bekannt, zu welchen Ergebnissen die Recherche führt. Außerdem hat er keinen Einfluss auf den Inhalt.

26 Dies bedeutet allerdings nicht, dass die Recherche im Geheimen ablaufen darf. Weiterer Schutzmechanismus sind die Informationspflichten aus Art. 14 DS-GVO (LAG Düsseldorf, aaO [= ZD 2024, 590] unter Hinweis auf Solmecke in Hoeren/Sieber/Holznagel, HdB Multimediarecht, 60. EL Oktober 2023, Teil 21.1 Social Media Rn. 64).

27 Die Bekl. ist der Informationspflicht aus Art. 14 DS-GVO nicht nachgekommen. Die Bekl. hat dem Kl. nicht die Kategorien der personenbezogenen Daten iSd Art. 14 Abs. 1 lit. d DS-GVO, die sie verarbeitet hat, mitgeteilt. Dabei kann dahingestellt bleiben, ob die Bekl. erstmals in dem hier in Rede stehenden Verfahren vor dem ArbG die Recherche vorgenommen hat. Selbst wenn dies der Fall wäre, wäre es nach Auffassung des Gerichts nicht ausreichend, dass die Mitteilung in einem Schriftsatz, der sich in erster Linie an das Gericht richtet, erfolgt. Vielmehr hätte dies unmittelbar ggü. dem Kl. erfolgen müssen, und zwar unmittelbar nach der Durchführung der Recherche.

28 Der Kl. hat durch die nicht erfolgte Information gem. Art. 14 Abs. 1 lit. d DS-GVO auch einen immateriellen Schaden erlitten.

29 Ein Anspruch auf Ersatz des immateriellen Schadens des Kl. scheidet nicht deshalb aus, weil es hier um einen bloßen Verstoß gegen die Bestimmungen der DS-GVO geht, der alleine nicht zur Begründung des Schadensersatzes ausreicht.

30 Der bloße Verstoß gegen die Bestimmungen dieser Verordnung reicht zwar nicht aus, um einen immateriellen Schadensersatzanspruch zu begründen. Die betroffene Person hat nachzuweisen, dass der Verstoß gegen die DS-GVO für sie negative Folgen gehabt hat, welche einen immateriellen Schaden darstellen. Dabei ist aber nicht Voraussetzung, dass der der betroffenen Person entstandene immaterielle Schaden einen be-

stimmten Grad an Erheblichkeit erreicht hat (EuGH v. 4.5.2023 – C-300/21 [= ZD 2023, 446 mAnm Mekat/Ligocki] Rn. 43 ff., 50, 51). Der Nachteil muss weder spürbar noch die Beeinträchtigung „objektiv" sein. Diese Auslegung ergibt sich aus der dritten Seite des 146. Erwägungsgrund DS-GVO, in dem es heißt, dass „(d)er Begriff des Schadens ... im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden (sollte), die den Zielen dieser Verordnung in vollem Umfang entspricht". Dies steht mit den Zielen der DS-GVO im Einklang, namentlich demjenigen, innerhalb der Union ein gleichmäßiges und hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. LAG Düsseldorf, aaO [= ZD 2024, 590] unter Hinweis auf EuGH v. 14.12.2023 – C-456/22 [= ZD 2024, 208] Rn. 20).

31 Dabei hat der EuGH klargestellt, dass der Unionsgesetzgeber unter den Schadensbegriff insb. auch den bloßen „Verlust der Kontrolle" über die eigenen Daten infolge eines Verstoßes gegen die DS-GVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte. Zur Begründung hat er auf der ersten Seite des 85. Erwägungsgrund DS-GVO verwiesen. Dort wird in einer beispielhaften Aufzählung von möglichen materiellen oder immateriellen Schäden explizit der Verlust der Kontrolle über die eigenen personenbezogenen Daten genannt (vgl. LAG Düsseldorf, aaO [= ZD 2024, 590] unter Hinweis auf EuGH v. 14.12.2023 – C-340/21 [= ZD 2024, 150 mAnm Ligocki/Sosna = MMR 2024, 231 mAnm Kohl/Rothkegel] Rn. 74–86).

32 Bei der Bemessung des immateriellen Schadensersatzanspruchs ist als einem wichtigen Faktor auf die Intensität der Persönlichkeitsrechtsverletzung abzustellen (LAG Düsseldorf, aaO [= ZD 2024, 590]).

33 In den „gegoogelten" Beiträgen wird dem Kl. ... unterstellt ... Die Datenverarbeitung betraf dementsprechend deutlich negative Werturteile mit Tatsachenkern. Dies beeinträchtigt den Kl. in seinem allgemeinen Persönlichkeitsrecht. Es liegt insoweit auch ein Kontrollverlust auf Seiten des Kl. vor.

34 Das Gericht hält vorliegend allerdings lediglich einen immateriellen Schadensersatz von 250 EUR für angemessen.

35 Ausschlaggebend hierfür ist Folgendes:

36 Das LAG Düsseldorf, aaO [= ZD 2024, 590] hat in dem von ihm zu entscheidenden Fall einen immateriellen Schadensersatzanspruch von 1.000 EUR zugesprochen. Dem lag allerdings zugrunde, dass das Ergebnis einer Google-Recherche, nämlich eine nicht rechtskräftige Verurteilung eines Bewerbers wegen gewerbsmäßigen Betrugs im Zusammenhang mit vermeintlichen Scheinbewerbungen auf diverse ausgeschriebene Arbeitsstellen zum Zwecke der Gewinnerzielung durch die Geltendmachung von Schadensersatzansprüchen wegen Verstößen gegen die DS-GVO und andere Vorschriften. Dementsprechend hatte die Recherche unmittelbaren (Mit-)Einfluss auf das Ergebnis eines Bewerbungsverfahrens.

37 Im vorliegenden Fall ist demgegenüber die Recherche während eines laufenden Rechtsstreits zur Wahrnehmung berechtigter Interessen, nämlich zur Verteidigung gegen einen geltend gemachten Schadensersatzanspruch erfolgt.

38 Die Recherche hatte dementsprechend für den Kl. anders als in dem o.g. Rechtsstreit keine Außenwirkung außerhalb des Rechtsstreits.

39 Vor diesem Hintergrund ist die immaterielle Beeinträchtigung des Kl. als wesentlich geringer zu bewerten.

40 Außerdem ist nach Auffassung des Gerichts zu berücksichtigen, dass der Kl. nach eigenen Angaben bereits eine Vielzahl von vergleichbaren Verfahren, die ungefähr zu beziffern er sich im Verhandlungstermin weigerte, geführt hat.

41 Unter diesen Umständen dürfte ein Datenschutzverstoß für ihn eine wesentlich geringere Strahlkraft haben als bei einem Durchschnitts-Gegoogeltem.

42 Unter diesen Umständen erscheint eine Entschädigung von 250 EUR als ausreichend.

43 Dem Anspruch steht im konkreten Fall der Einwand des Rechtsmissbrauchs nicht entgegen. Selbst wenn der Kl. sich rechtsmissbräuchlich beworben haben sollte, ändert dies nichts daran, dass es der Bekl. verwehrt war, über ihn unter Verstoß gegen die DS-GVO Daten zu erheben. ...

BAG: Entschädigung wegen Google-Recherche in Bewerbungsverfahren

DS-GVO Art. 82 Abs. 1; GG Art. 33 Abs. 2; ZPO § 287
Urteil vom 5.6.2025 – 8 AZR 117/24 (LAG Düsseldorf, ArbG Düsseldorf)

Leitsätze der Redaktion

1. Der maßgebliche Charakter des Entschädigungsanspruchs als Anspruch auf Ausgleich eines tatsächlich erlittenen Schadens ist nicht davon abhängig, ob Regelungen im nationalen Recht wegen eines Verstoßes gegen die DS-GVO die Verhängung eines Bußgelds gegen den Verantwortlichen ermöglichen oder nicht.

2. Hat ein Verantwortlicher im Rahmen desselben Verarbeitungsvorgangs mehrere Verstöße gegenüber derselben Person begangen, kann dies nicht als relevantes Kriterium für die Bemessung des der betroffenen Person gem. Art. 82 DS-GVO zu gewährenden Schadensersatzes herangezogen werden. Um den Betrag der als Ausgleich geschuldeten finanziellen Entschädigung festzulegen, ist allein der vom Betroffenen konkret erlittene Schaden zu berücksichtigen.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 23312. Die Berufungsinstanz (LAG Düsseldorf) ist veröffentlicht in ZD 2024, 590. Vgl. ferner AG Düsseldorf ZD 2026, 225 – in diesem Heft; EuGH ZD 2024, 515 mAnm Pauly/Kienle – Scalable Capital; EuGH ZD 2025, 22 mAnm R. Schneider; BAG ZD 2025, 213 mAnm Zeuke/Meier; BAG ZD 2025, 174 und EuGH ZD 2024, 381 mAnm Moos/Rothkegel = MMR 2024, 552 mAnm Halim.

Sachverhalt

Die Parteien streiten über Ansprüche auf materiellen und immateriellen Schadensersatz im Zusammenhang mit einem Stellenbesetzungsverfahren. Der Kl. ist Volljurist, Rechtsanwalt und Fachanwalt für Arbeitsrecht. Zudem verfügt er über einen Abschluss als Master of Laws (LL.M.) (Public Law). Am 6.7.2020 verurteilte ihn das LG München I – unter Strafaussetzung zur Bewährung – wegen Betrugs in drei Fällen und versuchten Betrugs in neun Fällen zu einer Gesamtfreiheitsstrafe von einem Jahr und vier Monaten. Gegen die Verurteilung legte der Kl. Revision zum BGH ein. Über den Kl. existierte ein Wikipedia-Eintrag, der u.a. Angaben zu diesem Strafverfahren und der erfolgten Verurteilung enthielt.

Stellenbewerbung
Vorstrafe
AGG-Hopping
Informationspflicht
Immaterieller Schaden

Die Bekl., eine Universität und Körperschaft des öffentlichen Rechts, schrieb eine kurzfristig und befristet iRe Mutterschutz- und Elternzeitvertretung für ca. 18 Monate zu besetzende Stelle

für „eine*einen Volljurist*in (m/w/d)“ aus. Der Kl. bewarb sich mit Schreiben v. 23.6.2021 auf die Stelle. Die Bekl. führte am 12. und 14.7.2021 Vorstellungsgespräche mit drei Bewerbern, darunter der Kl. Weitere Bewerber hatten im Vorfeld ihre Bewerbung zurückgezogen.

Am 16.7.2021 fertigte die Bekl. einen Auswahlvermerk. Zur Auswahlentscheidung lautet er wie folgt: „Es wird daher beabsichtigt, die ausgeschriebene Stelle mit (Name einer Mitbewerberin des Kl.) zu besetzen. Anmerkung: Aus öffentlich zugänglichen Quellen ist zu entnehmen, dass (der Kl.) bereits erstinstanzlich wegen gewerbsmäßigen Betruges zu einer Freiheitsstrafe von einem Jahr und vier Monaten auf Bewährung verurteilt wurde (LG München Urt. v. 6.7.2020, Az. …). Der Vorwurf lautete, (der Kl.) habe vielfach fingierte Bewerbungen eingereicht, um potenzielle Arbeitgeber anschließend wegen angeblicher Diskriminierung zur Zahlung von Entschädigungen (nach AGG) zu veranlassen. Das Urteil ist noch nicht rechtskräftig, (der Kl.) hat hiergegen Revision beim BGH eingelegt. Der o.g. Sachverhalt ist ein solch negativer Aspekt, der in gebotener Weise bei der Besetzung der Stelle ‚Volljurist*in‘ in der Stabsstelle Justitiariat zu berücksichtigen ist. Zudem werden in der Stabsstelle Justitiariat organisatorisch alle AGG-Fälle betreut. Hierbei ist eine sachliche und objektive Bearbeitung aller Fälle notwendig, was bei (dem Kl.) jedoch zu bezweifeln ist. Aus diesen Gründen wird (der Kl.) als nicht geeigneter Bewerber bewertet.“

Nach erfolgloser außergerichtlicher Geltendmachung reichte der Kl. Klage ein, mit der er u.a. von der Bekl. die Zahlung einer Geldentschädigung verlangt. Die Bekl. habe die Daten unzulässig mittels „Google“-Recherche „hinter seinem Rücken“ erhoben und es im Nachgang unterlassen, ihn über die erfolgte Datenverarbeitung zu informieren und ihm Gelegenheit zur Stellungnahme zu geben. Dadurch habe sie gegen mehrere Bestimmungen der DS-GVO verstoßen.

Das ArbG hat die Klage abgewiesen. Auf die Berufung des Kl. hat ihm das LAG eine Entschädigung nach Art. 82 Abs. 1 DS-GVO iHv 1.000 EUR zuerkannt, iÜ hat es die Berufung zurückgewiesen.

Aus den Gründen

20 II. … Die zulässige Revision des Kl. ist unbegründet. …

51 … Das LAG hat dem Kl. zu Recht keinen über 1.000 EUR … hinausgehenden immateriellen Schadensersatz zugesprochen. …

53 b) Zugunsten des Kl. kann unterstellt werden, dass ihm nicht nur – wie vom LAG angenommen – ein Anspruch auf Zahlung immateriellen Schadensersatzes gem. Art. 82 Abs. 1 DS-GVO wegen eines Verstoßes der Bekl. gegen ihre Informationspflichten aus Art. 14 Abs. 1 lit. d DS-GVO zusteht, sondern die Bekl. bereits die Daten über das gegen den Kl. anhängige Strafverfahren mangels Eingreifens eines Erlaubnistatbestands iSv Art. 6 und 10 DS-GVO unter Verstoß gegen Bestimmungen der DS-GVO erhoben hat, und demzufolge mehrere Verstöße gegen die Verordnung vorliegen. Dies führt aber nicht dazu, dass der vom LAG festgesetzte Entschädigungsbetrag rechtsfehlerhaft bemessen wäre.

54 aa) Bei der Bemessung der Höhe des nach Art. 82 Abs. 1 DS-GVO geschuldeten Schadensersatzes haben die nationalen Gerichte in Ermangelung einer Bestimmung in der DS-GVO die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden. Art. 82 Abs. 1 DS-GVO verlangt dabei nicht, dass die Schwere des Verschuldens berücksichtigt wird. Die Ausgleichsfunktion des in Art. 82 Abs. 1 DS-GVO verankerten Schadensersatzanspruchs schließt es sogar aus, dass eine etwaige Vorsätzlichkeit des Verstoßes gegen die DS-GVO bei der Bemessung des Schadensersatzes zum Tragen kommt. Der Betrag ist jedoch so festzulegen, dass er den konkret aufgrund des Verstoßes gegen die DS-GVO erlittenen Schaden in vollem Umfang ausgleicht (vgl. EuGH 20.6.2024 – C-182/22, C-189/22 [= ZD 2024, 515 mAnm Pauly/Kienle] Rn. 27 ff. mwN – Scalable Capital; BAG 25.7.2024 – 8 AZR 225/23 [= ZD 2025, 213 mAnm Zeuke/Meier] Rn. 36).

55 bb) Hinsichtlich der nach diesen Maßgaben vorzunehmenden Bemessung der Höhe eines Schadensersatzes steht den Tatsachengerichten nach § 287 Abs. 1 ZPO ein weiter Ermessensspielraum zu, innerhalb dessen sie die Besonderheiten jedes einzelnen Falls zu berücksichtigen haben. Die Festsetzung unterliegt nur der eingeschränkten Überprüfung durch das Revisionsgericht (vgl. BAG 25.7.2024 – 8 AZR 225/23 [= ZD 2025, 213 mAnm Zeuke/Meier] Rn. 37; v. 20.6.2024 – 8 AZR 124/23 [= ZD 2025, 174] Rn. 16).

56 cc) Der vom LAG ausgeurteilte Betrag von 1.000 EUR ist jedenfalls ausreichend, um einen dem Kl. entstandenen immateriellen Schaden auszugleichen.

57 (1) Das LAG hat darauf abgestellt, dass der Kl. durch die Art und Weise der Verarbeitung der Daten über das gegen ihn anhängige Strafverfahren in erheblicher Weise zum bloßen Objekt der Verarbeitung geworden sei, was seinen Achtungsanspruch als Person herabgesetzt habe und mit einem erheblichen Kontrollverlust einhergegangen sei. Damit hat es die vom Kl. angeführten tatsächlichen Beeinträchtigungen umfassend gewürdigt. Der auf dieser Grundlage festgesetzte Entschädigungsbetrag hält sich im tatrichterlichen Beurteilungsspielraum.

58 (2) Soweit der Kl. eine ausreichend „abschreckende Wirkung“ der ihm zuerkannten Entschädigung vermisst, zeigt er keinen Gesichtspunkt auf, der eine Erhöhung rechtfertigen könnte. Durch die Rspr. des EuGH ist geklärt, dass der in Art. 82 Abs. 1 DS-GVO geregelte Schadensersatzanspruch ausschließlich eine ausgleichende und keine strafende Funktion hat, und dass die Höhe eines auf der Grundlage dieser Bestimmung gewährten Schadensersatzes nicht über das hinausgehen darf, was zum Ausgleich eines erlittenen Schadens erforderlich ist (zuletzt EuGH 4.10.2024 – C-507/23 [= ZD 2025, 22 mAnm R. Schneider] Rn. 40 ff.). Der danach maßgebliche Charakter des Entschädigungsanspruchs als Anspruch auf Ausgleich eines tatsächlich erlittenen Schadens ist nicht davon abhängig, ob Regelungen im nationalen Recht wegen eines Verstoßes gegen die DS-GVO die Verhängung eines Bußgelds gegen den Verantwortlichen ermöglichen oder nicht.

59 (3) Der Kl. zeigt auch keinen revisiblen Rechtsfehler auf, soweit er geltend macht, das LAG sei lediglich von einem Verstoß gegen die DS-GVO ausgegangen, während tatsächlich mehrere Verstöße vorlägen. Selbst wenn Letzteres – was zugunsten des Kl. unterstellt werden kann – zutreffen sollte, beziehen sich die behaupteten Verstöße jedenfalls auf denselben Verarbeitungsvorgang. In einem solchen Fall kann, wie der EuGH bereits erkannt hat, der Umstand, dass der Verantwortliche mehrere Verstöße ggü. derselben Person begangen hat, nicht als relevantes Kriterium für die Bemessung des der betroffenen Person gem. Art. 82 DS-GVO zu gewährenden Schadensersatzes herangezogen werden. Um den Betrag der als Ausgleich geschuldeten finanziellen Entschädigung festzulegen, ist allein der vom Betroffenen konkret erlittene Schaden zu berücksichtigen (EuGH v. 11.4.2024 – C-741/21 [= ZD 2024, 381 mAnm Moos/Rothkegel = MMR 2024, 552 mAnm Halim] Rn. 64). …

LAG München: Einsichtsrecht in Compliance-Abschlussbericht

DS-GVO Art. 15; SprAuG § 26 Abs. 2 S. 1; BetrVG § 83 Abs. 1 S. 1; HinSchG § 8
Urteil vom 12.6.2025 – 2 SLa 70/25 (ArbG München); nicht rechtskräftig

Leitsatz der Redaktion

Arbeitnehmern steht nach einer internen Compliance-Untersuchung kein Anspruch auf Herausgabe einer vollständigen Kopie des Abschlussberichts nach Art. 15 DS-GVO zu. Stattdessen besteht ein Einsichtsrecht gem. § 83 Abs. 1 S. 1 BetrVG, § 26 Abs. 2 S. 1 SprAuG in den Bericht als Teil der Personalakte, soweit der Bericht Daten in Bezug auf die betreffende Person enthält.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 29469. Die Revision ist beim BAG unter dem Az. 8 AZR 169/25 anhängig. Vgl. ferner EuGH ZD 2024, 22 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble; EuGH ZD 2023, 539 und BFH ZD 2024, 581.

Sachverhalt

Die Parteien streiten um die Überlassung eines Compliance-Abschlussberichts. Die Kl. ist seit 1.2.2015 in unterschiedlichen Funktionen für die Bekl. tätig. Seit 21.7.2023 nimmt sie Elternzeit in Anspruch. Ihre Jahreszielvergütung betrug zuletzt (bei Vollzeittätigkeit) 179.600 EUR brutto zzgl. Aktien. Die Parteien sind übereinstimmend der Auffassung, dass die Kl. als leitende Angestellte iSv § 5 Abs. 3 BetrVG anzusehen ist.

Interne Untersuchungen
Hinweisgeberschutz
Herausgabeanspruch
Dokumentenkopie
Personalakte

Anfang April 2023 informierte die bei der Bekl. installierte Ombudsfrau die Compliance-Abteilung der Bekl., dass es Beschwerden über die Kl. gebe. Sie fasste die Vorwürfe wie folgt zusammen:

„Alle drei Hinweisgeber, die allesamt seit (zT vielen) Jahren für E. tätig sind, haben den Führungsstil von Frau A. unabhängig voneinander als einschüchternd, herabwürdigend, respektlos und unehrlich beschrieben. Mit verschiedenen Verhaltensweisen in den vergangenen 2 Jahren habe sie Mitarbeiter verunsichert, demotiviert und regelrecht krank gemacht. Mindestens zwei Mitarbeiter hätten deshalb auch bereits gekündigt.

Alle Hinweisgeber haben geäußert, dass es ihnen schwerfällt, weiterhin unter Frau A. zu arbeiten, weil die Arbeitsatmosphäre ziemlich vergiftet sei. Bei dem einen oder anderen Kollegen würden sich die Anspannung und die Unsicherheit inzwischen auch schon negativ auf die Gesundheit auswirken. Es wäre den Hinweisgebern daher sehr wichtig, dass sich am Status quo etwas ändert."

Vom 25.8.2023 bis zum 11.1.2024 führte die Bekl. daraufhin wegen des Verdachts auf Führungsfehlverhalten der Kl. eine Compliance-Untersuchung durch, deren Abschlussbericht Gegenstand des vorliegenden Verfahrens ist. Er enthält eine strukturierte Zusammenfassung der Ergebnisse der durch die Kanzlei geführten internen Compliance-Untersuchung. Die Vorwürfe gegen die Kl. würden aufgelistet, Hinweisgeber und Zeugen namentlich benannt und Aussagen in Gesamtzusammenhänge eingeordnet. Von diesem Abschlussbericht existieren zwei Fassungen: Der Bericht ist auf den 31.1.2024 datiert. Die finale Version übersandte die Kanzlei am 6.2.2024 an die Bekl.

Mit Schreiben v. 20.2.2024 beantragte die Bekl. beim zuständigen Gewerbeaufsichtsamt, die außerordentliche, hilfsweise ordentliche Kündigung des Arbeitsverhältnisses mit der Kl. während der Elternzeit für zulässig zu erklären, wobei sie sich zur Begründung auf Ergebnisse der Compliance-Untersuchung stützte.

Die Kl. hat erstinstanzlich die Auffassung vertreten, diese Untersuchung sei nicht mit der gebotenen Objektivität geführt worden. Die Bekl. sei bereits zuvor entschlossen gewesen, sie loszuwerden.

Die Kl. hat weiter die Ansicht vertreten, dass sie nach Art. 15 Abs. 1 Hs. 2 und Abs. 3 DS-GVO Anspruch auf Zurverfügungstellung einer Kopie des Compliance-Abschlussberichts habe. Nach der Rspr. des EuGH könne sie die Herausgabe des gesamten Berichts verlangen, der allenfalls die Schwärzung von Namen und einzelnen Passagen enthalten dürfe.

Mit Endurteil v. 16.1.2025 hat das ArbG der Klage im Hauptantrag stattgegeben und die Bekl. verurteilt, eine Kopie des Compliance-Abschlussberichts zur Verfügung zu stellen.

Aus den Gründen

54 B. Die Berufung ist teilweise begründet. Die Kl. hat keinen Anspruch auf Herausgabe einer Kopie des streitgegenständlichen Compliance-Abschlussberichts aus Art. 15 Abs. 1 Hs. 2, Abs. 3 S. 1 DS-GVO. Ihr steht jedoch gem. § 26 Abs. 2 S. 1 SprAuG ein Anspruch auf Einsichtnahme in den Bericht in seiner Fassung v. 6.2.2024 als Teil der Personalakte zu.

55 I. Der Klageantrag zu Ziff. 1 ist zulässig, aber unbegründet. …

57 … Die Kl. stützt ihr Begehren auf die Anspruchsgrundlage des Art. 15 Abs. 1 Hs. 2 DS-GVO iVm Art. 15 Abs. 3 DS-GVO. Daraus ergibt sich allerdings vorliegend kein Anspruch auf Überlassung einer Kopie des vollständigen Berichts. …

64 (a) Art. 15 Abs. 3 S. 1 DS-GVO gewährt keinen ggü. Art. 15 Abs. 1 DS-GVO eigenständigen Anspruch gegen den Verantwortlichen auf Zurverfügungstellung von Dokumenten mit personenbezogenen Daten. Art. 15 Abs. 1 DS-GVO gewährt der betroffenen Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die näher in Art. 15 Abs. 1 lit. a-h DS-GVO bezeichneten Informationen. Nach Art. 15 Abs. 3 S. 1 DS-GVO stellt der Verantwortliche der betroffenen Person eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Durch die Rspr. des EuGH ist geklärt, dass Art. 15 DS-GVO nicht dahin auszulegen ist, dass er in seinem Absatz 3 S. 1 ein anderes Recht als das in seinem Absatz 1 vorgesehene gewährt. IÜ bezieht sich der Begriff „Kopie" nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen. Die Kopie muss daher alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind (EuGH v. 26.10.2023 – C-307/22 [= ZD 2024, 22 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble] Rn. 72; EuGH v. 4.5.2023 – C-487/21 [= ZD 2023, 539] Rn. 32; BFH v. 12.3.2024 – IX R 35/21 [= ZD 2024, 581] Rn. 26 f.).

65 (b) Nur wenn die Zurverfügungstellung einer Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DS-GVO verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind, besteht nach Art. 15 Abs. 3 S. 1 DS-GVO ein Anspruch darauf, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken zu erhalten (vgl. EuGH v. 26.10.2023 – C-307/22 [= ZD 2024, 22 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/

Däuble] Rn. 75; EuGH v. 4.5.2023 – C-487/21 [= ZD 2023, 539] Rn. 41, 45). Hierfür besteht jedoch keine generelle Vermutung. Vielmehr obliegt es der betroffenen Person, darzulegen, dass die Kopie der personenbezogenen Daten sowie die Mitteilung der Informationen nach Art. 15 Abs. 1 lit. a-h DS-GVO für die Wahrnehmung der ihr durch die DS-GVO verliehenen Rechte nicht genügt (BFH v. 12.3.2024 – IX R 35/21 [= ZD 2024, 581] Rn. 28).

66 Begehrt die betroffene Person die Zurverfügungstellung von Kopien von Dokumenten mit ihren personenbezogenen Daten, ist es an ihr zu benennen, welche ihr durch die DS-GVO verliehenen Rechte sie auszuüben gedenkt und darzulegen, aus welchen Gründen die Zurverfügungstellung von Kopien von Akten mit personenbezogenen Daten hierfür unerlässlich ist. Andernfalls liefe das durch den EuGH aufgestellte Regel-Ausnahme-Prinzip ins Leere, denn nach der Rspr. des EuGH ist der Anspruch nach Art. 15 Abs. 1 und Abs. 3 DS-GVO grds. auf die Zurverfügungstellung einer Kopie der verarbeiteten personenbezogenen Daten der betroffenen Person gerichtet (EuGH v. 26.10.2023 – C-307/22 [= ZD 2024, 22 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble] Rn. 72; EuGH v. 4.5.2023 – C-487/21 [= ZD 2023, 539] Rn. 32). Wenn dies für die Wahrnehmung der Rechte aus der DS-GVO nicht genügt, kann ausnahmsweise ein Anspruch auf eine (auszugsweise) Kopie der Quelle, in der die personenbezogenen Daten verarbeitet sind, bestehen (vgl. EuGH v. 26.10.2023 – C-307/22 [= ZD 2024, 22 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble] Rn. 75; EuGH v. 4.5.2023 – C-487/21 [= ZD 2023, 539] Rn. 41, 45). Einer entsprechenden Vermutung der Unerlässlichkeit bedarf es iÜ auch nicht, um einen effektiven Datenschutz zu gewährleisten. Regelmäßig genügt es für die Wahrnehmung der durch die DS-GVO verliehenen Rechte, wenn die betroffene Person Kenntnis von den über sie verarbeiteten personenbezogenen Daten erlangt und ihr die Informationen nach Art. 15 Abs. 1 lit. a bis lit. h DS-GVO mitgeteilt werden. Insb. durch die Mitteilung, welche personenbezogenen Daten verarbeitet werden und zu welchem Zweck diese Verarbeitung erfolgt, ist die betroffene Person bereits regelmäßig in der Lage, die Richtigkeit der personenbezogenen Daten und die Rechtmäßigkeit deren Verarbeitung zu überprüfen (BFH v. 12.3.2024 – IX R 35/21 [= ZD 2024, 581] Rn. 28).

67 (c) Gemessen an diesem Maßstab besteht kein datenschutzrechtlicher Anspruch der Kl. darauf, dass die Bekl. ihr eine Kopie des Compliance-Abschlussberichts v. 31.1.2024 zur Verfügung stellt.

68 (aa) Die Kl. begründet ihr Begehren damit, es sei ihr vorrangiges Ziel, die Rechtmäßigkeit der Datenverarbeitung zu überprüfen, also welche Daten da über sie erhoben und gespeichert worden seien und in welcher Form das Ganze erfolgt sei. Die untersuchende Kanzlei habe sich in einem Interessenkonflikt befunden. Die Interviewführung sei nicht objektiv, sondern zielgelenkt erfolgt. Diesen Details wolle sie nachgehen und überprüfen, welche Aussagen über sie gemacht und gespeichert worden seien, ob diese Aussagen richtig seien und wie sie ermittelt worden seien. Insb. relevant seien auch die Ausführungen durch die untersuchungsführende Kanzlei um die einzelnen Zeugenaussagen herum, da sie nur so die faire und transparente Verarbeitung ihrer Daten überprüfen könne. Es sei von Relevanz, ob Zeugenaussagen hinterfragt, geprüft und verifiziert worden oder schlicht als vermeintlich wahr hingenommen und gespeichert worden seien. Gerade der Abbau von Informationsasymmetrien zwischen Arbeitgeber und Arbeitnehmer sei ein legitimes, rechtlich anzuerkennendes Ziel des Auskunftsanspruchs. Die Bekl. verstoße ihrerseits gegen das Gebot prozessualer Waffengleichheit, wenn sie einzelne Aspekte aus dem Compliance-Bericht zu ihren Gunsten anführe – und ihr die Durchsicht auf entlastende Umstände verwehre.

69 (bb) Dieses Vorbringen rechtfertigt nicht die Annahme, die Kl. benötige im Interesse eines effektiven Datenschutzes eine Kopie des gesamten Compliance-Abschlussberichts. Der Bericht enthält nach den unwidersprochenen Ausführungen der Bekl. über die personenbezogenen Daten der Kl. hinaus eine Vielzahl anderer Daten, nicht nur personenbezogene Daten der Zeugen, sondern auch Zusammenfassungen der Aussagen, Wertungen und Würdigungen durch die beauftragten Ermittler. Darüber hinaus enthält die Fassung v. 31.1.2024 noch Ausführungen der Kanzlei zur rechtlichen Bewertung. Um personenbezogene Daten der Kl. im Bericht handelt es sich aber nur, soweit Tatsachen über sie bzw. ihr Verhalten behauptet werden. Bereits Aussagen der Zeugen dazu, wie sie das Arbeitsumfeld empfunden haben, wie sie auf Arbeitsbedingungen reagiert haben oder ob/wie sie diese Bedingungen bewerteten, sind keine personenbezogenen Daten der Kl. Das gilt erst recht für daran anknüpfende ordnende, vergleichende und wertende Ausführungen der internen Ermittler, ebenso wie Empfehlungen der Ermittler zu Konsequenzen der Bekl. aus den Ergebnissen der Ermittlung. Der Bericht als Ganzes geht damit weit über eine Verarbeitung personenbezogener Daten der Kl. hinaus, auf deren Mitteilung ein Anspruch nach Art. 15 Abs. 1 DS-GVO bestünde, ggf. in Kombination mit einer Kopie dieser Daten nach Art. 15 Abs. 3 DS-GVO.

70 (cc) Soweit die Kl. darauf verweist, nach der neueren Rspr. des EuGH könne sich die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten, die u.a. personenbezogene Daten enthielten, die Gegenstand der Verarbeitung seien, als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten erforderlich sei, um ihre Verständlichkeit zu gewährleisten, verhilft dies ihrer Klage nicht zum Erfolg. Es ist nicht ersichtlich, inwiefern die über die personenbezogenen Daten der Kl. hinausgehenden Inhalte zur Verständlichkeit der erfassten Aussagen über die Kl. erforderlich sein sollten. Namentlich benötigt die Kl. zur Überprüfung der datenschutzrechtlichen Zulässigkeit – und dies ist ungeachtet der Motivation der Kl. der Auslegungsmaßstab für die Reichweite des datenschutzrechtlichen Auskunftsanspruchs – keine Informationen darüber, welche Schlüsse die Bekl. oder von ihr beauftragte Personen ihrerseits aus den erhobenen Daten ziehen oder wie sich die Zeugen insgesamt zu ihren Arbeitsbedingungen geäußert haben.

71 Die Kl. hat ausgeführt, die Ausführungen durch die untersuchungsführende Kanzlei um die einzelnen Zeugenaussagen herum seien für sie relevant, da sie nur so die faire und transparente Verarbeitung ihrer Daten überprüfen könne. Es sei von Relevanz, ob Zeugenaussagen hinterfragt, geprüft und verifiziert worden oder schlicht als vermeintlich wahr hingenommen und gespeichert worden seien. Gerade der Abbau von Informationsasymmetrien zwischen Arbeitgeber und Arbeitnehmer sei ein legitimes, rechtlich anzuerkennendes Ziel des Auskunftsanspruchs. Das mag in Bezug auf die unmittelbar personenbezogenen Daten zutreffen. Soweit die Bekl. bzw. die beauftragte Kanzlei aber andere erhobene Daten bewertet und Überlegungen für den Umgang mit Führungsverhalten anstellt, ist aber nicht ersichtlich, weshalb eine Kopie der diesbezüglichen Ausführungen erforderlich sein sollte, um eine Verständlichkeit der erfolgten Datenverarbeitung zu gewährleisten. Allenfalls könnte die Kl. eine Kopie der erfassten Äußerungen zu ihrer Person begehren, nicht aber darüber hinausgehend eine Kopie des Berichts – und sei es mit Schwärzungen. Nur letzteres hat sie aber beantragt.

72 (d) Entgegen ihrer Auffassung kann die Kl. auch nicht verlangen, dass die Bekl. ihr eine teilweise geschwärzte Kopie des Be-

richts zur Verfügung stellt. Nach ihren eigenen Ausführungen ist die Kl. nicht gewillt, sich mit einer Fassung des Berichts zu begnügen, in welcher außer ihren personenbezogenen Daten alle anderen Inhalte geschwärzt sind, was de facto einem Auszug aus dem Bericht gleichkäme, sondern sie will insb. die darüber hinaus gehenden Bewertungen der untersuchenden Kanzlei prüfen. Damit aber geht ihr Begehren über das hinaus, was sie im vorliegenden Fall allenfalls auf der Grundlage des Art. 15 Abs. 1, Abs. 3 DS-GVO verlangen könnte.

73 II. Der Klageantrag zu Ziff. 3 ist gleichfalls zulässig, aber unbegründet. Die Kl. hat auch keinen datenschutzrechtlichen Anspruch gegen die Bekl. darauf, eine Kopie des Compliance-Abschlussberichts idF v. 6.2.2024 zu erhalten. ...

78 III. Damit ist der als Antrag zu Ziff. 2 gestellte Hilfsantrag zur Entscheidung angefallen. ...

80 2. Der Antrag ist begründet. Die Kl. kann gem. § 26 Abs. 2 S. 1 SprAuG Einsicht in den Compliance-Abschlussbericht als Teil ihrer Personalakte verlangen.

a) § 26 Abs. 2 S. 1 SprAuG ist § 83 Abs. 1 S. 1 BetrVG wortgleich nachgebildet und hat deshalb den gleichen Regelungsinhalt (BAG v. 16.11.2010 – 9 AZR 573/09 Rn. 21 mwN). Nach dieser Vorschrift hat ein leitender Angestellter das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen. Die Kl. als leitende Angestellte iSd § 5 Abs. 3 BetrVG ist also aktivlegitimiert.

81 b) Personalakten sind eine Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse eines Mitarbeiters betreffen und in einem inneren Zusammenhang mit dem Dienstverhältnis stehen (BAG v. 19.7.2012 – 2 AZR 782/11 Rn. 18). ...

82 Folglich sind auch interne Ermittlungsakten Teil der Personalakte der betroffenen Mitarbeiter (HWK/Sittard, 11. Aufl. 2024, BetrVG § 83 Rn. 2; Fitting, BetrVG, 32. Aufl. 2024, § 83 Rn. 6; Musiol NZA 2024, 28 (29) mwN).

83 c) Unter Zugrundelegung dieses Maßstabs zählt der streitgegenständliche Compliance-Abschlussbericht v. 31.1.2024 zur Personalakte der Kl. Unstreitig bezieht sich dieses Dokument auf das Verhalten der Kl. im Arbeitsverhältnis, namentlich auf ihr Führungsverhalten. Der innere Zusammenhang mit dem Arbeitsverhältnis wird auch daran deutlich, dass die Bekl. die Ergebnisse der Compliance-Untersuchung zum Anlass genommen hat, beim Gewerbeaufsichtsamt die Zustimmung zu einer Kündigung des Arbeitsverhältnisses zu beantragen.

d) Die Bekl. kann die Einsicht in den Compliance-Abschlussbericht nicht mit dem Hinweis auf den Schutz berechtigter Interessen Dritter verweigern.

84 aa) Das Einsichtsrecht eines leitenden Angestellten in seine Personalakte nach § 26 Abs. 2 S. 1 SprAuG ist gesetzlich nicht eingeschränkt. Es besteht – wie ausgeführt – bzgl. aller Aufzeichnungen, die sich mit seiner Person und dem Inhalt der Entwicklung seines Arbeitsverhältnisses befassen.

85 bb) Vorliegend kann offenbleiben, ob der Anspruch der Kl. auf Einsicht in die Personalakte nach § 8 Abs. 1 HinSchG beschränkt sein kann (bejahend Musiol NZA 2024, 28 (31) f.). Das ArbG hat zutreffend festgestellt, dass der sachliche Anwendungsbereich des HinSchG nicht eröffnet ist, weil sich die von der Bekl. vorgetragenen Hinweise nicht auf einen in § 2 HinSchG genannten Verstoß beziehen. ...

87 cc) Der Einsichtnahme stehen auch nicht ausnahmsweise überwiegende Arbeitgeberinteressen entgegen, welche nach § 242 BGB dem klägerischen Anspruch entgegengehalten werden könnten. Das gilt insb. im Hinblick auf Sinn und Zweck des betrieblichen Compliance-Verfahrens, welches im Interesse der Wahrheitsfindung so weit wie möglich auch die vertrauliche Behandlung der Informationen und der Identität von Zeugen erfordert, um Hemmungen der Betroffenen abzubauen, an einem solchen Verfahren mitzuwirken (hierzu Musiol NZA 2024, 28 (29 f.) mwN).

88 (1) Allerdings gefährdet die Einsichtnahme vorliegend keine laufende interne Untersuchung. Die Ermittlungen der Bekl. sind abgeschlossen, dies dokumentiert gerade der streitgegenständliche Abschlussbericht, sodass insoweit keine Begrenzung des Einsichtsrecht erforderlich ist, um das Compliance Verfahren nicht zu gefährden (ebenso Musiol NZA 2024, 28 (30)).

89 (2) Das Einsichtsrecht ist auch nicht zur Sicherung berechtigter Interessen Dritter, insb. der im Verfahren befragten Mitarbeiter der Bekl., eingeschränkt. Sichert der Arbeitgeber bei Hinweisen aus der Belegschaft über betriebliches Fehlverhalten anderer Mitarbeiter dem Hinweisgeber die Wahrung seiner Anonymität zu, ist er diesen ggü. nicht befugt, die Daten weiterzugeben, die die Person des Hinweisgebers offenbaren oder Rückschlüsse auf die Person zulassen. Weil aber andererseits das Führen von Geheimakten iRd Personalakte unzulässig ist (allg.M. ErfK/Kania, 25. Aufl. 2025, BetrVG § 83 Rn. 2; Fitting, BetrVG, 32. Aufl. 2024, § 83 Rn. 5; Richardi BetrVG/Thüsing, 17. Aufl. 2022, § 83 Rn. 9; BeckOK ArbR/Werner, 6/2025, BetrVG § 83 Rn. 3), kann der Arbeitgeber bei Zusicherung der Anonymität des Hinweisgebers nur den Teil des Hinweises zur Personalakte im materiellen Sinne nehmen, der die Person des Hinweisgebers nicht offenbart oder Rückschlüsse auf die Person des Hinweisgebers zulässt. Deswegen sind die Teile der Mitteilungen eines Hinweisgebers, dem Anonymität zugesichert worden ist, insoweit nicht zur Personalakte zu nehmen bzw. durch Schwärzung oder eine sonstige technische Vorkehrung unkenntlich zu machen, dass weder die Person des Hinweisgebers erkennbar ist, noch dass Rückschlüsse auf die Person möglich sind (Klasen/Schaefer DB 2012, 1384 (1385); Fitting, BetrVG, 32. Aufl. 2024, § 83 Rn. 6). Dem berechtigten Schutzinteresse von Zeugen, denen Anonymität zugesichert worden ist, hat die Bekl. folglich durch Unkenntlichmachung entsprechender Passagen in der Akte Rechnung zu tragen, die die Person des Hinweisgebers erkennen lassen oder Rückschlüsse auf diese Person zulassen. Unterlässt der Arbeitgeber diese Anonymisierung, kann er dem Angestellten, der Einsicht in seine Personalakte begehrt, dies nicht unter Hinweis auf die von ihm unterlassene Anonymisierung verweigern. ...

Anmerkung

RAin Wiebke Reuter, LL.M. (London), FAin für IT-Recht, Taylor Wessing, Berlin / RA Dr. Benedikt Groh, FA für Arbeitsrecht, Taylor Wessing, München

Das LAG München positioniert sich mit seiner Entscheidung in einem Spannungsfeld zwischen Art. 15 DS-GVO, Compliance-Untersuchungen, Hinweisgeberschutz und dem Einsichtsrecht in die Personalakte. Dogmatisch bemerkenswert ist die doppelte Weichenstellung: Zum einen begrenzen die Richter den Kopieanspruch im Lichte der jüngeren EuGH- und BFH-Rspr. deutlich. Zum anderen weiten sie den Personalaktenbegriff aus und sichern so über das Einsichtsrecht faktisch dennoch einen Zugang zum Bericht – in der Praxis oft bedeutsamer als der Streit um den „Kopiendogmatismus" des Art. 15 DS-GVO.

1. Art. 15 DS-GVO: Kopie der personenbezogenen Daten, nicht des Dokuments

Ausgangspunkt der Entscheidung ist die inzwischen gefestigte Rspr. des EuGH, wonach Art. 15 Abs. 3 DS-GVO keinen eigenständigen Anspruch auf Herausgabe von Dokumenten begrün-

det, sondern den Auskunftsanspruch aus Art. 15 Abs. 1 DS-GVO lediglich flankiert (vgl. auch EDSA, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.0, Rn. 4, 23). Die Kopie bezieht sich nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen (EuGH ZD 2023, 539 Rn. 32 – Österreichische Datenschutzbehörde; EuGH ZD 2024, 22 Rn. 72 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble – FT/DW). Nur ausnahmsweise kann die Zurverfügungstellung von Auszügen oder ganzen Dokumenten „unerlässlich" sein, wenn andernfalls die wirksame Ausübung der Betroffenenrechte nicht gewährleistet wäre (EuGH ZD 2024, 22 Rn. 75 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble – FT/DW).

a) Strenge Darlegungslast für die Unerlässlichkeit einer Dokumentenkopie

Das LAG übernimmt diesen Ansatz vollständig und betont – im Anschluss an den BFH ZD 2024, 581 Rn. 28 –, dass es der betroffenen Person obliegt darzulegen, warum eine bloße Mitteilung der Daten (ggf. samt Kopie der Daten) nicht genügt und warum gerade eine Dokumentenkopie „unerlässlich" ist. Eine Vermutung zugunsten der Unerlässlichkeit lehnte das Gericht im Einklang mit dem BFH ausdrücklich ab. Der EuGH hat die Frage der Darlegungslast nicht explizit adressiert. Ob er mit Blick auf seine weitreichende Auslegung des Auskunfts- und Kopieanspruchs einer so strengen Darlegungslast folgen würde, ist fraglich.

b) Enge Bestimmung personenbezogener Daten im Compliance-Bericht

Für Compliance-Berichte zieht das LAG eine scharfe Trennlinie: Personenbezogene Daten der Kl. sind nur diejenigen Angaben, die Tatsachen über sie bzw. ihr Verhalten betreffen. Bewertungen, rechtliche Würdigungen, Kontextausführungen, Empfehlungen der beauftragten Kanzlei und weite Teile der Zeugenaussagen qualifiziert das Gericht demgegenüber als nicht personenbezogene Daten der Kl. Der Bericht als Ganzes gehe „weit über" die Verarbeitung personenbezogener Daten der Kl. hinaus. Damit sei der begehrte Anspruch auf Überlassung einer Kopie des vollständigen Abschlussberichts schon deshalb von Art. 15 DS-GVO nicht gedeckt.

c) Restriktive Anwendung des Maßstabs der „Unerlässlichkeit"

Besonders restriktiv wendet das LAG den Maßstab der „Unerlässlichkeit" an: Die Kl. hatte u.a. geltend gemacht, sie wolle die Objektivität der Untersuchung, die Interviewführung, die Einordnung und Gewichtung der Aussagen sowie etwaige entlastende Umstände überprüfen. Das Gericht hält dem entgegen, hierfür sei eine Kopie des gesamten Berichts nicht erforderlich. Entscheidend sei allein, dass die Kl. Kenntnis von den über sie verarbeiteten personenbezogenen Daten und den in Art. 15 Abs. 1 lit. a bis lit. h DS-GVO genannten Informationen erhalte; welche Schlüsse die Bekl. oder ihre Kanzlei aus diesen Daten ziehe, sei für die datenschutzrechtliche Prüfung nicht maßgeblich.

d) Kritik: EuGH verlangt Kontext, wenn dieser für das Verständnis notwendig ist

Diese Sichtweise ist diskussionswürdig. Der EuGH betont ausdrücklich, dass Kontextinformationen „unerlässlich" sein können, wenn sie für das Verständnis der verarbeiteten Daten erforderlich sind. So umfasst der Auskunftsanspruch etwa im Gesundheitsbereich auch die Kopie der relevanten Patientendaten einschließlich Diagnosen, Untersuchungsergebnissen und ärztlichen Befunden, weil nur deren Einbettung die Daten verständlich macht (EuGH ZD 2024, 22 Rn. 79 mAnm Winnenburg = MMR 2023, 939 mAnm Hense/Däuble – FT/DW).

Gerade bei komplexen, narrativ aufgebauten Compliance-Berichten kann jedoch die Einbettung einzelner Äußerungen – also Fragen, Nachfragen, Einwände und Wertungen – entscheidend dafür sein, ob die Verarbeitung aus Sicht der betroffenen Person als fair und transparent erscheint.

Praktisch brisant ist zudem, dass die vom LAG vorgenommene enge Abgrenzung Missbrauchsanreize setzen kann: Arbeitgeber könnten versucht sein, belastende Inhalte gezielt in den Bereich „Bewertung/Würdigung/Empfehlung" zu verschieben, um sie dem Kernbereich des Auskunftsanspruchs zu entziehen. Dass die Grenze zwischen „Tatsache" und „Bewertung" fließend ist, zeigt gerade der vorliegende Fall.

2. Rechtsmissbrauch, Geschäftsgeheimnisse, Hinweisgeberschutz

Das LAG ließ Fragen zu Geschäftsgeheimnissen und Hinweisgeberschutz ausdrücklich offen, deutete aber an, dass eine pauschale Berufung auf Geheimhaltung bei personenbezogenen Daten des Betroffenen eng zu sehen ist. Zugleich betont es – im Einklang mit dem EuGH –, dass Art. 15 DS-GVO nicht auf datenschutzbezogene Zwecke beschränkt ist und der Betroffene seine Motive nicht offenlegen muss; ein pauschaler „Ausforschungsverdacht" greift daher nicht.

3. Compliance-Abschlussbericht als Teil der Personalakte

Die zweite Achse der Entscheidung betrifft das Einsichtsrecht in die Personalakte.

Das LAG vertrat die Auffassung, dass der streitgegenständliche Compliance-Abschlussbericht zur Personalakte der Kl. gehörte. In diese hat die Kl. als leitende Angestellte gem. § 26 Abs. 2 S. 1 SprAuG ein Einsichtsrecht. Dabei ist § 26 Abs. 2 S. 1 SprAuG dem § 83 Abs. 1 S. 1 BetrVG wortgleich nachgebildet und hat deshalb den gleichen Regelungsinhalt. Entscheidend ist dabei nicht, was der Arbeitgeber als Personalakte bezeichnet. Es sind nämlich ebenso Sonder- oder Nebenakten, gleichgültig wo sie geführt werden, Bestandteile der Personalakte.

Ganz allgemein vertrat das LAG die Ansicht, dass eine Sammlung von Urkunden und Vorgängen, die persönliche und dienstliche Verhältnisse der Person betreffen und in einem inneren Zusammenhang mit dem Arbeits-/Dienstverhältnis stehen, dazugehören. Der Compliance-Abschlussbericht bezieht sich auf das Verhalten der Kl. im Arbeitsverhältnis (insb. Führungsverhalten). Das Gericht bejahte auch einen zu fordernden inneren Zusammenhang mit dem Arbeitsverhältnis dadurch, dass der Compliance-Bericht dazu verwendet wurde, die Zustimmung zu einer Kündigung des Arbeitsverhältnisses zu beantragen.

Eine Absage erteilte das Gericht dabei dem Argument des Arbeitgebers, die Einsicht in den Bericht wäre wegen dem Schutz berechtigter Interessen Dritter zu verweigern. Zwar hat es offengelassen, ob eine solche Einschränkung nach § 8 Abs. 1 HinSchG bestehen könnte, weil nach den Feststellungen des LAG der Anwendungsbereich des HinSchG nicht eröffnet war. Jedoch war es für das LAG gerade nicht ausreichend, das Einsichtsrecht wegen der Sicherung berechtigter Interessen Dritter einzuschränken. Das Argument des LAG ist dabei recht gnadenlos: Sofern der Arbeitgeber es versäumt, der den Hinweisgebern zugesicherten Anonymität durch Unkenntlichmachung entsprechender Passagen in der Akte Rechnung zu tragen, und der Bericht ohne solche Schwärzungen oder Maßnahmen Eingang in die Personalakte findet, kann die Herausgabe nicht mehr wegen unterlassener Anonymisierung verweigert werden. Mit anderen Worten: der Arbeitgeber muss die Zusicherung ernsthaft vornehmen und ein entsprechendes Dokument zur Akte nehmen, das eben nicht Rückschlüsse auf die Person des Hinweisgebers ermöglicht. Unterlässt er dies, kann

er den selbst verursachten fehlenden Schutz nicht als Verweigerungsgrund anführen.

4. Bewertung

Bemerkenswert ist, wie ausführlich sich das LAG mit Art. 15 Abs. 3 DS-GVO und der dazu ergangenen Rspr. auseinandersetzt. Die Auslegung fällt im Ergebnis sehr streng aus – insb. hinsichtlich des Umfangs des Kopieanspruchs, der Darlegungs- und Nachweispflicht zur Unerlässlichkeit sowie der Abgrenzung, welche Bestandteile eines Dokuments überhaupt personenbezogene Daten darstellen. Diese enge Sichtweise steht möglicherweise nicht vollständig im Einklang mit der betroffenenfreundlichen Auslegung des EuGH zum Anspruch auf Kopie.

Andererseits gewährt das LAG im Ergebnis einen vergleichbaren Schutz über das Einsichtsrecht in die Personalakte, das der Kl. faktisch einen weitgehenden Zugang zum Bericht eröffnet. Das Einsichtsrecht in die Personalakte von Arbeitnehmenden nach § 83 Abs. 1 S. 1 BetrVG ist ein individualrechtlicher Anspruch. Dieser hat den Ursprung in den Nebenpflichten des Arbeitgebers im Arbeitsverhältnis. Deshalb gelten diese Grundsätze auch für Arbeitnehmer in nicht betriebsratsfähigen oder betriebsratslosen Betrieben (Fitting, BetrVG, § 83 Rn. 1, 2).

Arbeitgeber sollten deshalb genau prüfen, wie sie entsprechende Berichte dokumentieren und archivieren. Wenn Hinweisgebern bzw. befragten Mitarbeitenden Anonymität zugesichert wurde, muss dies technisch und organisatorisch umgesetzt werden. Wird dies versäumt, kann der Arbeitgeber eine Verweigerung der Herausgabe nicht allein durch eine mögliche Rechtsverletzung der nun nicht anonymisierten Personendaten begründen.

5. Praktische Konsequenzen und Ausblick

Es bleibt abzuwarten, ob sich die strenge Auslegung des Kopieanspruchs durchsetzen wird. Sie fügt sich in die wachsende Kritik ein, dass Art. 15 DS-GVO zunehmend ausufert und über seinen ursprünglichen Transparenzzweck hinaus als allgemeines Informationsinstrument genutzt wird. Zugleich stärkt die Entscheidung das Einsichtsrecht in die Personalakte und eröffnet damit einen alternativen Zugang zu relevanten Informationen.

Gestaltungshinweise ergeben sich nahezu von selbst: Arbeitgeber sollten sorgfältig prüfen, welche Inhalte Teil der Personalakte werden. Strategische, prozessuale oder rechtliche Beratungsteile sind konsequent von sachlichen, personenbezogenen Feststellungen zu trennen – etwa durch gesonderte Mandantenmemoranden außerhalb des Personalaktenkontexts. Ebenso sollte frühzeitig geklärt werden, welche Teile einer Untersuchung personalaktenecht sind und wie sie so gestaltet werden, dass eine spätere Einsichtnahme möglich bleibt, ohne die Rechte Dritter unzulässig zu beeinträchtigen.

Die Revision zum BAG ist zugelassen (Az. 8 AZR 169/25). Es ist daher zu erwarten, dass sich das Gericht bald zur Reichweite des Kopieanspruchs bei komplexen Dokumenten äußern und den vom EuGH eingeführten Unerlässlichkeitsmaßstab für das Arbeitsverhältnis präzisieren wird.

Schon jetzt zeigt die Entscheidung des LAG München jedoch deutlich: Wer allein auf Art. 15 DS-GVO als Schlüssel zu internen Untersuchungsberichten setzt, wird häufig enttäuscht werden. Die eigentliche Brücke zur Transparenz im Arbeitsverhältnis verläuft über den Personalaktenzugang – und genau dort ist die Entscheidung konsequent arbeitnehmerfreundlich. Sie erinnert daran, dass Datenschutzrecht und Arbeitsrecht nicht gegeneinanderstehen, sondern gemeinsam den Rahmen fairer innerbetrieblicher Transparenz bilden.

VG Wiesbaden: Auskunftsanspruch über Zustandekommen des Scorewerts

DS-GVO Art. 4 Nr. 4, 15 Abs. 1, Abs. 4, 22 Abs. 1
Urteil vom 19.11.2025 – 6 K 788/20.WI; nicht rechtskräftig

Leitsätze der Redaktion

1. Die automatisiert und mithilfe eines mathematisch-statistischen Verfahrens erfolgte Ermittlung und Zusammenstellung von personenbezogenen Daten zwecks Profilbildung und die daraus folgende Erstellung eines finalen Scorewerts durch eine Wirtschaftsauskunftei stellen Profiling iSd Art. 4 Nr. 4 DS-GVO dar.

2. Die Erstellung des Scorewerts stellt des Weiteren eine auf einer ausschließlich automatisierenden Verarbeitung – einschließlich Profiling – beruhenden Entscheidung dar, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt gem. Art. 22 Abs. 1 DS-GVO. Die Scorewert-Erstellung ist als solche schon geeignet, eine Vorgriffswirkung auf die Begründung, Änderung oder Aufhebung einer rechtlichen Position einer betroffenen Person, etwa im Hinblick auf eine Kreditvergabe, zu entfalten, weil hierbei eine Einschätzung ihrer Kreditwürdigkeit getroffen wird.

3. Die Wirtschaftsauskunftei schuldet der betroffenen Person nach Art. 15 Abs. 1 lit. h DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache in Bezug auf den ermittelten Scorewert eine einzelfallbezogene Begründung, warum ihr Score mit diesem und nicht mit einem anderen Ergebnis berechnet wurde.

4. Eine Verpflichtung der Wirtschaftsauskunftei, den ihren Scorewerten zugrunde liegenden Algorithmus oder das statistische Verfahren, das der Scorewert-Bildung zugrunde liegt, mitzuteilen, besteht gem. Art. 15 Abs. 4 DS-GVO nicht.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 35877. Die Berufung ist beim VGH Hessen unter dem Az. 10 A 169/26 anhängig. Der Vorlagebeschluss des VG Wiesbaden ist veröffentlicht in ZD 2022, 121 mAnm Qasim, die Vorabentscheidung des EuGH in ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke – SCHUFA. Vgl ferner Dirkers/Rothkegel ZD 2026, 192 – in diesem Heft; BGH MMR 2011, 409; EuGH ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz; BGH MMR 2014, 489; EuGH ZD 2024, 166 mAnm Schild; EuGH ZD 2022, 553 mAnm Schild; VG Wiesbaden ZD 2022, 706 und ÖOGH ZD 2026, 210 – in diesem Heft.

Sachverhalt

Die Kl. begehrt ein aufsichtliches Einschreiten des Bekl. gerichtet auf eine Auskunftserteilung durch die Beigel.

Die Beigel. ist eine privatwirtschaftliche Wirtschaftsauskunftei mit Sitz in Deutschland, die ihre Vertragspartner mit Informationen zur Kreditwürdigkeit Dritter, insb. von Verbrauchern, versorgt. Die Beigel. speichert die ihr übermittelten Daten, um ihren Vertragspartnern wiederum Auskünfte zu erteilen. Vor dem Abschluss eines kreditrelevanten Geschäfts können die Vertragspartner der Beigel. mithilfe der Auskunft und weiteren Informationen prüfen, welche Risiken das in Aussicht genommene Geschäft birgt. Die Beigel. erstellt hierzu einen sog. Scorewert. Der Scorewert soll dem Vertragspartner der Beigel. Auskunft darüber geben, wie hoch das Risiko von Zahlungsstörungen der betreffenden Person ist, wenn das geplante kreditrelevante Geschäft abgeschlossen wird. Zur Ermittlung des Scorewerts prognostiziert die Beigel. aus bestimmten Merkmalen einer Person auf der Grundlage mathematisch-

Wirtschaftsauskunftei
Kreditwürdigkeit
Automatisierte Entscheidung
Profiling
Algorithmus

statistischer Verfahren für diese die Wahrscheinlichkeit eines künftigen Verhaltens, wie zB die Rückzahlung eines Kredits. Die Erstellung von Scorewerten basiert auf der Annahme, dass durch die Zuordnung einer Person zu einer Gruppe anderer Personen mit bestimmten vergleichbaren Merkmalen, die sich in einer bestimmten Weise verhalten haben, ein ähnliches Verhalten vorausgesagt werden kann. Weist die Person ein bestimmtes Profil auf, wird ihr der ermittelte Scorewert von der Beigel. zugerechnet. Nach eigenen Angaben der Beigel. erstellt sie neben einem allgemeinen Score auch individuelle Score-Modelle für spezielle Vertragspartner, die die spezifischen Anforderungen dieser Unternehmen sowie die individuelle Risikopolitik berücksichtigen sollen.

Die Kl. beabsichtigte im Juli 2018 bei der D-Bank AG einen Kredit über eine Summe von 5.000 EUR aufzunehmen. In diesem Zusammenhang holte die D-Bank eine Auskunft bei der Beigel. über die Kl. ein. Im Juli 2018 übermittelte die Beigel. der D-Bank einen Bonitätsscore von 85,96% zur Person der Kl. Die Kl. gibt hierzu an, sie habe von der D-Bank in der Folge die Information erhalten, dass sie durch die Beigel. mit einem Scorewert von 85,96% eingestuft worden sei, ohne dass bei der Kl. sog. „harte Negativmerkmale" vorgelegen hätten. Die D-Bank lehnte eine Kreditvergabe an die Kl. in der Folge ab. Die Kl. verlangte sodann von der Beigel. Auskunft darüber, welche Elemente die Score-Berechnung beeinflussten, welche Kriterien der Score-Bewertung zugrunde lägen und auf welche Weise der Scorewert konkret berechnet werde. Die Beigel. teilte der Kl. zunächst mit Schreiben v. 10.7.2018 Folgendes mit: „Sie (erhalten) gemäß Art. 15 Datenschutzgrundverordnung (DS-GVO) eine Kopie der am 10.7.2018 zu Ihrer Person bei der SCHUFA gespeicherten personenbezogenen Daten."

Als Anlage war u.a. eine Seite mit folgendem Inhalt beigefügt: „Am 2.7.2018 beträgt Ihr Basisscore 97,35% von theoretisch möglichen 100%. Der Basisscore ermöglicht Ihnen eine branchenunabhängie Einschätzung Ihrer Bonität. Er wird als Erfüllungswahrscheinlichkeit in Form eines Prozentwertes dargestellt. Die Berechnung erfolgt einmal pro Quartal auf Basis der zu Ihrer Person bei der SCHUFA gespeicherten Daten." Mit Schreiben v. 23.8.2018 teilte die Beigel. der Kl. mit, die Elemente, die die Scoreberechnung beeinflussten, seien vollständig in der der Kl. erteilten Kopie der personenbezogenen Daten (nach Art. 15 DS-GVO) v. 10.7.2018 ausgewiesen. Die Scores ergäben sich aus einer statistischen Auswertung gleicher oder ähnlicher Datensätze. Sie würden anhand moderner mathematisch-statistischer Verfahren berechnet. Die Beigel. sei zu einer Offenlegung ihrer Berechnungsmethoden nicht verpflichtet, weil diese unter das Betriebs- und Geschäftsgeheimnis fielen. Mit Schreiben ihres Bevollmächtigten v. 18.10.2018 erhob die Kl. Beschwerde bei dem Bekl., mit der sie Folgendes geltend machte: Die Kl. begehre von der Beigel. Auskunft über die für ihre Bewertung zugrunde gelegten Scorewerte sowie Löschung falscher Eintragungen. Es lägen keinerlei Tatsachen vor, die eine Einstufung mit einem Scorewert von 85,96% rechtfertigen könnten. Die Kl. habe keinerlei Schulden und verfüge über eine gute Bonität. Die Vorgehensweise der Beigel., insb. die offensichtliche Verwendung rein automatisierter Prozesse zur Erstellung von Bewertungen, verstoße gegen Art. 22 DS-GVO. Mit „Verfügung" v. 3.6.2020 teilte der Bekl. der Kl. mit, die Nutzung von Bonitäts- oder Scorewerten zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses sei grds. zulässig. Dies ergebe sich aus Art. 6 Abs. 1 lit. b und lit. f DS-GVO und aus § 31 BDSG. Die Anforderungen zur Berechnung des Bonitätswerts nach § 31 BDSG erfülle die Beigel. in aller Regel. Mit Schreiben ihres Bevollmächtigten hat die Kl. Klage erhoben. Die Kl. ist der Auffassung, sie habe gegen den Bekl. einen Anspruch auf weitere Befassung und Überprüfung ihrer Beschwerde nach Art. 78 Abs. 2 DS-GVO iVm Art. 57 DS-GVO sowie einen Anspruch auf aufsichtliches Einschreiten ggü. der Beigel. gem. Art. 58 DS-GVO. Sie habe einen Auskunftsanspruch ggü. der Beigel. gem. Art. 15 Abs. 1 lit. h, 22 Abs. 1 DS-GVO, der nicht erfüllt sei. Die Beigel. müsse der Kl. ggü. detailliert offenlegen, welche Daten zur konkreten Scoring-Wertermittlung für ihre Person genutzt würden.

Aus den Gründen

77 II. Die Klage ist hinsichtlich des ersten Hilfsantrags begründet.

78 Der Bescheid des Bekl. v. 3.6.2020 ist rechtswidrig und verletzt die Kl. in ihren Rechten; die Kl. hat im maßgeblichen Zeitpunkt der gerichtlichen Entscheidung einen Anspruch auf ein Einschreiten des Bekl. ggü. der Beigel. zur Erfüllung des Auskunftsrechts aus Art. 15 Abs. 1 DS-GVO, § 113 Abs. 5 S. 1 VwGO. Die konkret zu ergreifende Abhilfemaßnahme nach Art. 58 Abs. 2 DS-GVO steht dabei im pflichtgemäßen Ermessen des Bekl. ...

85 2. Das der Kl. in Art. 15 Abs. 1 DS-GVO gewährte Auskunftsrecht ggü. der Beigel. ist im Hinblick auf das Recht, die in Art. 15 Abs. 1 lit. h DS-GVO genannten Informationen zu erhalten, nicht (vollständig) durch die Beigel. erfüllt. Die der Kl. erteilte Auskunft durch die Beigel. ist – gemessen an Art. 15 Abs. 1 lit. h DS-GVO – defizitär. Der Bekl. hat daher zu Unrecht im Hinblick auf die Beschwerde der Kl. v. 18.10.2018 ein aufsichtliches Einschreiten ggü. der Beigel. zur Erfüllung des Auskunftsanspruchs aus Art. 15 Abs. 1 DS-GVO abgelehnt. ...

95 Gem. Art. 15 Abs. 1 DS-GVO hat eine betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf die in den lit. a bis h des Art. 15 Abs. 1 DS-GVO genannten Informationen...

96 a) Zunächst ist der Anwendungsbereich des Auskunftsrechts nach Art. 15 Abs. 1 DS-GVO eröffnet.

97 Die der Erstellung des Scorewerts und dessen Zuordnung zu der Person der Kl. zugrunde liegenden Daten sind personenbezogene Daten der Kl. ...

102 b) Darüber hinaus sind auch die Tatbestandsvoraussetzungen des besonderen Auskunftsrechts aus Art. 15 Abs. 1 lit. h DS-GVO erfüllt.

103 Der Anwendungsbereich des Art. 15 Abs. 1 lit. h DS-GVO knüpft mit dem Begriff „automatisierte Entscheidungsfindung" an den Regelungsbereich des Art. 22 DS-GVO, der unter der amtlichen Überschrift „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling" steht, an.

104 Was hierunter zu verstehen ist, ergibt sich aus Art. 22 Abs. 1 DS-GVO. Nach Art. 22 Abs. 1 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr ggü. rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

105 Die Tätigkeit der Beigel. – die Erstellung des streitgegenständlichen Scorewerts – erfüllt nach Auffassung der Kammer die Voraussetzungen des Art. 22 Abs. 1 DS-GVO.

106 aa) Zunächst handelt es sich bei der Scorewert-Erstellung durch die Beigel. um Profiling iSv Art. 4 Nr. 4 DS-GVO, welche einen Unterfall einer ausschließlich auf einer „automatisierten Verarbeitung" beruhenden Tätigkeit iSv Art. 22 Abs. 1 DS-GVO darstellt (vgl. EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 47). ...

108 Durch die automatisiert und mithilfe eines statistisch-mathematischen Verfahrens erfolgte Ermittlung und Zusammenstellung von personenbezogenen Daten zwecks Profilbildung und der daraus folgenden Erstellung eines finalen Scorewerts betreibt die Beigel. Profiling im o.g. Sinne (so auch OLG Dresden Urt. v. 7.10.2025 – 4 U 884/24 Rn. 30). Diese Verarbeitung erfordert nämlich, wie sich aus dem 71. Erwägungsgrund DS-GVO ergibt, die Bewertung persönlicher Aspekte in Bezug auf die von dieser Verarbeitung betroffene natürliche Person, insb. zur Analyse oder Prognose von Aspekten bzgl. ihrer Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, Vorlieben oder Interessen, Zuverlässigkeit oder ihres Verhaltens, ihres Aufenthaltsorts oder Ortswechsels (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 58). Das Verfahren der Beigel. greift auf personenbezogene Daten zurück, um bestimmte Aspekte, die sich auf natürliche Personen beziehen, zu bewerten, um Aspekte bzgl. ihrer wirtschaftlichen Lage, ihrer Zuverlässigkeit und ihres wahrscheinlichen Verhaltens zu analysieren oder vorherzusagen. Wie die Beigel. selbst erläutert, liefert die von ihr angewandte Methode auf der Grundlage bestimmter Kriterien einen „Scorewert", dh ein Ergebnis, das Rückschlüsse auf die Kreditwürdigkeit der betroffenen Person erlaubt.

109 bb) Die Erstellung des Scorewerts durch die Beigel. erfüllt im vorliegenden Fall den Tatbestand des Art. 22 Abs. 1 DS-GVO.

110 Der EuGH hat auf die Vorlagefrage der Kammer im hiesigen Verfahren entschieden, „dass Art. 22 Abs. 1 DS-GVO dahin auszulegen ist, dass eine ‚automatisierte Entscheidung im Einzelfall' im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet" (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 73).

111 Das erkennende Gericht ist hieran gebunden. Ein Urteil des EuGH im Vorabentscheidungsverfahren bindet nach dessen stRspr das nationale Gericht hinsichtlich der Auslegung oder der Gültigkeit der fraglichen Handlungen der Unionsorgane bei der Entscheidung über den Ausgangsrechtsstreit (vgl. EuGH Urt. v. 16.6.2015 – C-62/14 Rn. 16). Das vorlegende Gericht ist nicht befugt, den Inhalt der Vorabentscheidung zu überprüfen, zu ignorieren oder abzuändern (vgl. Wegener in: Calliess/Ruffert, EUV/AEUV, 6. Aufl. 2022, AEUV Art. 267 Rn. 50 mwN).

112 Diese vom EuGH aufgestellten Voraussetzungen sind im Hinblick auf die Erstellung des Scorewerts durch die Beigel. erfüllt; die Erstellung des in Bezug auf die Kl. ermittelten Scorewerts durch die Beigel. stellt im vorliegenden Fall eine auf einer „ausschließlich auf einer automatisierenden Verarbeitung – einschließlich Profiling – beruhenden Entscheidung, die ihr ggü. rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" gem. Art. 22 Abs. 1 DS-GVO dar.

113 Im Hinblick auf die Auslegung des nicht näher definierten Begriffs „Entscheidung" iSv Art. 22 Abs. 1 DS-GVO ist nach der Rspr. des EuGH – der sich die Kammer anschließt – ein weites Begriffsverständnis zugrunde zu legen.

114 So nimmt der EuGH an, „dass sich bereits aus dem Wortlaut dieser Bestimmung ergibt, dass sich dieser Begriff nicht nur auf Handlungen bezieht, die rechtliche Wirkung gegenüber der betroffenen Person entfalten, sondern auch auf Handlungen, die diese Person in ähnlicher Weise erheblich beeinträchtigen. Die weite Bedeutung des Begriffs ‚Entscheidung' wird durch den 71. Erwägungsgrund DS-GVO bestätigt, wonach eine Entscheidung zur Bewertung persönlicher Aspekte, die eine Person betreffen, ‚eine Maßnahme einschließen (kann)', die entweder ‚rechtliche Wirkung für die betroffene Person' entfaltet oder ‚sie in ähnlicher Weise erheblich beeinträchtigt', wobei die betroffene Person das Recht haben sollte, einer solchen Entscheidung nicht unterworfen zu werden. Nach diesem Erwägungsgrund umfasst der Begriff ‚Entscheidung' beispielsweise die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Da der Begriff ‚Entscheidung' im Sinne von Art. 22 Abs. 1 DS-GVO somit ... mehrere Handlungen umfassen kann, die die betroffene Person in vielerlei Weise beeinträchtigen können, ist dieser Begriff weit genug, um das Ergebnis der Berechnung der Fähigkeit einer Person zur Erfüllung künftiger Zahlungsverpflichtungen in Form eines Wahrscheinlichkeitswerts mit einzuschließen." (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 44 ff.).

115 Ein derart weites Begriffsverständnis ist auch vor dem Hintergrund der Vermeidung von Rechtsschutzlücken im Hinblick auf den Auskunftsanspruch angezeigt: „Wäre Art. 22 Abs. 1 DS-GVO hingegen dahin auszulegen, dass die Eigenschaft einer ‚automatisierten Entscheidung im Einzelfall' in einer Situation wie der vorliegenden nur der Entscheidung des Dritten gegenüber der betroffenen Person zuerkannt werden könne, ergäbe sich daraus eine Rechtsschutzlücke. Zum einen wäre nämlich eine Gesellschaft wie die Beigel. nicht verpflichtet, Auskunft über die zusätzlichen Informationen zu erteilen, auf die die betroffene Person nach Art. 15 Abs. 1 lit. h DS-GVO Anspruch habe, da sie nicht diejenige wäre, die eine ‚automatisierte Entscheidung' im Sinne dieser Bestimmung und folglich im Sinne von Art. 22 Abs. 1 DS-GVO treffe. Zum anderen könnte der Dritte, dem der Wahrscheinlichkeitswert mitgeteilt wird, diese zusätzlichen Informationen nicht vorlegen, da er nicht darüber verfüge" (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 23).

116 Insofern hat der EuGH herausgestellt, dass die weite Bedeutung des Begriffs „Entscheidung" iSv Art. 22 Abs. 1 DS-GVO den wirksamen Schutz verstärkt, auf den diese Bestimmung abzielt (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 60). So könnte die betroffene Person zum einen bei der Wirtschaftsauskunftei, die den sie betreffenden Wahrscheinlichkeitswert ermittelt, ihr Recht auf Auskunft über die in Art. 15 Abs. 1 lit. h DS-GVO genannten spezifischen Informationen nicht geltend machen, wenn keine automatisierte Entscheidungsfindung durch dieses Unternehmen vorliegt. Zum anderen wäre der Dritte – unter der Annahme, dass die von ihm vorgenommene Handlung unter Art. 22 Abs. 1 DS-GVO fiele, da sie die Voraussetzungen für die Anwendung dieser Bestimmung erfüllte – nicht in der Lage, diese spezifischen Informationen vorzulegen, weil er darüber im Allgemeinen nicht verfügt (EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 63).

117 Genau diese Situation, die es nach der vom EuGH ins Feld geführten teleologischen Auslegung des Auskunftsrechts nach Art. 15 Abs. 1 lit. h DS-GVO iVm Art. 22 Abs. 1 DS-GVO zu vermeiden gilt, würde aber im Falle der Kl. eintreten, wenn sie nicht Auskunft gem. Art. 15 Abs. 1 lit. h DS-GVO von der Beigel. verlangen könnte.

118 So hat die D-Bank auf die gerichtliche Anfrage hin mit Schreiben v. 20.6.2025 mitgeteilt, dass man nicht mehr beant-

worten könne, warum der Kreditantrag der Kl. im Jahre 2018 abgelehnt worden sei, welche Kriterien hierbei eine Rolle gespielt hatten und ob die Kreditablehnung maßgeblich oder ausschließlich auf dem übermittelten Bonitätsscore beruhte, da man die Antragsdaten der Kl. bereits gelöscht habe.

119 Weiterhin stünde der Kl. ggü. der D-Bank nur dann das Auskunftsrecht nach Art. 15 Abs. 1 lit. h DS-GVO zur Seite, wenn die Entscheidung der D-Bank über die Kreditvergabe selbst eine „automatisierte Entscheidungsfindung" iSv Art. 22 Abs. 1 DS-GVO darstellen würde, was jedenfalls dann zu verneinen wäre, wenn die abschließende Entscheidung über die Kreditvergabe von einer natürlichen Person getroffen wird.

120 Kann die Kl. bei der D-Bank aber keine Auskunft bekommen, jedenfalls deshalb, weil ihre Daten bei der D-Bank längst gelöscht worden sind, und stünde ihr nicht das Auskunftsrecht ggü. der Beigel. aus Art. 15 Abs. 1 lit. h DS-GVO zur Seite, würde eine Rechtsschutzlücke entstehen.

121 Zwar entfaltet, wie die Beigel. und der Bekl. zutreffend ausführen, die Scorewert-Erstellung durch die Beigel. (als automatisierte Entscheidung in Gestalt des Profilings) ggü. der Kl. zunächst keine unmittelbare rechtliche Wirkung; eine solche rechtliche (Außen-)Wirkung entsteht erst infolge der Entscheidung des Dritten, etwa über die Kreditvergabe. Allerdings wird die Kl. schon durch die Scorewert-Erstellung in „ähnlicher Weise erheblich beeinträchtigt", Art. 22 Abs. 1 Alt. 2 DS-GVO.

122 Denn nach Auffassung der Kammer ist die Scorewert-Erstellung als solche schon geeignet, eine Vorgriffswirkung auf die Begründung, Änderung oder Aufhebung einer rechtlichen Position der betroffenen Person, etwa im Hinblick auf eine Kreditvergabe, zu entfalten, weil hierbei eine Einschätzung ihrer Kreditwürdigkeit getroffen wird. Zwar wird in der obergerichtlichen Zivilrechtsprechung eine rechtliche oder dieser ähnliche Wirkung als „bloßes Internum" abgelehnt, wenn der Scorewert nicht an Vertragspartner herausgegeben wird (OLG München Hinweisbeschl. v. 3.2.2025 – 24 U 3326/24 e Rn. 28; OLG Stuttgart Hinweisbeschl. v. 18.3.2025 – 9 U 20/25 Rn. 25; OLG Brandenburg Beschl. v. 7.7.2025 – 1 U 68/24 Rn. 47 ff.). Diese Einschätzung der Kreditwürdigkeit ist im vorliegenden Fall aber tatsächlich einem Dritten – der D-Bank – zur Kenntnis gegeben worden, weshalb allein schon aus diesem Grund nicht von einem bloßen Internum ohne rechtliche Außenwirkung ausgegangen werden kann.

123 Ob das von der Beigel. vorgenommene Profiling die betroffene Person „in ähnlicher Weise erheblich beeinträchtigt" (die einer rechtlichen Wirkung gleichkommt), setzt nach Auffassung der Kammer nicht voraus, dass ein Dritter den Scorewert auch tatsächlich als einziges oder ausschließliches Kriterium verwendet, um zu entscheiden, ob dieser ein Vertragsverhältnis zu dem Betroffenen eingeht.

124 Die noch zur alten Rechtslage ergangene Rspr. des BGH (BGH MMR 2014, 489: „Von einer automatisierten Einzelentscheidung kann im Falle des Scorings nur dann ausgegangen werden, wenn die für die Entscheidung verantwortliche Stelle eine rechtliche Folgen für den Betroffenen nach sich ziehende oder ihn erhebliche beeinträchtigende Entscheidung ausschließlich aufgrund eines Score-Ergebnisses ohne weitere inhaltliche Prüfung trifft, nicht aber, wenn die mittels automatisierter Datenverarbeitung gewonnenen Erkenntnisse lediglich Grundlage für eine von einem Menschen noch zu treffende abschließende Entscheidung sind.") ist durch das Inkrafttreten der DS-GVO überholt.

125 Denn iRd Auskunftsanspruchs gem. Art. 15 Abs. 1 lit. h DS-GVO ist es unerheblich, ob die Kl. ausreichend konkret vorgetragen und bewiesen hat, dass der Verantwortliche – die Beigel. – sie (nur) mit der Übermittlung dieses Bonitätsscores an Dritte einer gem. Art. 22 Abs. 2 bis 4 DS-GVO iVm nationalen Datenschutzvorschriften unzulässigen automatisierten Entscheidung mit rechtlichen Wirkungen oder erheblichen Beeinträchtigungen unterworfen hat. Denn Zweck des Art. 22 DS-GVO ist es, Personen vor den besonderen Risiken für ihre Rechte und Freiheiten zu schützen, die mit der automatisierten Verarbeitung personenbezogener Daten – einschließlich Profiling – verbunden sind, wie durch Erwägungsgrund Nr. 71 herausgestellt wird. Diese Risiken ergeben sich insb. aus der Bewertung persönlicher Aspekte und Daten, wie sie auch bei der Ermittlung der Wahrscheinlichkeit eines Forderungsausfalls heranzuziehen sind. Der Umfang des Auskunftsanspruchs aus Art. 15 Abs. 1 lit. h DS-GVO kann daher nicht maßgeblich davon abhängen, ob und inwieweit mit der auf einem Profiling beruhenden Bonitätsauskunft der Beigel. jeweils konkret gegen Art. 22 Abs. 1 und Abs. 4 DS-GVO nachweislich verstoßen wird. Vielmehr stehen mit Blick auf Zweck und Zielrichtung der Vorschrift der betroffenen Person Auskunftsrechte jedenfalls in den Fällen zu, in denen die Verarbeitung personenbezogener Daten zu einer automatisierten Entscheidungsfindung in Form einer Bonitätsscoreermittlung führt und insb. auf einem Profiling beruht, wie sich auch aus der Formulierung der Vorschrift selbst ergibt. Bestätigt wird dies durch den Erwägungsgrund Nr. 63 S. 3 DS-GVO, der gleichfalls in Fällen eines Profiling besondere Auskunftsrechte der betroffenen Person vorsieht (vgl. OLG Dresden Urt. v. 7.10.2025 – 4 U 884/24 Rn. 31).

127 Zunächst ist festzuhalten, dass aus einer ökonomischen Perspektive heraus Scoring allgemein als sinnvoll eingestuft wird: Nicht nur für Kreditinstitute als Darlehensgeber, sondern für alle Unternehmen, die bei ihren Geschäften kreditorische Risiken eingehen, sind Informationen über die Kreditwürdigkeit ihrer (potenziellen) Kunden bedeutsam. Der Bonitätsprüfung liegt im Allgemeinen ein (Kredit-)Scoring zugrunde (vgl. Taeger BKR 2024, 41 (42)). Ein Kreditinstitut ist gem. § 18a Abs. 1 KWG und jeder Darlehensgeber gem. §§ 505a, 505b BGB verpflichtet, vor Abschluss eines Verbraucherdarlehensvertrags die Kreditwürdigkeit des Verbrauchers zu prüfen. In der Praxis kommen Kreditinstitute ihrer Verpflichtung zur Minimierung von Risiken mit einem internen Kreditscoring nach, in das idR auch die von einer Wirtschaftsauskunftei wie der Beigel. übermittelten Scorewerte über die Kreditausfallwahrscheinlichkeit eines potenziellen Darlehensnehmers einfließen, um das interne Rating zuverlässiger zu machen (vgl. Thiele/v. Keitz/Brücks, Internationales Bilanzrecht, 2023, S. 342). Auch der BGH hat angemerkt, dass die Erteilung von zutreffenden Bonitätsauskünften für das Funktionieren der Wirtschaft von erheblicher Bedeutung ist und Angaben einer Wirtschaftsauskunftei, die geeignet sind, etwaige Kreditgeber zu einer sorgfältigen Bonitätsprüfung zu veranlassen, für das Kreditgewerbe erforderlich sind (BGH Urt. v. 22.2.2011 – VI ZR 120/10 [= MMR 2011, 409] Rn. 21).

128 Im Gesetzentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die VO (EU) 2016/679 und zur Umsetzung der RL (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) heißt es zu § 31 (Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften): „Die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften bilden das Fundament des deutschen Kreditwesens und damit auch der Funktionsfähigkeit der Wirtschaft ... Für die Verwendung des Score-Wertes wird auf die Kriterien der derzeitigen § 28a Abs. 1 und § 28b zurückgegriffen, die die im Wirtschaftsleben bedeutsame Tätigkeit von Auskunfteien sowie die Ermittlung von Score-Werten grds. ermöglichen ... Insoweit wird für alle Beteiligten Sicherheit in der Weise geschaffen, dass Scoringverfahren und Kreditinformationssysteme mit der Einmeldung von Positiv- und Negativ-

daten, die zB durch Kreditinstitute, Finanzdienstleistungsunternehmen, Zahlungsinstitute, Telekommunikations-, Handels-, Energieversorgungs- und Versicherungsunternehmen oder Leasinggesellschaften erfolgt, prinzipiell weiter zulässig bleiben. Sie werden nach wie vor als wichtige Voraussetzungen für das Wirtschaftsleben angesehen" (BT-Drs. 18/11325, 101 f.).

129 Dass der Einsatz von automatisierten Verfahren mittels IT-Systemen zur Bewertung der Kreditwürdigkeit von Personen besondere Gefahren mit sich bringt und eine hiervon betroffene Person deshalb besonders schutzwürdig ist, ergibt sich aus der Wertung des Unionsrechts. Sowohl in dem Erwägungsgrund 56 RL (EU) 2023/2225 des Europäischen Parlaments und des Rates v. 18.10.2023 über Verbraucherkreditverträge und zur Aufhebung der RL 2008/48/EG (Verbraucherkredit-RL (Abl. L 2023/2225 v. 30.10.2023)) als auch in Erwägungsgrund 58 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der RL 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz (Abl. L 2024/1689 v. 12.7.2024)) heißt es, dass KI-Systeme, die zur Bewertung der Kreditwürdigkeit natürlicher Personen verwendet werden, als Hochrisiko-KI-Systeme eingestuft werden (sollten), da sie den Zugang dieser Personen zu Finanzmitteln oder wesentlichen Dienstleistungen wie Wohnraum, Elektrizität und TK-Dienstleistungen bestimmen.

130 Dass zahlreiche Banken und Kreditinstitute auf „externes Scoring" bei ihrer Entscheidung, ob und in welcher Höhe ein Kredit vergeben werden soll, zurückgreifen, lässt sich bereits anhand der allgemein zugänglichen Informationen, etwa auf den Internetseiten der Einrichtungen, ablesen. ...

134 Eine Kreditvergabe mag also trotz eines grds. ausreichenden Scorewerts (aus anderen Gründen, wie etwa des Fehlens von Sicherheiten oder Zweifeln am Erfolg einer zu finanzierenden Investition) versagt werden; ein nicht ausreichender Scorewert hingegen wird jedenfalls im Bereich der Verbraucherdarlehen häufig und auch dann zur Versagung eines Kredits führen, wenn etwa eine Investition iÜ als lohnend erscheint. Dass Scorewerten bei der Kreditvergabe und der Gestaltung ihrer Bedingungen die bedeutende Rolle zukommt, zeigen auch Erfahrungen aus der behördlichen Datenschutzaufsicht (s. LfDI BW, Neue Broschüre: Scoring – solide Prognose oder miese Num..., https://www.badenwuerttemberg.datenschutz.de/wp-content/uploads/2021/06/20210629_Scoring_web.pdf ... Der Dritte muss seine Kredit-Entscheidung zwar nicht allein vom Scorewert abhängig machen, tut es in aller Regel jedoch maßgeblich.

135 Da sonach bereits anzunehmen ist, dass ein von der Beigel. erstellter Wahrscheinlichkeitswert über eine Person hinsichtlich deren Fähigkeit, künftig einen Kredit zu bedienen, schon an sich – ohne Weiteres – geeignet ist, die betroffene Person zumindest erheblich zu beeinträchtigen (so EuGH Urt. v. 7.12.2023 – C-634/21 [= ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild = MMR 2024, 153 mAnm Radtke] Rn. 49), ist dies nach Auffassung der Kammer im vorliegenden Fall erst recht in Bezug auf der Erstellung eines für die Team Bank eigens berechneten Scorewerts durch die Beigel. gegeben. ...

139 Auf die von dem Bevollmächtigten der Kl. aufgeworfene Frage, ob die D-Bank selbst durch die Verwendung einer Software die Kreditentscheidung automatisiert getroffen hat oder die Entscheidung durch einen Menschen unter Zuhilfenahme der Software erfolgt sei, kommt es nicht an. Denn die automatisierte Entscheidung iSv Art. 15 Abs. 1 lit. h DS-GVO iVm Art. 22 Abs. 1 DS-GVO erfolgte durch die Beigel.; diese erfüllt das vom EuGH aufgestellte Kriterium der Maßgeblichkeit, unabhängig davon, ob sich die D-Bank wiederum einer Software bei ihrer Kreditentscheidung bedient hatte.

140 c) Sind demnach die Voraussetzungen des Auskunftsanspruchs nach Art. 15 Abs. 1 lit. h DS-GVO erfüllt, folgt daraus ein Recht auf Informationen über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Artikel 22 Abs. 1 und Abs. 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

141 Was unter „aussagekräftigen Informationen über die involvierte Logik" zu verstehen ist, hat der EuGH im Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] dahingehend präzisiert, dass der betroffenen Personen „anhand der maßgeblichen Informationen in präziser, transparenter und leicht zugänglicher Form die Verfahren und Grundsätze zu erläutern sind, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – beispielsweise – eines Bonitätsprofils konkret angewandt wurden" (EuGH Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz]).

142 Welche Informationen hierzu erforderlich sind, hängt wiederum von den Umständen des konkreten Einzelfalls ab. Hierbei kommt es darauf an, welche Informationen betreffend die Kl. – unter Berücksichtigung derer, die ihr bereits erteilt wurden oder ihr sonst bekannt sind – im konkreten Fall noch benötigt werden, um sie in die Lage zu versetzen, ihre datenschutzrechtlichen Ansprüche, wirksam geltend machen zu können.

143 Denn die zu erteilenden Auskünfte sind nach der Rspr. des EuGH (Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz]) maßgeblich am Transparenzgebot gem. Art. 12 Abs. 1 DS-GVO sowie an der teleologischen Auslegung des Umfangs und Inhalts des Auskunftsanspruchs aus Art. 15 Abs. 1 lit. h DS-GVO im Lichte der Betroffenenrechte nach Art. 22 Abs. 3 DS-GVO auszurichten. Zum einen verpflichtet Art. 12 Abs. 1 DS-GVO den Verantwortlichen dazu, der betroffenen Person die relevanten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zur Verfügung zu stellen (EuGH Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 49). Zum anderen soll das Auskunftsrecht der betroffenen Person ermöglichen, ihre datenschutzrechtlichen Ansprüche wirksam geltend machen zu können. Bei automatisierten Entscheidungen soll die betroffene Person durch die erteilten Informationen in die Lage versetzt werden, ihre Rechte aus Art. 22 Abs. 3 DS-GVO – insb. das Recht auf Darlegung des eigenen Standpunkts sowie auf Anfechtung der Entscheidung – wirksam auszuüben (vgl. EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 53 ff.). Daraus folgt zugleich, dass der Betroffene ein Recht „auf Erläuterung des Verfahrens" sowie der „Grundsätze" hat, die bei der automatisierten Verarbeitung seiner personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – zB eines Bonitätsprofils – konkret angewandt wurden (vgl. EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 58). Die DS-GVO verpflichtet den Verantwortlichen zwar „nicht unbedingt zu einer ausführlichen Erläuterung der verwendeten Algorithmen oder zur Offenlegung des gesamten Algorithmus" (vgl. EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 60). Die „aussagekräftigen Informationen über die involvierte Logik" einer automatisierten Entscheidungsfindung iSv Art. 15 Abs. 1 lit. h

DS-GVO müssen aber das Verfahren und die Grundsätze, die konkret zur Anwendung kommen, so beschreiben, dass die betroffene Person nachvollziehen kann, welche ihrer personenbezogenen Daten iRd in Rede stehenden automatisierten Entscheidungsfindung auf welche Art verwendet wurden, ohne dass die Komplexität der im Rahmen einer automatisierten Entscheidungsfindung vorzunehmenden Arbeitsschritte den Verantwortlichen von seiner Erläuterungspflicht entbinden könnte (vgl. EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 61). Zudem sollten sich die Erläuterungen sowohl auf die Funktionsweise des automatisierten Entscheidungsmechanismus als auch auf das konkrete Ergebnis beziehen, zu dem die Entscheidung geführt hat (EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 57). Abstrakte Informationen genügen insofern nicht. Erforderlich ist vielmehr eine individualisierte Darlegung der Verfahren und Grundsätze, die bei der Verarbeitung – etwa zur Erstellung eines Bonitätsprofils – „konkret" (EuGH, aaO [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 61, 66) angewandt wurden. Hierbei ist auch den Gefahren zu begegnen, die für den Betroffenen durch eine – oft sogar ohne dessen Kenntnis erfolgte – automatisierte Entscheidungsfindung insb. Profiling iSv Art. 22 Abs. 1 DS-GVO ausgehen.

144 Maßstab für den geschuldeten Informationsumfang ist somit die „Aussagekraft" der Informationen. Mit diesem unbestimmten Rechtsbegriff adressiert Art. 15 Abs. 1 lit. d DS-GVO zum einen das Erfordernis, dass die Information ein gewisses Mindestmaß an Verständlichkeit für die betroffene Person aufweisen muss. Aufgrund der o.g. Auswirkungen eines solchen zur Bonitätsprüfung maßgeblichen Profilings muss der Betroffene zum anderen auch in die Lage versetzt werden, sein Verhalten auszurichten, indem er zB solche Faktoren, die zu einem für ihn ungünstigen Score beitragen, durch eigenes Verhalten, etwa Wohnortwechsel, Umstellung seines Verhaltens etwa im Hinblick auf die Häufigkeit der Eröffnung von Konten und Kreditanfragen etc. beeinflussen bzw. verändern kann. Hierbei ist ein objektiver Maßstab zugrunde zu legen, wonach auf einen Betroffenen mit durchschnittlichen Fähigkeiten und Erkenntnismöglichkeit abzustellen ist.

145 d) Diesen Anforderungen genügt die von der Beigel. der Kl. erteilte Auskunft im Hinblick auf die Bewertung der Kl. mit einem Scorewert von 85,96% ... nicht. Der Anspruch aus Art. 15 Abs. 1 lit. h DS-GVO ist daher nicht durch die der Kl. bereits erteilten Auskünfte erfüllt worden.

146 Zwar sind Informationen darüber, dass eine „automatisierte Entscheidungsfindung einschließlich Profiling" durch die Beigel. vorliegt, vorhanden.

147 Auch informiert die Beigel. über die „Tragweite" des Scorings auf ihrer Webseite öffentlich zugänglich. Auch die angestrebten „Auswirkungen" der automatisiert erstellten Scorewerte sind angesichts des der Kl. bekannten Geschäftszwecks der Beigel., ihren Kunden Anhaltspunkte für Entscheidungen über Geschäfte mit vom Scoring betroffenen Personen mit kreditrelevantem Inhalt zu treffen, offenbart. Jedoch genügen vor dem Hintergrund des Transparenzgebots allgemein gehaltene Information, etwa über die Webseite der Beigel., ohnehin nicht, den Informationspflichten über die Datenverarbeitung ausreichend nachzukommen. Sinn und Zweck des Auskunftsrechts ist es, es der betroffenen Person problemlos und in angemessenen Zeitabständen zu ermöglichen, sich der Verarbeitung der sie betreffenden Daten bewusst zu werden und die Rechtmäßigkeit dieser Verarbeitung überprüfen zu können. Die Informationen müssen sich daher insofern direkt an den Betroffenen richten, als ihm eine individuelle Überprüfung seiner bei der Beigel. gespeicherten Daten ermöglicht wird.

148 Hinsichtlich des im Auskunftsschreiben v. 10.7.2018 samt Anlagen mitgeteilten, der D-Bank übermittelten Scorewerts nach „individuellen SCHUFA-Scorekarte D-Bank III" wird die Kl. zwar über den auf sie persönlich bezogenen Prozentsatz der Erfüllungswahrscheinlichkeit (von 85,96%) sowie darüber informiert, welche personenbezogenen Daten über die Kl. bei der Beigel. gespeichert sind. In der als Anlage beigefügten tabellarischen Aufstellung der von der Beigel. an deren Vertragspartner übermittelten Wahrscheinlichkeitswerte im Hinblick auf die Kl., lässt sich zwar entnehmen, dass die Kreditaktivität der Kl. als deutlich überdurchschnittliches Risiko (- -), die Kreditnutzung als unterdurchschnittliches Risiko (+) und die Länge der Kredithistorie als überdurchschnittliches Risiko (-) in Ansatz gebracht worden sind. Die allgemeinen Daten zur Kl. sind als deutlich unterdurchschnittliches Risiko (+ +) in Ansatz gebracht worden. Hierbei begegnet es keinen Bedenken, dass die entsprechenden Erläuterungen sich erst in der Legende zu der Tabelle finden, da diese leicht aufzufinden und auch hinreichend klar erläutert wird, sodass die geforderte Transparenz für die Kontrolle der Richtigkeit der Daten gegeben ist. Der Tabelle lässt sich entnehmen, dass zB das Kriterium „Anschriftendaten" nicht verwendet wurde (hier Kürzel „n/v").

149 Die Beigel. informiert indes lediglich allgemein über die Datenarten, die von ihr zur Score-Berechnung verwendet werden, namentlich Allgemeine Daten (zB Geburtsdatum, Geschlecht oder Anzahl im Geschäftsverkehr verwendeter Anschriften), bisherige Zahlungsstörungen, Kreditaktivität letztes Jahr, Kreditnutzung, Länge Kredithistorie sowie Anschriftendaten (nur wenn wenige personenbezogene kreditrelevante Informationen vorliegen). Nach Angaben der Beigel. fließt aber nicht jede Datenart auch in jede einzelne Scoreberechnung mit ein. Hierüber aber muss die Beigel. aber aufklären. Es fehlen sonach Angaben, ob und ggf. welche der eingangs des Schreibens aufgeführten personenbezogenen Daten der Kl. genau (alle Daten oder nur einige?) verwendet hat. Insb. enthält die Tabellenspalte „Allgemeine Daten" keine weiteren Angaben, welche Daten im Falle der Kl. im vorliegenden Fall für die Berechnung des Team Bank-Scorewerts verwendet worden sind und mit welcher Einzelgewichtung. Diese Angaben sind auch nicht offensichtlich oder aus dem Gesamtzusammenhang der übrigen Angaben der Beigel. wie den allgemeinen oder online abrufbaren Informationen zu ermitteln, da nicht erklärt wird, worauf der Wert individuell – bezogen auf die Kl. – beruht oder wie ihre hier konkret herangezogenen personenbezogenen Daten im Einzelnen gewichtet wurden. Die Auskunft der Beigel. erschöpft sich vielmehr in abstrakten Erklärungen und allgemeinen Angaben, ohne dass diese individuellen Bezug auf die Kl. nehmen. Es fehlt auch eine leicht verständliche und nachvollziehbare Beschreibung, warum die von der Beigel. gebildeten einzelnen Datenkategorien, wie etwa Kreditaktivität, Kredithistorie sowie die allgemeinen Daten, etwa zum Alter und Wohnort, für das Profiling aussagekräftig sind.

150 Diese Informationspflicht besteht insb. auch deshalb, weil aus den von der Beigel. der Kl. am 10.7.2018 übermittelten zweiseitigen Auflistung der von den Vertragspartnern der Beigel. im Hinblick auf die Kl. zur Verfügung gestellten Informationen sowie die von den Vertragspartnern der Beigel. im Hinblick auf die Kl. gestellten Anfragen nichts dafür ersichtlich ist, dass die Kl. bislang in Zahlungsschwierigkeiten gewesen wäre oder sonstige Anhaltspunkte ersichtlich sind, warum die Beigel. im Hinblick auf die Kl. ein „deutlich erhöhtes bis hohes Risiko" angenommen hat. Es besteht daher Aufklärungsbedarf, worauf diese Einstufung mit 85,96% und einem deutlich erhöhten bis hohen Risiko beruht. Denn für die Kl. ist unter Berücksichtigung der bei der Beigel. über sie gespeicherten Informationen über ihre finanziellen Aktivitäten ein Score von 85,96% ungewöhnlich.

151 Wenn die Beigel. lediglich die einzelnen Kategorien aufführt, die abstrakt den Scorewert bestimmen, so muss dies inhaltlich konkretisiert und auf die Person der Kl. hin bestimmt werden. Daran fehlt es hier. Die Beigel. führt nicht aus, welcher prozentuale Wert in jeder Kategorie im Einzelfall auf die Kl. entfällt, also inwieweit die Kl. zB in der Kategorie „Kreditaktivität letztes Jahr", den allgemein von der Beigel. errechneten Wert voll erreicht oder die Beigel. einen Abschlag vornimmt, und wenn ja, warum. ...

153 e) Dies zugrunde gelegt, schuldet die Beigel. nach der Rechtsauffassung der Kammer der Kl., in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache in Bezug auf den ermittelten D-Bank Scorewert von 85,96% eine einzelfallbezogene Begründung, warum ihr Score mit 85,96% berechnet wurde und nicht mit einem anderen Ergebnis.

154 Unter Berücksichtigung der Umstände des konkreten Falls und mit Rücksicht auf die bereits erfolgten Auskünfte der Beigel. ist der Kl. nach Auffassung der Kammer noch mitzuteilen:

155 (1) Welche personenbezogenen Daten der Kl. sie für die Erstellung des Scorewerts konkret genutzt hat und welche sie zwar erhoben, aber nicht verwertet hat. Dazu gehört die Information, warum die einzelnen verwendeten Daten für das Profiling der Kl. im konkreten Fall bzgl. des D-Bank-Scores relevant und aussagekräftig sind, welchen Aussagewert sie also für die Bewertung ihrer Bonität haben. Die Information hierüber muss der Kl., soweit möglich, eine Steuerung ihres Verhaltens ermöglichen, indem ihr aufgezeigt wird, ob das einzelne Datum in ihrem Fall gut oder schlecht für die Bewertung ihrer Bonität ist. Weiter gehört hierzu die Information, ob Daten in die Scorewert-Berechnung eingeflossen sind, die mittelbar aus den über die Kl. gespeicherten Informationen abgeleitet werden und wenn ja, welche.

156 (2) In welcher Gewichtung die Daten Eingang in die Berechnung des Scorewerts hatten. Welcher Darstellungsweise die Beigel. sich bedient, bleibt ihr unter Vorbehalt der Lesbarkeit und Verständlichkeit vorbehalten. Sachgerecht könnte insoweit ein Ranking sein, in dem die zur Berechnung genutzten Daten in ab- oder aufsteigender Reihenfolge ihrer Bedeutung für das berechnete Ergebnis dargestellt werden.

157 (3) Warum der im Falle der Kl. errechnete Scorewert von 85,96% als „deutlich erhöhtes bis hohes Risiko" bewertet worden ist.

158 f) Weitergehende Auskünfte, die auch die Offenbarung der Score-Formel bzw. den verwendeten Algorithmus umfassen, kann die Kl. – unter Berücksichtigung ihres Informationsinteresses einerseits und etwaigen gegenläufigen schützwürdigen Interessen der Beigel. oder Dritter – nicht verlangen.

159 Der Auskunftsanspruch wird beschränkt durch die Rechte und Freiheiten anderer Personen, Art. 15 Abs. 4 DS-GVO. Hierzu gehören auch Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insb. das Urheberrecht an Software, wozu der von der Beigel. verwendete Algorithmus oder auch die anonymisierten und anhand von mathematisch-statistischen Verfahren ausgewerteten und gewichteten Daten der jeweiligen Vergleichsgruppen (Altfälle) auch in den einzelnen Datenarten gehören (vgl. OLG Dresden Urt. v. 7.10.2025 – 4 U 884/24 Rn. 40).

160 Geschäftsgeheimnisse sind als allgemeiner Grundsatz des Unionsrechts sowie grundrechtlich nach Art. 16, 17 GRCh geschützt. Auch erkennt Erwägungsgrund 63 DS-GVO den Schutz von Geschäftsgeheimnissen ausdrücklich an. Um eine konkrete Auskunft zu verweigern, genügt aber nicht ein pauschaler Verweis auf ein Geschäftsgeheimnis durch die Beigel.

161 Nach der Rspr. des EuGH sind im Fall eines Konflikts zwischen der Ausübung des Rechts auf vollständige und umfassende Auskunft über die personenbezogenen Daten zum einen und den Rechten oder Freiheiten anderer Personen zum anderen die fraglichen Rechte gegeneinander abzuwägen (EuGH Urt. v. 27.2.2025 – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 72).

162 Sofern Geschäftsgeheimnisse oder sonstige schutzwürdige Interessen Dritter betroffen sind, hat die Beigel. die Aspekte, die in die Abwägung einfließen sowie die Abwägungsgründe zu erläutern, damit diese einer Überprüfung durch den Bekl. als Aufsichtsbehörde und letztlich auch einer gerichtlichen Überprüfung zugänglich sind.

163 Es ist nichts dafür ersichtlich, dass die – wie unter 3.e) [= Rn. 153] von der Kammer konkretisierte – geschuldete Auskunft durch die Beigel. geeignet wäre, zu einer Beeinträchtigung der Rechte und Freiheiten anderer Personen zu führen, insb., weil sie durch die DS-GVO geschützte personenbezogene Daten Dritter oder ein Geschäftsgeheimnis iSv Art. 2 Nr. 1 RL 2016/943 enthalten. Zum einen kann nach Auffassung der Kammer die Beigel. ihrer Auskunftspflicht nachkommen, ohne personenbezogene Daten Dritter preiszugeben.

164 Zum anderen steht der Kl. – entgegen ihrer nunmehr in der mündlichen Verhandlung geäußerten Begehr, auch die Score-Formel zu erhalten – ein Auskunftsrecht nur insoweit zu, als ihr damit eine Überprüfung der Bonitätsscorewerte auf Fehler und mangelnde Plausibilität ermöglicht wird. Allein zu diesem Zweck schuldet die Beigel. eine auch für einen Laien verständliche Information, die diesem eine Prüfung ermöglicht, ob die betreffenden Daten richtig sind und ob sie in zulässiger Weise verarbeitet werden (vgl. EuGH, aaO – C-203/22 [= ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz] Rn. 53).

165 Eine Verpflichtung der Beigel., den ihren Scorewerten zugrundeliegenden Algorithmus oder das statistische Verfahren, das der Scorewert-Bildung zugrunde liegt, mitzuteilen, besteht hier nicht. ...

168 Die Kammer kann für die hier allein streitgegenständliche Frage der Erfüllung der Auskunftspflicht nach Art. 15 Abs. 1 lit. h DS-GVO iÜ offenlassen, ob die Tätigkeit der Beigel., also die Erstellung eines Scorewerts als solche nach Maßgabe von Art. 22 DS-GVO, der in Absatz 1 ein grundsätzliches Verbot der automatisierten Datenverarbeitung – einschließlich Profiling – statuiert, rechtswidrig ist. Dies wäre dann der Fall, wenn kein Erlaubnistatbestand nach Absatz 2 der Norm eingreift. Der Anwendungsbereich des Art. 15 Abs. 1 lit. b DS-GVO verweist lediglich iSe Tatbestandsverweisung auf das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. in Art. 22 Abs. 1 und Abs. 4 DS-GVO, ohne dass es für die Frage, ob ein Auskunftsrecht nach Art. 15 Abs. 1 lit. h DS-GVO besteht, auf die Rechtmäßigkeit der Scorewert-Erstellung als solcher ankommt. ...

Anmerkung

VorsRiVG i.R. Hans-Hermann Schild, Wiss. Mitarb. (Öffentliches Recht, IT-Recht & Umweltrecht), Universität Kassel

Was lange währt, wird endlich gut. 23 Monate nach der EuGH-Entscheidung zum SCHUFA Scoring (EuGH ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild) hat nun das VG Wiesbaden über die Frage des Auskunftsanspruchs der Kl. aus Art. 15 Abs. 1 lit. h DS-GVO im Sinne des Kl. gegen die Aufsichtsbehörde und die Beigel. entschieden. Für die Entscheidung war die in diesem Verfahren notwendige Vorlagefrage und noch eine zweite Entscheidung des EuGH zur Frage der Auskunft nach

Art. 15 Abs. 1 lit. h DS-GVO in dem Verfahren Dun & Bradstreet Austria (EuGH ZD 2025, 261 mAnm Radtke = MMR 2025, 421 mAnm Hense/Niekrenz) von besonderer Bedeutung für den Ausgang des vorliegenden Verfahrens.

Nicht entscheidungserheblich war dabei, dass vorliegend die Erstellung und Verarbeitung eines Scorewerts als solchem gegen das grundsätzliche Verbot der automatisierten Entscheidung im Einzelfall – einschließlich Profiling – nach Art. 22 Abs. 1 DS-GVO verstoßen haben dürfte und damit rechtswidrig war. Insoweit weist die Kammer zu Recht nur kurz darauf hin, dass das Auskunftsrecht nach Art. 15 Abs. 1 lit. h DS-GVO unabhängig davon besteht, ob die Scorewert-Erstellung als solche rechtmäßig war.

1. Rechtmäßigkeit der Scorewert-Nutzung

Zwar besteht eine Verpflichtung der Banken zur Überprüfung der Kreditwürdigkeit, gerade bei Verbraucher-Darlehensverträgen. Wenn eine Bank diese Prüfung aber primär auf einen Score-Ersteller abgewälzt (hier die SCHUFA) und dieser Scorewert iRe automatisierten Verfahrens über eine voll automatisierte Kreditentscheidung zu einer negativen Kreditprüfung führt, liegt darin eine automatisierte Einzelfallentscheidung iSv Art. 22 Abs. 1 DS-GVO durch den Scorewert-Ersteller als Verantwortlichen (EuGH ZD 2024, 157 mAnm Söbbing/Schwarz und mAnm Schild). Allerdings fehlt es an einer nationalen Rechtsgrundlage hierfür (s. Art. 22 Abs. 2 lit. b DS-GVO). Soweit sich die Beigel. bzw. auch der Bekl. auf § 31 BDSG beziehen, geht dies fehl. § 31 BDSG ist nach der klaren Aussage des Vertreters der Bundesregierung in der mündlichen Verhandlung in der Rs. C-634/21 beim EuGH am 26.1.2023 gerade keine datenschutzrechtliche Norm und damit keine Erlaubnisnorm nach Art. 22 Abs. 2 lit. b DS-GVO. § 31 BDSG ist damit allenfalls eine Norm im Bereich des Verbraucherschutzes. Eine Erkenntnis, die spätestens seit der mündlichen Verhandlung in Luxemburg in dem vorliegenden SCHUFA-Verfahren allen Beteiligten bekannt ist. Damit fehlt es für die Score-Erstellung und erst recht für deren Anwendung an einer Rechtsgrundlage, mit der Folge, dass die Datenverarbeitung vorliegend rechtswidrig war. Wie sich dann der Bekl. in dem vorliegenden Verfahren noch darauf berufen kann, dass ein von der SCHUFA vorgelegtes Gutachten die Erfüllung der Anforderungen des § 31 Abs. 1 BDSG bestätigt habe und damit die Zulässigkeit der Datenverarbeitung und deren Richtigkeit belegt seien, erschließt sich nicht. Das Gutachten hat allenfalls eine Placebo-Funktion, die dazu diente, die Aufsichtsbehörde zu „blenden". Allerdings muss zugestanden werden, dass dieses Gutachten wohl noch zu Zeiten des alten BDSG (1990, zum Stand des Änderungsgesetzes v. 18.5.2001 – BGBl. I 2001, 904) erstellt worden sein dürfte, einer Zeit, in der die Datenschutzaufsicht noch beim Regierungspräsidium Darmstadt lag. Wenn dem so ist, stellt sich die Frage eines hinreichenden Problembewusstseins bei der Aufsichtsbehörde.

2. Scorewert-Erstellung und Verantwortlichkeit

In dem vorliegenden Urteil, das mit 70 Seiten auffällig umfangreich ist, wird an verschiedensten Stellen relativ ausführlich dargestellt, dass der Scorewert als solcher geeignet ist, eine Vorgriffswirkung auf die Begründung, Änderung oder Aufhebung einer rechtlichen Position der betroffenen Person, etwa im Hinblick auf die Kreditvergabe, zu entfalten, weil hierbei eine Einschätzung hinsichtlich der Kreditwürdigkeit getroffen wird. Dabei stellt sich die Kammer mit dem OLG Dresden (Urt. v. 7.10.2025 – 4 U 884/24) zu Recht gegen die landläufige Zivilrechtsprechung, die dem Scorewert eine rechtliche oder ähnliche Wirkung als „bloßes Internum" verwehrt (s. nur OLG München Hinweisbeschl. v. 23.10.2025 – 19 U 1468/25, das sich wohl gestützt auf das kontradiktorische Verfahren des Zivilrechts und die Beweislast herauswindet). Vorliegend wurde von der D-Bank AG die Einschätzung der Kreditwürdigkeit – also der Scorewert der SCHUFA – aber wohl maßgeblich zugrunde gelegt. Eine Praxis, die nach den Ermittlungen der Kammer bei zahlreichen Banken und Kreditinstituten bezogen auf sog. ‚externes Scoring' zutrifft und von der Rspr. der ordentlichen Gerichtsbarkeiten wohl verdrängt wird. Eine Bank muss eine Kreditentscheidung zwar nicht allein von einem Scorewert abhängig machen, tut es in der Regel jedoch maßgeblich, so die Feststellung der Kammer bei der D-Bank AG.

Damit liegt auch eine automatisierte Entscheidung im Einzelfall durch die SCHUFA vor. Sie ist die verantwortliche Stelle und damit auch auskunftspflichtig nach Art. 15 Abs. 1 lit. h DS-GVO iVm Art. 22 Abs. 1 DS-GVO. Hinzu kommt vorliegend, dass der Score von der SCHUFA speziell auf Basis des Portfolios der D-Bank AG erstellt worden ist.

3. Geschäftsgeheimnis

Das angesprochene Gutachten zu § 31 BDSG ist wohl nach altem Recht erstellt und kann damit kein Geschäftsgeheimnis mehr darstellen. Hierauf hat die Kammer aber zu Recht nicht abgestellt.

Nach der nunmehrigen Verpflichtung der Aufsichtsbehörde, unter Beachtung der Rechtsauffassung des Gerichts über den Auskunftsantrag der Kl. erneut zu entscheiden, ist es vielmehr Sache des Bekl. zu klären, ob und inwieweit zu einer Auskunft ggf. auch der Algorithmus zur Berechnung der Scorewerte vorliegend erforderlich ist. Denn er wurde wohl ausdrücklich von der SCHUFA nur für die D-Bank AG erstellt. Ob insoweit die Aussage der Kammer richtig ist, dass „eine Verpflichtung der Beigel., den in ihrem Scorewert zugrunde liegenden Algorithmus oder das statistische Verfahren, das der Scorewert-Bildung zugrunde liegt, mitzuteilen, hier nicht (bestehe)", richtig ist, muss offenbleiben. Denn darüber muss die Aufsichtsbehörde iRd Abwägung der einander gegenüberstehen Rechte und Interessen nun entscheiden, um den Umfang des in Art. 15 DS-GVO statuierten Auskunftsrechts der betroffenen Person nach den Vorgaben des Gerichts zu ermitteln.

Zumindest ist zu beachten, dass eine automatisierte Entscheidung (Score), und damit auch eine KI-Entscheidung nach der KI-VO, ggf. inhaltlich gerichtlich überprüfbar sein muss. Hierzu hatte der EuGH bereits in der sog. PNR-Entscheidung (ZD 2022, 553 mAnm Schild) ausgeführt, dass die Rechtmäßigkeit sämtlicher automatisierter Verarbeitungen schließlich von dem Datenschutzbeauftragten und von der nationalen Kontrollstelle (Art. 6 Abs. 7 und Art. 15 Abs. 3 lit. b PNR-RL) sowie von den nationalen Gerichten iRe gerichtlichen Rechtsbehelfs (Art. 13 Abs. 1 PNR-RL) überprüft werden können muss (EuGH ZD 2022, 553 Rn. 179 mAnm Schild). Dies bedeutet, dass ein Gericht, das mit der Rechtmäßigkeitsprüfung der Entscheidung betraut ist, sowie der Betroffene selbst sowohl von allen Gründen als auch von den Beweisen, auf deren Grundlage diese Entscheidung getroffen wurde, Kenntnis erlangen können müssen (vgl. entsprechend EuGH Urt. v. 4.6.2013 – C-300/11 Rn. 54 bis 59 – ZZ), einschließlich der im Voraus festgelegten Prüfkriterien und der Funktionsweise der Programme, mit denen diese Kriterien angewandt werden (EuGH ZD 2022, 553 Rn. 21 mAnm Schild).

Damit muss bei automatisierten Entscheidungsfindungen (einschließlich Profiling) iSv Art. 22 Abs. 1 DS-GVO die betroffene Person mindestens von dem Verantwortlichen iRd Anspruchs auf Erteilung „aussagekräftiger Informationen über die involvierte Logik" verlangen können, ihr anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form die Verfahren und Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer perso-

nenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – zB eines Bonitätsprofils – konkret angewandt wurden. Allgemeine Umschreibungen genügen nicht.

Insoweit dürfte gerade auch im Hinblick auf eine gerichtliche Überprüfbarkeit eine Berufung auf ein Geschäftsgeheimnis schwerfallen. Vielmehr sind die Verfahren zur automatisierten Entscheidungsfindung so zu gestalten, dass sie von Anfang an transparent in der Entscheidungsentstehung bzw. ihrer Entwicklung sind. Ein Problem, das bei der Anwendung richtiger KI-Werkzeuge nicht zu lösen sein dürfte, mit der Folge, dass der KI-Anbieter (Art. 3 Nr. 3 KI-VO) bzw. der Betreiber (Art. 3 Nr. 4 KI-VO) sich die mangelnde Transparenz wird zuschreiben lassen müssen, will heißen, die Ergebnisse können nicht verwendet werden. Andernfalls könnte ein Verstoß gegen die GRCh gegeben sein (zB Art. 7, 8, 47 GRCh).

4. Ausblick

a) Nationale Perspektive

Es liegt ein Gesetzentwurf der letzten Bundesregierung v. 7.2. 2024 für ein Erstes Gesetz zur Änderung des BDSG vor (abrufbar unter: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/VII4/aendg-bdsg.pdf?__blob=publicationFile&v=4). Dieser Entwurf enthält einen § 37a „Scoring" mit sechs Absätzen, der in dem vorliegenden Urteil angesprochen wird. Die hier geplante Norm soll eine Ermächtigungsgrundlage für das Scoring nach Art. 22 Abs. 2 lit. b DS-GVO schaffen, wenn zu einer natürlichen Person Wahrscheinlichkeitswerte erstellt oder verwendet werden über

- ein bestimmtes zukünftiges Verhalten der Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person oder
- ihre Zahlungsfähig- und -willigkeit durch Auskunfteien und unter Einbeziehung von Informationen über Forderungen.

Dabei stellt sich allerdings schon die Frage, ob die in § 37a Abs. 4 BDSG-E enthaltenen Offenbarungspflichten des Verantwortlichen (welcher ist hier gemeint?) ggü. der betroffenen Person, die schon nach der DS-GVO bestehen, iVm den Vorgaben des § 31 Abs. 2 BDSG geltender Fassung, tatsächlich angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person darstellen, wie dies Art. 22 Abs. 2 lit. b DS-GVO fordert. Also schlicht gesagt, die angedachte Regelung in der geplanten Art überhaupt DS-GVO-konform sein würde.

Insoweit ist es gut, wenn der Entwurf der Diskontinuität anheimgefallen ist. Auch ist fraglich, ob es noch einer nationalen Ermächtigungsnorm bedarf.

b) Europäische Perspektive

Denn nun hat die Kommission am 19.11.2025 einen Vorschlag für eine Verordnung des Parlaments und des Rates zur Änderung der VO (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 und der RL 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 in Bezug auf die Vereinfachung des Rechtsrahmens für den digitalen Bereich und zur Aufhebung der VO (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 und der RL (EU) 2019/1024 (Digital Omnibus) SWD (2025) 836 final – KOM(2025) 837 endg. 2025/0360 vorgelegt.

Dieser Vorschlag sieht eine gravierende Änderung der DS-GVO bei Art. 22 DS-GVO vor. Zwar soll Art. 22 DS-GVO im Kapitel III „Rechte der betroffenen Person", Abschnitt 4 „Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall" weiter angesiedelt sein. Die Norm soll aber zu einer Rechtsgrundlage für eine Datenverarbeitung für automatisierte Einzelentscheidungen umgestellt werden. Aus Absatz 1, dem Abwehranspruch, und Absatz 2, der Öffnungsmöglichkeit, soll ein Absatz werden:

„(1) Eine Entscheidung, die gegenüber einer betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, darf ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhen, wenn diese Entscheidung

(a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und einem Verantwortlichen erforderlich ist, unabhängig davon, ob die Entscheidung auch ohne ausschließliche Anwendung automatisierter Verfahren getroffen werden könnte;

(b) durch das Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, zugelassen ist und das auch geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorsieht; oder

(c) auf der ausdrücklichen Einwilligung der betroffenen Person beruht."

Diese hier vorgeschlagene Änderung der Kommission könnte eine neue Grundlage schaffen, die für das Scoring genutzt werden könnte. Denn durch die neue Formulierung der Ermächtigungsnorm unter lit. a könnte man auf den Gedanken kommen, dass nun auch ein Scoring für die Kreditvergabe zulässig sein könnte, denn statt einer individuellen Einzelfallprüfung wäre der Verantwortliche nicht gehindert die Entscheidung durch eine ausschließlich automatisierte Verarbeitung zu treffen (Erwägungsgrund 38 des Entwurfs). In diese Richtung tendiert die Vorlage des ÖOGH ZD 2026, 210 – in diesem Heft hinsichtlich des Bonitäts-Scorings bei Versandhändlern im Online-Handel.

Allerdings müsste der Begriff der Erforderlichkeit iSd Rspr. des EuGH sehr eng, also auf das unbedingt Erforderliche beschränkt werden. Legt man diese Messlatte wiederum an, hätte dies zur Folge, dass lit. a nicht weiter hilft und es doch einer nationalen Öffnungsnorm bedürfte. Man darf schon gespannt nach Luxemburg schauen (s. dazu auch EDPB-EDPS JOINT OPINION 2/2026, On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), Adopted on 10 February 2026, Nr. 7.3, Automated individual decision making, S. 22).

5. Fazit

Alles in allem weist die Entscheidung des VG Wiesbaden zum Umfang des Auskunftsrechts bei der Anwendung von Scores in die richtige Richtung eines europäischen Verständnisses. Sollte gegen die vorliegende Entscheidung ein Rechtsmittel eingelegt werden, wäre es ggf. die Sache des Rechtsmittelgerichts, erneut den EuGH anzurufen, falls es dem VG Wiesbaden nicht folgen will (Schild/Horlbeck, Der Datenschutzverstoß – im Erscheinen, § 4 Rn. 196 ff.). Ansonsten bleibt zu hoffen, dass sich die durch die vorliegende Entscheidung gewonnene Erkenntnis auch bei den übrigen nationalen Gerichtsbarkeiten (Zivil-, Arbeits-, Sozial- und insb. Finanzgerichtsbarkeit) weiterentwickelt. Sind doch die die nationalen Richter auch und gerade im Anwendungsbereich der DS-GVO Europarichter (Schild/Horlbeck, aaO, § 4 Rn. 218), was letztendlich bedeutet, dass sie dem EU-Recht Geltung verschaffen müssen.

6. Hinweis

Hinsichtlich der Vorlagen des VG Wiesbaden zur Restschuldenbefreiung die SCHUFA betreffend sei an dieser Stelle noch darauf hingewiesen, dass das Verfahren des EuGH ZD 2024, 166 mAnm Schild (Vorlagebeschluss des VG Wiesbaden ZD 2022, 706), eingestellt wurde und in dem Verfahren des EuGH in der Rs. C-64/22 und des VG Wiesbaden Az. 6 K 219/20.WI, eine Klageabweisung wegen fehlenden Feststellungsinteresse erfolgte (s.a. https://verwaltungsgerichtsbarkeit.hessen.de/presse/SCHUFA-muss-auskunft-ueber-scorewert-erteilen).

der Strafverfolgung iRe Sicherungsanordnung iSd § 100g Abs. 7 StPO-E. Strafprozessual werden die bisherigen Eingriffsschwellen für den Abruf von Standortdaten (gem. § 3 Nr. 56 TKG) und Funkzellendaten („aller in einer Funkzelle angefallenen Verkehrsdaten") angepasst und gelockert (§ 100g Abs. 3 und 4 StPO-E).

Am 9.2.2026 veröffentlichte das BMJV nun die eingegangenen Stellungnahmen verschiedener Verbände, Vereine und Unternehmen. Diese zeichnen ein gemischtes Bild. Grundsätzlich positiv äußerten sich zB der Deutsche Richterbund, der Bund Deutscher Kriminalbeamter (BDK), die Mobilfunknetzbetreiber, der Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) und Bitkom. Die Deutsche Polizeigewerkschaft (DPolG) fordert sogar eine Speicherdauer der IP-Adressdaten von mindestens sechs Monaten. Allerdings findet sich in den Stellungnahmen auch harsche Kritik, insb. mit Blick auf europa- und verfassungsrechtlichen Schranken. Die Bundesrechtsanwaltskammer (BRAK) äußert etwa „erhebliche Skepsis" und hält fest, sie hätte sich „stets gegen eine anlasslose und dauerhafte Speicherpflicht zu staatlichen Überwachungszwecken ausgesprochen." Die Speicherpflicht hinsichtlich der IP-Adressdaten greife „ohne hinreichende Rechtfertigung in die Grundrechte des Einzelnen auf ungestörte, unüberwachte Telekommunikation, auf Wohnung, freie Entfaltung der Persönlichkeit, auf das Recht auf informationelle Selbstbestimmung sowie in die Freiheit der Berufsausübung ein – wie auch in die Grundrechte der Versammlungsfreiheit, der Vereinigungsfreiheit und der Medienunternehmen und der Rundfunkanstalten." Von diesen Eingriffen seien namentlich u.a. Rechtsanwälte, Abgeordnete und Journalisten betroffen. Das Medienbündnis, bestehend aus ARD, ZDF, Deutschlandradio, dem DJV, dem dju, dem BDZV, dem MVFP, dem Presserat, VAUNET und Reporter ohne Grenzen, äußerte ebenfalls die Kritik, der Entwurf verkenne die „Grundrechtsrelevanz der Vorschläge" mit Blick auf Presse- und Rundfunkfreiheit. Befürchtet wird etwa ein erheblich verringertes Schutzniveau von Journalistinnen und Journalisten, sowie die teilweise Unvereinbarkeit mit dem EMFA und der Rspr. des EGMR.

Die (potenzielle) Verfassungswidrigkeit und insb. die mögliche Verletzung des Rechts auf informationelle Selbstbestimmung wird in diversen weiteren Stellungnahmen diskutiert, etwa von der Neue Richter*innenvereinigung (NRV), der Gesellschaft für Informatik, dem gemeinnützigen Verein Digitale Gesellschaft und dem Arbeitskreis Vorratsdatenspeicherung. Der Deutsche Anwaltverein (DAV) kommt hinsichtlich der IP-Adressspeicherung zu dem Ergebnis, dass diese klar europarechtswidrig sei und zudem ggf. verfassungswidrig. Mehrere Stellungnahmen stellen überdies Defizite hinsichtlich der Bestimmtheit des Entwurfs fest. Der BREKO hegt darüber hinaus Zweifel an der Angemessenheit der Belastungen für Unternehmen in der Umsetzung der IP-Adressspeicherung, besonders für kleine und mittlere Netzbetreiber. Diesen Aspekt hebt iÜ auch der DAV hervor. Kritik wird außerdem an dem Vorgehen des BMJV geäußert. So geht zB aus den Stellungnahmen des Medienbündnisses und der Gewerkschaft der Polizei (GdP) die Kritik hervor, gar nicht oder erst kurz vor Fristende über den Entwurf und die Möglichkeit zur Stellungnahme unterrichtet worden so sein.

Wie und wann das Gesetzgebungsverfahren weitergehen wird, bleibt abzuwarten. Mit Blick auf die doch sehr umfangreichen Kritikpunkte und die erheblichen Zweifel an der Vereinbarkeit der Regelungen mit dem Verfassungsrecht wie dem Unionsrecht, zeichnet sich ab, dass das letzte Wort sicherlich noch nicht gesprochen ist. Relevant wird hier außerdem die umfangreiche Rspr. in dem Bereich sein – zB auf Bundesebene hinsichtlich der Funkzellenabfrage (BGH MMR 2024, 676) oder auf Unionsebene iRd Vorratsdatenspeicherung (EuGH ZD 2024, 569).

■ Vgl. hierzu auch BGH MMR 2024, 676; EuGH ZD 2024, 569; BGH ZD 2024, 341; Roßnagel ZD 2022, 650; LG Hamburg MMR 2025, 154; MMR-Aktuell 2025, 01554; hierzu MMR-Aktuell 2025, 01303; MMR-Aktuell 2025, 01340; MMR-Aktuell 2025, 01234; MMR-Aktuell 2025, 01303; Seyda/Zurawski ZD-Aktuell 2024, 01929; Etteldorf MMR-Aktuell 2024, 01438; MMR-Aktuell 2023, 01151; ZD-Aktuell 2023, 01341; EuGH ZD 2022, 666; Roßnagel ZD 2022, 650 und MMR-Aktuell 2022, 452018.

Hannah Waegner
ist Wissenschaftliche Mitarbeiterin an der rechtswissenschaftlichen Fakultät der Universität Münster und Lehrbeauftragte an der FOM Hochschule für Oekonomie und Management.

OLG Dresden: Schadensersatz wegen Meta Business Tools

ZD-Aktuell 2026, 01148

Das OLG Dresden hat mit Urt. v. 3.2.2026 – 4 U 196/25, 4 U 292/25, 4 U 293/25, 4 U 296/25 (ZD wird die Entscheidungen demnächst veröffentlichen) in vier Parallelverfahren zu den sog. Meta Business Tools den Meta Konzern zur Zahlung von immateriellem Schadensersatz nach Art. 82 Abs. 1 DS-GVO iHv jeweils 1.500 EUR sowie zur Unterlassung der Weiterverarbeitung hiermit gewonnener personenbezogener Daten verurteilt.

Meta, die Konzernmutter von Facebook und Instagram, bietet Unternehmen Programmschnittstellen, sog. Business-Tools, zur Installation auf deren Webseiten an. Über diese können personenbezogene Daten der Webseitennutzer gesammelt und mit dem Meta-Konzern geteilt werden.

In vier ersten Verfahren hat das OLG Dresden Meta nun dazu verurteilt, betroffenen Instagram-Nutzern jeweils 1.500 EUR immateriellem Schadensersatz zu zahlen. Außerdem muss Meta es unterlassen, mit den Business-Tools gewonnene personenbezogene Daten weiterzuverarbeiten.

Die für die Datenverarbeitung erforderlichen Einwilligungserklärungen der Nutzer hätten nicht vorgelegen. Meta habe sich hierfür auch nicht auf einen weiteren der nach der DS-GVO möglichen Rechtfertigungsgründe berufen können.

Durch eine solche Verarbeitung personenbezogener Daten entstehe ein Kontrollverlust, der bei betroffenen Nutzern ein Gefühl der umfassenden Überwachung hervorrufen könne. Dies rechtfertige es, einen immateriellen Schadensersatz auf der Grundlage von Art. 82 DS-GVO auch dann zuzusprechen, wenn der einzelne Nutzer hierdurch keine psychische Beeinträchtigung erlitten habe. Nicht erforderlich sei es hierfür, dass der Nutzer nachweist, Webseiten besucht zu haben, die seine personenbezogenen Daten mit Hilfe dieser Business Tools an den Meta-Konzern weiterleiten.

Die Revision wurde nicht zugelassen. Die Urteile sind damit rechtskräftig.

■ Vgl. hierzu auch Schmitz ZD-Aktuell 2026, 01117; LG Leipzig ZD 2025, 580 mAnm Däuble; LG Lübeck ZD 2025, 228 mAnm Niekrenz; VG Köln ZD 2025, 593 mAnm Meyer und Frey/Westphal MMR 2025, 779.

ZD FOKUS

Hannah Waegner Datenleak von mSpy: Spionagesoftware zur Kontrolle von Kindern als illegales Tool zum Cyberstalking

ZD-Aktuell 2026, 01140

Um Eltern die Möglichkeit zu geben, die Endgeräte ihrer Kinder zu kontrollieren, bieten Software-Unternehmen entsprechende Spyware an, die die vollständige Überwachung von Smartphones ermöglicht. Ein Datenleak bei einem dieser Anbieter zeigte jetzt auf, dass diese Tools oftmals genutzt werden, um etwa den eigenen Partner zu überwachen. Zwar können die Täter strafrechtlich belangt werden, die Rechtsdurchsetzung gegenüber den dahinterstehenden Unternehmen gestaltet sich jedoch schwierig.

Ende Januar 2026 berichteten SWR und netzpolitik.org, dass ihnen interne Nachrichten des Spionagesoftware-Anbieters mSpy vorlägen. Der geleakte Datensatz mit Millionen Kundenanfragen zeigt auf, dass das Spionage-Tool vielfach auch dazu genutzt wird, andere Erwachsene zu überwachen. Das Unternehmen mSpy bewirbt die eigene Anwendung als „Kinderschutz-App". Im Abo-Modell können Kundinnen und Kunden ein Konto anlegen, das Tool auf dem Endgerät der zu überwachenden Person – im Anwendungsbeispiel des Anbieters des eigenen Kindes – installieren und anschließend Textnachrichten mitlesen, Anrufprotokolle einsehen, Standortdaten abrufen, den Browserverlauf checken sowie mit der Fernsteuerung von Kamera und Mikrofon weitere Kontrollmöglichkeiten ausüben. Das alles soll nach Aussage des Anbieters möglich sein, ohne dass der Nutzer des Endgeräts von diesen Überwachungsmaßnahmen erfährt. Der Anbieter wirbt auf der eigenen Website mit einer „erstklassigen Telefonüberwachung" und bezeichnet die eigene Anwendung als die „leistungsstärkste Überwachungs-App der Welt".

Zielgruppe dieser Spyware sind besorgte Eltern, die ihre Kinder kontrollieren wollen. Eine solche Überwachung ist grds. legal. Anders verhält es sich jedoch, wenn so die Geräte Volljähriger überwacht werden. Relevante Straftatbestände sind hier § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen on Daten) sowie § 238 StGB (Nachstellung). Für diejenigen Personen, die entsprechende Programme in den Verkehr bringen, gilt ferner der § 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten). Der Leak der Kundenanfragen bei mSpy zeigt nun auf, dass das Spionage-Tool oftmals genutzt wird, um etwa den eigenen Partner zu überwachen. Unter den Anfragen sind mutmaßlich mehrere tausend von deutschen Nutzerinnen und Nutzern. Der Datensatz zeigt den Recherchen zufolge auch auf, dass der Kundendienst von mSpy wusste, dass die Software für illegale Zwecke, also zur unbemerkten Überwachung etwa des Partners, genutzt wird, und dennoch Hilfestellung bei der Installation und Verschleierung der Verwendung des Programms leistete. Opfer von einer solchen illegalen Überwachung können strafrechtlich gegen die Täter vorgehen. Hinsichtlich der Anbieter solcher Spyware besteht diese Möglichkeit iRd § 202c StGB grds. auch, jedoch stellt sich hier oft die Frage nach der Durchsetzbarkeit. Im Falle mSpy verlieren sich die Spuren des Unternehmens: Den Recherchen zufolge seien die Verantwortlichen zwischen einer Briefkastenfirma in Tschechien, einigen Strohmännern in der Ukraine und einer Holding in den Vereinigten Arabischen Emiraten so gut wie unauffindbar. Jegliche Ansprüche aus der DS-GVO gegen das Unternehmen seien damit auch wertlos.

Geräte zur heimlichen Überwachung sind innerhalb der EU iÜ verboten, entsprechende Software jedoch nicht. Im Koalitionsvertrag von CDU, CSU und SPD findet sich die Forderung, dass Tracking-Apps als solche klar erkennbar sein müssen – ein entsprechender Gesetzesentwurf lässt jedoch auf sich warten. Der Vertrag führt diese Forderung explizit im Kontext von Gewalt gegen Frauen auf. Cyberstalking und die rechtswidrige Überwachung von Endgeräten ist ein klassisches Beispiel von digitaler Gewalt innerhalb einer Partnerschaft. Spyware ist aber auch darüber hinaus ein bekanntes Problem, etwa auch vor dem Hintergrund der Überwachung von Medienschaffenden, Aktivistinnen und Aktivisten oder Politikerinnen und Politikern. Die Gesellschaft für Freiheitsrechte (GFF) hat daher bereits vor geraumer Zeit die sog. SpywareShield-Initiative gegründet, die ein Verbot kommerzieller Spionagesoftware fordert.

■ Vgl. hierzu auch ZD-Aktuell 2022, 01063; ZD-Aktuell 2023, 01345 und Müller ZD-Aktuell 2021, 05457.

Hannah Waegner
ist Wissenschaftliche Mitarbeiterin an der rechtswissenschaftlichen Fakultät der Universität Münster und Lehrbeauftragte an der FOM Hochschule für Oekonomie und Management.

LG Berlin II: Facebooks Freunde-Finder-Funktion verstößt gegen Datenschutzrecht

ZD-Aktuell 2026, 01164

Das LG Berlin II hat mit Urt. v. 2.12.2025 – 15 O 569/18 (ZD wird die Entscheidung demnächst veröffentlichen) entschieden, dass Facebook nicht über seine Freunde-Finder-Funktion auf Kontaktdaten von Personen zugreifen darf, die selbst nicht Nutzer der Plattform sind.

Mit der Freunde-Finder-Funktion können registrierte Facebook-Nutzer die auf ihren Endgeräten gespeicherten Kontaktdaten auf einen Server hochladen. (Gegenstand der Klage des Verbraucherzentrale Bundesverbands (vzbv) war die Funktionsweise der Freunde-Finder-Funktion, wie sie sich zum Zeitpunkt der Klage 2018 darstellte). Die erfassten Kontakte der Facebook-Nutzer hätten der Datenverarbeitung durch Meta Irland weder zugestimmt noch einen Vorteil aus der Datenverarbeitung gehabt; ein durchschnittlicher Verbraucher könne nicht erwarten, dass seine Daten trotz Nichtnutzung eines sozialen Netzwerks erfasst werden. Meta Irland muss diese Praxis künftig unterlassen, andernfalls droht ein Ordnungsgeld.

Für Facebook-Nutzer ändert sich zunächst nichts, da das Gericht Meta nicht verpflichtet hat, bereits hochgeladene Daten zu löschen. Rechtswidrig ist laut Gericht außerdem das Erstellen von Werbe-Nutzungsprofilen zu registrierten Nutzern ohne vorherige eindeutige Einwilligung. Die vzbv begrüßt das Urteil als wichtiges Signal gegen „Datensauger" sozialer Netzwerke. In einem Punkt gab das Gericht der Klage nicht statt: Ein Verbot der Profilbildung zu Werbezwecken von nicht registrierten Facebook-Seitenbesuchern wurde mangels Beweises abgelehnt. Das Urteil ist noch nicht rechtskräftig.

■ Vgl. hierzu auch LG Berlin ZD 2012, 276 mAnm Solmecke/Baursch und KG ZD 2014, 412.

Timo Sebastian Hoffmann

OLG Dresden: Rechtliche Hürden für Hobby-Ordnungshüter

ZD-Aktuell 2026, 01141

Parkverstöße gehören zum Stadtbild vieler deutscher Städte. Einige Verkehrsteilnehmer machen in diesem Kontext ein Vollzugsdefizit bei den Ordnungsbehörden aus. Nicht jede Stadt bietet die Möglichkeit, Parkverstöße niederschwellig und effektiv (zB über Apps des örtlichen Ordnungsamts) zu melden. Die Internetseite www.weg.li erlaubt es Privatpersonen, automatisiert Anzeigen an die zuständigen Ordnungsbehörden zu generieren, in der Hoffnung darauf, dass die Meldung zu einer Ahndung der Verkehrsverstöße bzw. zu einer Umsetzung der Fahrzeuge führt. Über diese Internetseite hatte der Bekl. am 28.1.2024 ein Parkvergehen gemeldet, indem er das Foto eines verkehrswidrig in einer Busspur abgestellten Fahrzeugs hochlud, das auch den Beifahrer des Fahrzeugs zeigte, ohne dass dieser unkenntlich gemacht worden war. Gegen die damit einhergehende Datenverarbeitung wendete sich der Beifahrer als Berufungskläger erfolgreich vor dem OLG Dresden (Urt. v. 9.9.2025 – 4 U 464/25; ZD wird die Entscheidung demnächst veröffentlichen).

Der Kl. hatte den Bekl. zunächst außergerichtlich abgemahnt und zur Abgabe einer Unterlassungserklärung aufgefordert. Dies hatte der Bekl. verweigert. In der Vorinstanz hatte das LG Leipzig (U. v. 14.3.2025 – 08 O 2194/24) den Anspruch des Kl. auf Unterlassung der Verbreitung des Bildes und Schadensersatz abgelehnt. Dagegen wendete sich der Kl. in der Berufung vor dem OLG.

1. Entscheidung

Das OLG gab der Berufung in weiten Teilen statt und verurteilte den Bekl. zur Löschung des gegenständlichen Bilds und zur Zahlung von Schadensersatz.

a) Anspruch auf Löschung des Lichtbilds

Den Anspruch auf Löschung gründet das OLG auf Art. 17 Abs. 1 DS-GVO iVm Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Dazu grenzt das Gericht zunächst umfassend und nachvollziehbar die Anwendbarkeit der DS-GVO gegenüber den §§ 22, 23 KUG und dem allgemeinen Persönlichkeitsrecht ab und stellt den Anwendungsvorrang der datenschutzrechtlichen Regelungen heraus, zumal Deutschland nicht von der Öffnungsklausel des Art. 85 Abs. 2 DS-GVO Gebrauch gemacht habe (Rn. 6). Das Hochladen des vom Bekl. gefertigten Fotos stelle eine Verarbeitung gem. Art. 2 Abs. 1 DS-GVO von personenbezogenen Daten gem. Art. 4 Nr. 1 DS-GVO dar. Die Veröffentlichung personenbezogener Daten durch das Hochladen auf eine Webseite qualifiziert das Gericht als automatisierte Verarbeitung der Daten unter Bezugnahme auf die einschlägige Rspr. des EuGH (Rn. 7 mwN), zumal weg.li den Datensatz an die örtliche Bußgeldstelle weiterleitete.

Der Bekl. sei ferner Verantwortlicher iSd Art 4 Nr. 7 DS-GVO, da er durch das Anfertigen des Fotos und Hochladen auf die Server der Website über die Zwecke und Mittel der Verarbeitung entschieden habe. Die Betreiber der Website selbst haben die Daten gem. Art. 4 Nr. 8 DS-GVO nur in seinem Auftrag verarbeitet (Rn. 9).

Die Ausnahme nach Art. 2 Abs. 2 lit. d DS-GVO für Strafverfolgungs- bzw. Gefahrenabwehrtätigkeiten sei nicht einschlägig, da der Bekl. als Privatperson gehandelt habe (Rn. 10). Ebenso wenig könne dieser sich auf die Haushaltsausnahme aus Art. 2 Abs. 2 lit. c DS-GVO für ausschließlich persönlich-familiäre Tätigkeiten berufen (Rn. 11).

Eine die Verarbeitung rechtfertigende Einwilligung des Kl. gem. Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO liege nicht vor (Rn. 13). Eine Rechtfertigung aus Art. 17 Abs. 3 lit. b DS-GVO iVm Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO liege auch nicht vor. Ob die Datenverarbeitung zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, geschah, könne dahinstehen, da diese auf die Wahrnehmung von öffentlichen Aufgaben beschränkt sei, die dem Verantwortlichen durch einen Rechtsakt übertragen seien (Rn. 14), wie zB bei der Verarbeitung durch Behörden.

Auch könne sich der Bekl. nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO berufen, die Datenverarbeitung sei zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich gewesen. Die Interessenabwägung komme zu dem Ergebnis, dass die Interessen des Kl. gegenüber denen des Bekl. überwiegen (Rn. 15). Ein Interesse an der Anzeige von Straftaten auch außerhalb persönlicher Betroffenheit durch den in Rede stehenden Verkehrsverstoß werde zwar auch für Ordnungswidrigkeiten vertreten; ob die Verkehrssituationen gesetzeswidrige Tatbestände mit hinreichender Schwere betreffen, wird jedoch nicht durch das Gericht bewertet (Rn. 16). Denn im Ergebnis überwiege eindeutig das Recht des Kl. am eigenen Bild, das sich aus dem Recht auf informationelle Selbstbestimmung und dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG konkretisiere. Der Kl. sei ohne sein Wissen im geparkten Fahrzeug, auf dem Beifahrersitz, bei einer privaten Betätigung und nicht im öffentlichen Raum fotografiert worden, womit seine schutzbedürftige Sozialphäre als schwerwiegende Verletzung seines Allgemeinen Persönlichkeitsrechts betroffen sei (Rn. 17). Datenerhebungen zur Ermittlung weiterer Zeugen unterlägen allein dem Interesse der Bußgeldbehörde. Diese benötigten gem. Art. 6 Abs. 3 S. 1 DS-GVO zudem konkrete Rechtsgrundlagen (Rn. 19).

Der Bekl. habe es weiterhin unterlassen, Maßnahmen zu ergreifen, die dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DS-GVO entsprochen hätten. So hätte der Bekl. den Kläger zB unkenntlich machen können (Rn. 18).

Während die Vorinstanz dem Kl. das Rechtsschutzbedürfnis mit dem Argument absprach, man könne nicht gleichzeitig wichtiger Zeuge (wie im Bußgeldverfahren zur Entlastung der Fahrerin) und unbeteiligter Dritter sein, überzeugte der umfangreiche Vortrag des Bekl. zum gesteigerten Beweiswert des Fotos für das Bußgeldverfahren durch den identifizierbaren Kl. das OLG nicht. Der in solchen Fällen erforderliche besonders enge Sachbezug zu einem – zu diesem Zeitpunkt noch nicht einmal anhängigen – Bußgeldverfahren könne jedenfalls nicht dadurch hergestellt worden sein, dass sich der Kl. zufällig im Auto befunden habe (Rn. 22).

Da der Bekl. im Termin nicht überzeugend glaubhaft machen konnte, das Foto gelöscht zu haben, bestehe der Löschungsanspruch des Kl. weiterhin (Rn. 23).

b) Anspruch auf Schadensersatz

Den Anspruch des Kl. auf Schadensersatz stützt das Gericht auf die Verarbeitung der klägerischen Daten ohne ausreichenden Rechtfertigungsgrund gem. Art. 6 DS-GVO. Der dem Kl. aus dem Verstoß gegen die DS-GVO kausal entstandene Kontrollverlust sei ein immaterieller Schaden iSv Art. 82 DS-GVO. Zur Schadens-

höhe gewichtet das Gericht die Dauer von rd. 1,5 Jahren, in denen der Kontrollverlust andauerte, da die biometrischen Daten in Kombination mit Daten zu Zeit und Ort im Internet abrufbar waren und einem uneingeschränkten Personenkreis innerhalb der Bußgeldstelle zugänglich waren (Rn. 29). Diese Kontrolle habe er erst mit der Löschung des Bilds vom Mobiltelefon des Bekl. und der Löschung der spezifischen URL auf weg.li wiedererlangt. Im Ergebnis spricht das Gericht dem Kl. einen Betrag von 100 EUR zu (Rn. 30).
Der Bekl. habe dem Kl. daher auch die vorgerichtlichen Anwaltskosten zu ersetzen. Das Gericht bezifferte den Streitwert des Löschungsanspruchs mit 5.000 EUR und den Schadensersatzanspruch mit 100 EUR. Ein zusätzlich geltend gemachter Unterlassungsanspruch verfolge dasselbe Ziel wie der Löschungsanspruch, weshalb dieser sich nicht streitwerterhöhend auswirke (Rn. 31).

2. Bewertung

Dass die DS-GVO in der Vorinstanz nicht geprüft und stattdessen dem KUG Vorrang eingeräumt wurde, überrascht.
Das OLG korrigiert dies mit ausführlicher und nachvollziehbarer Begründung. Das Gericht sieht davon ab, das Dokumentieren von Verkehrsverstößen durch Privatpersonen grds. (negativ) zu bewerten, und liefert stattdessen konkrete Hinweise, wie dieses unter Berücksichtigung des Grundsatzes der Datenminimierung datenschutzrechtskonform erfolgen könne. In Betracht komme neben einer Perspektive des Fotos, welche die Ablichtung unbeteiligter Menschen vermeide, zB das Verpixeln der biometrischen Daten. Ein Abweichen nach oben vom (Mindest-)Betrag von 100 EUR an Schadensersatz, der sich für den bloß kurzzeitigen Kontrollverlust über die eigenen Daten etabliert zu haben scheint, wäre mit entsprechender Argumentation denkbar gewesen. Da es sich bei dem Bekl. aber um eine Privatperson handelte, die keinen finanziellen Nutzen aus der Datenverarbeitung gezogen hat, ist die moderate Bemessung des Schadensersatzes gem. Art. 82 DS-GVO im Ergebnis nachvollziehbar.
Das Versäumnis des Bekl. in Hinblick auf den nicht unkenntlich gemachten Beifahrer wird für diesen teuer. Mit den zu erstattenden vorgerichtlichen Anwaltskosten dürften auf den Bekl. aufgrund des nahezu vollständigen Unterliegens instanzübergreifend Prozesskosten von rd. 6.000 EUR zukommen.

■ Vgl. auch Schindler ZD-Aktuell 2023, 01054; ZD-Aktuell 2023, 01013; Delventhal ZD-Aktuell 2022, 01448 mwN; ZD-Aktuell 2022, 01395; Hofmann MMR 2022, 862; Lehr/Becker ZD 2022, 370 und Wanser ZD-Aktuell 2021, 05574.

Ass. iur. Timo Sebastian Hoffmann, LL.M. Eur., Mag. rer. publ.,
ist Wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik (IRI) an der Leibniz Universität Hannover.

Christina Meese ÖVwGH: Jahresfrist für Datenschutzbeschwerden widerspricht nicht der DS-GVO

ZD-Aktuell 2026, 01154

Mit nun veröffentlichter Entscheidung v. 17.12.2025 hat der österreichische Verwaltungsgerichtshof (ÖVwGH) entschieden, dass die im österreichischen Datenschutzgesetz verankerte Frist von einem Jahr, innerhalb deren eine Beschwerde bei der Datenschutzbehörde (DSB) wegen Datenschutzverletzungen erhoben werden muss, mit der DS-GVO vereinbar ist. Eine solche Regelung beschneide nicht die in der DS-GVO garantierte effektive Rechtewahrnehmung, sondern sei Betroffenen ohne Weiteres zumutbar.
Im zugrunde liegenden Fall ging es darum, dass ein Bankkunde im April 2019 bemerkt hatte, dass ein Mitarbeiter der Bank seine der Bank gegenüber angegebene E-Mail-Adresse für die Kontaktaufnahme in einer privaten Angelegenheit genutzt hatte. U.a. wegen eines vorgebrachten Verstoßes gegen den Zweckbindungsgrundsatz erhob der Bankkunde im Juni 2021 Beschwerde bei der DSB. Da in Österreich gem. § 24 Abs. 4 öDSG jedoch eine Präklusionsfrist für Beschwerden von einem Jahr gilt und der Bf. keinen andauernden Verstoß geltend gemacht hatte, wies die DSB die Beschwerde unter Berufung auf die Verfristung zurück. Die hiergegen erhobene Beschwerde hatte vor dem ÖBVwG keinen Erfolg. Das ÖBVwG stellte fest, dass sich das Beschwerderecht zwar unmittelbar aus Art. 77 DS-GVO ergebe, dort aber keine Fristen geregelt seien. Diese ergäben sich, im Einklang mit der Regulierung von Befugnissen der Aufsichtsbehörden nach Art. 58 Abs. 4 DS-GVO, aus nationalem Verfahrensrecht.
Es sei nicht ersichtlich, dass die Frist des § 24 öDSG das Beschwerderecht nach der DS-GVO unverhältnismäßig beschränke oder zu einer Ungleichbehandlung von dem Unionsrecht unterliegenden Beschwerden im Vergleich zu solchen unter nationalem Recht führe. Dennoch ließ das ÖBVwG die Revision zum ÖVwGH zu, um die Vereinbarkeit der Fristbindung mit EU-Recht für die Fälle entscheiden (bzw. eine mögliche Vorlage an den EuGH erwägen) zu lassen, in denen sich der Bf. explizit auf Art. 77 DS-GVO beruft – eine Konstellation, die in der österreichischen Fachliteratur durchaus umstritten ist.
Der ÖVwGH konnte nunmehr einen Widerspruch zur DS-GVO nicht erkennen und sah auch von einer Vorlage an den EuGH mangels Notwendigkeit ab. Insbesondere verwarf er das vom Bf. vorgebrachte Argument, dass Art. 77 DS-GVO gerade keine nationale „Durchführung" des Beschwerderechts vorsehe und daher für nationale Konkretisierungen gesperrt sei. Unter Darstellung der hierzu in der Literatur vertretenen unterschiedlichen Auffassungen kommt der ÖVwGH zu dem Ergebnis, dass die DS-GVO eine nationale Verfahrensautonomie zulasse und sogar in bestimmten Teilen mangels eigener Regelungen erforderlich mache. Zur Begründung beruft der ÖVwGH sich maßgeblich auf eine Entscheidung des EuGH (EuGH ZD 2023, 209 mAnm Schwamberger – BE / Nemzeti Adatvédelmi és Információszabadság Hatóság), in der dieser ausgeführt hatte, dass es mangels einer einschlägigen Unionsregelung nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten Sache der einzelnen Mitgliedstaaten ist, die Modalitäten für das Verwaltungsverfahren (und das Gerichtsverfahren) zu regeln, die ein hohes Schutzniveau der dem Einzelnen aus dem Unionsrecht erwachsenden Rechte gewährleisten sollen.
Dies gilt laut EuGH jedenfalls dann, wenn die nationale Regelung den Grundsätzen der Äquivalenz und Effektivität entspricht. Eben dies hält der ÖVwGH durch § 24 öDSG für erfüllt. Die hierin normierten Fristen differenzierten nämlich zum einen nicht, ob in einer Datenschutzbeschwerde ein Verstoß gegen die DS-GVO und/oder das österreichische Datenschutzgesetz geltend gemacht wird. Zum anderen, im Hinblick auf die Äquivalenz, erfolge keine unangemessene Schlech-

terstellung der Betroffenen im Vergleich zur Unionsregelung. Der Gesetzgeber habe mit der Einführung der Fristen die im Interesse der Rechtssicherheit liegende Zielsetzung verfolgt, dass die Ermittlung von Sachverhalten, die lange zurückliegen, erfahrungsgemäß auf erhebliche Schwierigkeiten stoße und eine verlässliche Beurteilung des Vorliegens von Datenschutzverletzungen verhindere. Umgekehrt und auch um die Einhaltung der Präklusionsfrist zu erleichtern, sieht das österreichische Recht zahlreiche Erleichterungen für Betroffene bei der Einreichung von Beschwerden vor. Diese können zB einfach über ein Online-Formular eingereicht werden und müssen keine vertieften Begründungen enthalten, sodass jedem Betroffenen die Erhebung einer Beschwerde innerhalb eines Jahres ohne Weiteres möglich und zumutbar sei. Zudem gebe es auch die Möglichkeiten, dass die DSB präkludierte Beschwerden behandelt oder auf Antrag eine Wiedereinsetzung in den vorigen Stand vornimmt. Für nicht relevant im vorliegenden Fall hielt der ÖVwGH auch, dass der EuGH in seinem Urteil v. 16.1.2024 (EuGH ZD 2024, 269 mAnm Schild – Österreichische Datenschutzbehörde) speziell zu den österreichischen Konkretisierungen der Art. 77 bis 79 DS-GVO entschieden hatte, dass für Art. 77 Abs. 1 DS-GVO keine nationalen Durchführungsmaßnahmen erforderlich sind und diese Bestimmung hinreichend klar, genau und unbedingt ist, um unmittelbar anwendbar zu sein. Das, so der ÖVwGH, habe sich nämlich nur auf Zuständigkeitsfragen der DSB und nicht auf Verfahrensregelungen wie die vorliegenden bezogen.

■ Vgl. auch Kulaga ZD 2026, 27; EuGH ZD 2024, 269 mAnm Schild und EuGH ZD 2023, 209 mAnm Schwamberger.

Ass. iur. Christina Meese
ist Wissenschaftliche Referentin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

BGH: Privatautonome Selbstbestimmung statt BGB-Vertrag als Maßstab für Art. 6 Abs. 1 lit. b DS-GVO

ZD-Aktuell 2026, 01147

Mit Urt. v. 10.12.2025 – II ZR 132/24 (ZD wird die Entscheidung demnächst veröffentlichen) hat der BGH nicht nur über einen vereinsrechtlichen Auskunftsanspruch entschieden, sondern bemerkenswerte Aussagen zum unionsautonomen Vertragsbegriff gemacht. Demnach ist nicht das zivilrechtliche Vertragsverständnis des BGB maßgeblich für die Rechtsgrundlage nach Art. 6 Abs. 1 lit. b DS-GVO, sondern ein privatautonom begründetes Rechtsverhältnis.

In dem zugrundeliegenden Sachverhalt verlangte ein Mitglied eines Sportvereins zur Wahrung seiner mitgliedschaftlichen Rechte die Herausgabe der E--Mail-Adressen anderer Mitglieder, um vor einer Mitgliederversammlung auf deren Meinungsbildung und Abstimmungsverhalten Einfluss zu nehmen. Der beklagte Verein verweigerte die Auskunft mit dem Hinweis auf datenschutzrechtliche Vorgaben.

Der BGH stellt zunächst klar, dass die Übermittlung der E--Mail-Adressen zur Durchsetzung der Mitgliedschaftsrechte erforderlich seien und eine bloße Weiterleitung von Informationen durch den Vorstand nicht ausreiche, um die Kommunikation zwischen Mitgliedern zu ermöglichen. Darüber hinaus setzt der BGH sich bemerkenswert mit dem Umfang des Vertragsbegriffs in Art. 6 Abs. 1 lit. b DS-GVO auseinander und stellt fest, dass dieser nicht an dem zivilrechtlichen Vertragsverständnis des BGB zu messen ist. Nach Ansicht des BGH „kommt nicht darauf an, ob das Rechtsverhältnis, zu dessen Erfüllung die Verarbeitung erforderlich ist, ein Vertrag iSd Bürgerlichen Gesetzbuchs ist, sondern ob das datenschutzrechtliche Telos des Erlaubnistatbestands erfüllt ist."

Der Vereinsbeitritt wird als ein solches privatautonom begründetes Verhältnis eingeordnet. Die Satzung konkretisiert die Rechte und Pflichten der Beteiligten und bildet den inhaltlichen Rahmen dieses „Vertrags" im datenschutzrechtlichen Sinne. Der BGH verlagert damit die Anwendbarkeit des Art. 6 Abs. 1 lit b DS-GVO von formalen zivilrechtlichen Vertragskriterien hin zur materiellen Selbstbestimmung der betroffenen Person. Ausschlaggebend ist die freiwillige, autonome Entscheidungsmöglichkeit der beteiligten Personen und dass die konkrete Datenverarbeitung der Erfüllung dieses Verhältnisses dient. Diese Auslegung weg vom formalen Vertragsbegriff des nationalen Zivilrechts hin zu einem unionsrechtlich geprägten Rechtsverständnis ist auch hilfreich für Konstellationen, in denen Leistungen nicht klassisch gegen Geld, sondern gegen personenbezogene Daten erbracht werden. Wenn bereits ein selbstbestimmt eingegangenes, privatautonomes Nutzungs- oder Teilnahmeverhältnis ausreicht, um Art. 6 Abs. 1 lit. b DS-GVO zu eröffnen, könnte dies die datenschutzrechtliche Rechtfertigung vieler datenbasierter Geschäftsmodelle stärken – auch dort, wo kein zivilrechtlicher Vertrag im engeren Sinne vorliegt.

■ Vgl. hierzu auch Starke ZD 2024, 63; Buchner/Kuhn ZD 2024, 548 und Spindler MMR 2021, 451.

CNIL: Bericht zu Sanktionen im Jahr 2025 veröffentlicht

ZD-Aktuell 2026, 01160

Am 9.2.2026 hat die CNIL ihren Jahresrückblick zu Sanktionen und aufsichtsrechtlichen Maßnahmen für das Jahr 2025 veröffentlicht. Darin berichtet die Behörde, dass sie insgesamt 83 Sanktionen mit einem Gesamtbußgeld von 486,8 Mio. EUR verhängt hat. Schwerpunkte der Maßnahmen lagen in den Bereichen Cookies und andere Tracking-Technologien, Videoüberwachung von Beschäftigten, Datensicherheit sowie Verstöße gegen Pflichten von Auftragsverarbeitern. Insgesamt traf die CNIL 259 Entscheidungen, darunter 143 Anordnungen zur Herstellung der Datenschutz-Compliance und 31 Hinweise auf gesetzliche Anforderungen.

Ein besonders großer Teil der Sanktionen betraf Verstöße gegen die Regeln zu Cookies und Trackern. 21 Unternehmen wurden sanktioniert, weil sie etwa Tracking-Technologien ohne Einwilligung einsetzten, Nutzer unzureichend informierten oder Widerrufe nicht berücksichtigten. Zwei große Marktakteure erhielten dabei Bußgelder iHv 325 Mio. EUR bzw. 150 Mio. EUR (s. dazu ZD-Aktuell 2025, 01394). Die CNIL verwies darauf, dass die Rechtslage seit Jahren klar kommuniziert sei und Verstöße deshalb als besonders schwer wiegen.

Ein weiterer Schwerpunkt waren unzulässige Praktiken bei der Videoüberwachung von Beschäftigten. 16 Organisationen wurden sanktioniert, weil sie Mitarbeiter dauerhaft oder verdeckt filmten,

ohne dass außergewöhnliche Umstände oder besondere Sicherheitsanforderungen vorlagen. Solche Maßnahmen verstoßen nach Auffassung der CNIL grds. gegen den Schutz der Privatsphäre am Arbeitsplatz.

Zudem sanktionierte die CNIL mehrere Verstöße von Auftragsverarbeitern, darunter fehlende technische und organisatorische Maßnahmen, die Verarbeitung ohne Weisung des Verantwortlichen oder die unterlassene Löschung personenbezogener Daten nach Vertragsende. Auch im vereinfachten Sanktionsverfahren spielten Sicherheitsmängel eine große Rolle: 14 Organisationen hatten unzureichende IT-Sicherheitsmaßnahmen wie schwache Passwörter oder geteilte Benutzerkonten im Einsatz. Weitere 14 Organisationen wurden sanktioniert, weil sie nicht mit der CNIL kooperierten, und in nochmals 14 Fällen wurden Betroffenenrechte wie Lösch--, Widerspruchs- oder Auskunftsrechte nicht gewahrt.

Darüber hinaus verhängte die CNIL Bußgelder wegen unerlaubter kommerzieller oder politischer Werbung. Für Direktwerbung per elektronischen Kommunikationsmitteln betonte die Behörde erneut, dass hierfür grds. eine Einwilligung erforderlich ist. Fünf politische Kandidaten der Europawahl 2024 wurden sanktioniert, weil sie die Rechtmäßigkeit ihrer politischen Ansprache nicht nachweisen konnten. Neben den Sanktionen sprach die CNIL 143 Compliance-Anordnungen aus, insb. im Bereich der Kinder- und Jugendhilfe. Dort stellte sie u.a. unzureichende Löschkonzepte, mangelhafte Passwort- und Berechtigungssysteme, fehlende Verarbeitungsverzeichnisse und fehlende Datenschutz-Folgenabschätzungen fest. Auch zahlreiche Webseiten, Apps und Online-Spiele wurden verpflichtet, Tracking-Mechanismen zu korrigieren, Altersskontrollen zu verbessern und transparenter über Datenverarbeitungen zu informieren.

■ Vgl. hierzu auch ZD-Aktuell 2026, 01145; Etteldorf ZD-Aktuell 2022, 01189 und ZD-Aktuell 2025, 01394.

CNIL: Arbeitsprogramm 2026–2028 veröffentlicht

ZD-Aktuell 2026, 01145

Die französische Datenschutzbehörde CNIL (Commission nationale de l'informatique et des libertés) hat ihr neues Arbeitsprogramm für die Jahre 2026–2028 vorgestellt. Ziel ist es, die wirtschaftlichen Aspekte der Datenökonomie besser zu verstehen und die ökonomischen Auswirkungen der eigenen Entscheidungen präziser zu messen.

Neben den bisherigen Themen (wie zB Wettbewerbsfähigkeit, Sanktionen und KI-Nutzung) behandelt die Behörde fortan nun auch weitere spezifische Themen, wie zB Wert und Preis personenbezogener Daten oder die Wirtschaftlichkeit von Gesundheitsdatenbanken, insb. im Hinblick auf das bevorstehende Inkrafttreten der Verordnung zum Europäischen Gesundheitsdatenraum.

Die CNIL will zudem vereinfachte Tools zur Einhaltung der DS-GVO für Investoren und Start-ups entwickeln, die auf diese Akteure in frühen Innovationsphasen zugeschnitten sind.

Auch eine jährliche Evaluation der CNIL zu Wirksamkeit ihrer Maßnahmen und zur Zufriedenheit ihrer Zielgruppen ist geplant.

■ Vgl. hierzu auch ZD-Aktuell 2025, 01327; ZD-Aktuell 2025, 01394; ZD-Aktuell 2026, 01123 und ZD-Aktuell 2025, 01481.

ZEITSCHRIFT FÜR DATENSCHUTZRECHT

ZD

ISSN 2192–5593

ZD – Zeitschrift für Datenschutzrecht

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (V.i.S.d.P.); Nina Himmelstoß, Redakteurin; Christine Völker-Albert, Redakteurin, Karin Löscher, Redaktionsassistentin; Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-226, Telefax: 089/38189-625, E-Mail: zd@beck.de.

https://de.linkedin.com/showcase/zeitschriftzd

Manuskripte und andere Einsendungen:
Alle Einsendungen sind an die o. g. Adresse zu richten. Es besteht keine Haftung für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss in Textform erfolgen. Mit der Annahme zur Veröffentlichung überträgt die Autorin/der Autor dem Verlag C.H.Beck an ihrem/seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht der Autorin/des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet.

Redaktionsrichtlinie C.H.Beck:
Redaktionsrichtlinien und Werkabkürzungen sind im Zitierportal des Verlags C.H.Beck abrufbar: www.zitierportal.de.

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, soweit sie vom Einsendenden oder von der Schriftleitung erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch im Hinblick auf Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form vervielfältigt, verbreitet oder öffentlich wiedergegeben oder zugänglich gemacht, in Datenbanken aufgenommen, auf elektronischen Datenträgern gespeichert oder in sonstiger Weise elektronisch vervielfältigt, verbreitet oder verwertet werden. Der Verlag behält sich auch das Recht vor, das Werk für die automatisierte Analyse insbesondere zur Erkennung von Mustern, Trends und Korrelationen zu verwenden.

Media Sales:
Verlag C.H.Beck GmbH & Co. KG, Media Sales, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media Consultants: Telefon (0 89) 3 81 89-687, Telefax (0 89) 3 81 89-589, E-Mail: mediasales@beck.de.
Auftragsmanagement: Telefon (089) 381 89-609, Telefax (089) 38189-589, E-Mail: anzeigen@beck.de.
Verantwortlich für den Anzeigenteil: Simon Holtz.

Verlag: Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: (0 89) 3 81 89-0, Telefax: (089) 38189-398, info@beck.de, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Amtsgericht München, HRA 48 045. Persönlich haftende Gesellschafter: Dr. h. c. Wolfgang Beck (Verleger in München) und C.H.Beck Verwaltungs GmbH, Amtsgericht München, HRB 254521.

Erscheinungsweise: Monatlich.

Bezugspreise 2026: Jahresabo € 379,– (inkl. MwSt.). Vorzugspreis für Mitglieder von Kooperationspartnern, Bezieher von MMR und IT-Recht PLUS jährlich € 295,– (inkl. MwSt.). Einzelheft € 41,– (inkl. MwSt.). Versandkosten jeweils zuzüglich. Das Abonnement beinhaltet den Zugang zum Online-Modul ZDDirekt, den Newsletter ZD-Aktuell und die ZD App. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestelei und -register sind nur mit dem jeweiligen Heft lieferbar.
Hinweise zu Preiserhöhungen finden Sie in den beck-shop AGB unter Ziff. 10.4.

Bestellungen über jede Buchhandlung und beim Verlag.

KundenServiceCenter:
Telefon: (0 89) 3 81 89-750,
Telefax: (0 89) 3 81 89-358.
E-Mail: kundenservice@beck.de

myclimate shape our future
chbeck.de/nachhaltig
produktsicherheit.beck.de

Abbestellung:
Abbestellfristen finden Sie unter: www.beck-shop.de/zd-zeitschrift-datenschutz/product/9002683

Hinweis gemäß Art. 21 Abs. 1 DS-GVO: Bei Anschriftenänderung kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeauftrag gestellt ist. Hiergegen kann jederzeit mit Wirkung für die Zukunft Widerspruch bei der Post AG eingelegt werden.

Satz: FotoSatz Pfeifer GmbH, 82110 Germering.

Druck: Druckerei Himmer GmbH, Steinerne Furt 95, 86167 Augsburg

Richtungsweisend
in 2. Auflage.

Martini/Wendehorst
KI-VO • Verordnung über Künstliche Intelligenz

2. Auflage. 2026. XX, 1374 Seiten.
In Leinen € 209,–
ISBN 978-3-406-83929-0
Neu im Dezember 2025

beck-shop.de/39073891

Auch im beck-online-Modul:
KI-Recht PLUS

Vorteile auf einen Blick

- **ausführliche Kommentierung aller Normen der KI-VO übersichtlich aufbereitet**
- **wissenschaftlich fundiert und gleichzeitig praxisnah dank vieler Beispiele**
- **stellenweise Erläuterungen zu Überschneidungen bzw. Abgrenzbarkeit zu anderen Regelwerken wie der DS-GVO**

Der Großkommentar

erläutert sämtliche Vorschriften der KI-VO ausführlich, strukturiert und gut verständlich. Er geht wissenschaftlich in die Tiefe und stellt dennoch einen engen Praxisbezug her. Dank komprimierter Einleitung durch die Herausgebenden finden die Leserinnen und Leser einen schnellen Zugang zu dieser komplexen Rechtsmaterie.

Die aktualisierte und erweiterte Neuauflage

berücksichtigt insbesondere die im Frühjahr/Sommer 2025 veröffentlichten Leitlinien, Praxisleitfäden und sonstigen Handreichungen der Europäischen Kommission

- zum Begriff des KI-Systems,
- zur KI-Kompetenz,
- zu den verbotenen KI-Praktiken,
- zu KI-Modellen mit allgemeinem Verwendungszweck und
- zu Sanktionen,

ebenso wie den Referentenentwurf zum Gesetz zur Durchführung der KI-Verordnung. Ferner wurde die seit der 1. Auflage erschienene, einschlägige Literatur umfangreich eingearbeitet.

„

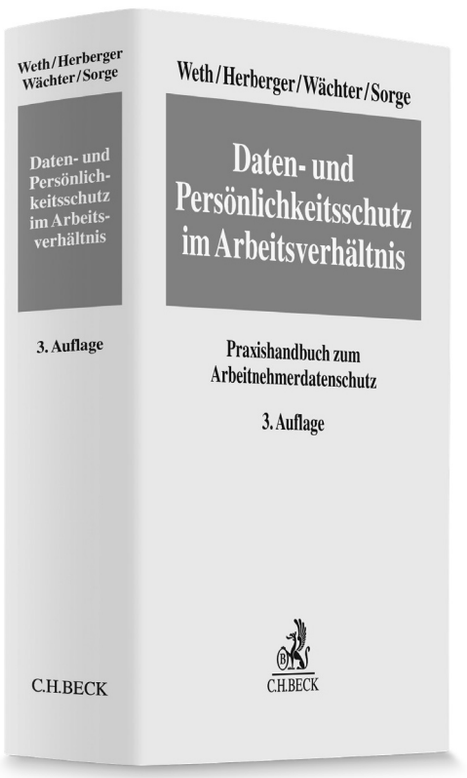
Der »Martini/Wendehorst« leistet unentbehrliche Pionierarbeiten in einer Materie, die branchen- und sektorenübergreifend nahezu jeden Arbeitgeber betrifft.

Dr. Maurice Heine, in: NZA 6/2025, zur Vorauflage

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.Beck GmbH & Co. KG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt.
178664 | Irrtümer, Preisänderungen und Druckfehler vorbehalten. Folgen Sie uns auf Mehr Infos: ch.beck.de/socialmedia

C.H.BECK

Klare Lösungen
für die Praxis.



Vorteile auf einen Blick

- aktuelle Rechtslage
- umfassende Darstellung
- Muster und Arbeitshilfen

Weth/Herberger/Wächter/Sorge
Daten- und Persönlichkeitsschutz im Arbeitsverhältnis
Praxishandbuch zum Arbeitnehmerdatenschutz

3. Auflage. 2026. XXXV, 758 Seiten.
In Leinen € 139,–
ISBN 978-3-406-78735-5
Neu im Januar 2026

beck-shop.de/33562584

Auch in den beck-online-Modulen:
Arbeitsrecht OPTIMUM
beck-personal-portal PREMIUM
Datenschutz- und Informationsfreiheitsrecht PREMIUM
Betriebsrat PLUS | PREMIUM

Das Praxishandbuch

behandelt in einzelnen Kapiteln alle Aspekte der sich im Arbeitsverhältnis stellenden Rechtsfragen zum Daten- und Persönlichkeitsschutz. Gerade im Hinblick auf zukunftsorientierte Themen wie die Durchführung von Videokonferenzen, Fragen der Gender-Gerechtigkeit und die Rolle der Rechtsinformatik bietet dieses Handbuch einen wertvollen und systematischen Überblick über diesen Problemkreis und Antworten auf offene Fragestellungen.

Die 3. Auflage

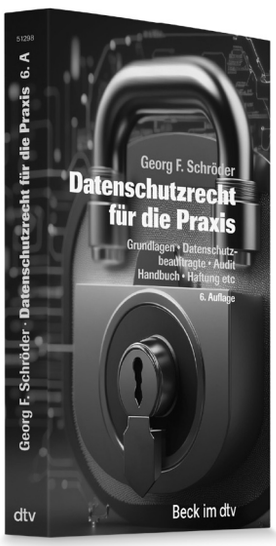
enthält u.a. neue Ausführungen zu den Themenbereichen:

- Mobiles Arbeiten, Nutzung von Video-Konferenzsystemen
- Lebenszyklus von Arbeitnehmerdaten
- People Analytics
- Daten der Schwerbehindertenvertretung
- Videos zur eigenen Person
- Betriebsvereinbarung für KI und Robotik
- Whistle Blowing
- Self-Tracking, Life-Logging, Work-Logging
- Smart Glasses und Metauniversen
- Zukunft von Legal Tech und Rechtsinformatik

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.Beck GmbH & Co. KG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt.
178784 | Irrtümer, Preisänderungen und Druckfehler vorbehalten. Folgen Sie uns auf Mehr Infos: ch.beck.de/socialmedia

C.H.BECK

Rechtssicherer Umgang mit geschützten Daten.



beck-shop.de/38959351

Von Dr. Georg F. Schröder, LL.M., RA
6. Auflage. 2026. XVII, 308 Seiten. Kartoniert € 25,90
(dtv-Band 51298) | **Neu im Dezember 2025**

Der anschauliche Band

erläutert die **wichtigsten Aspekte** des **Datenschutzrechts.** Gut verständlich aufbereitet, mit optischen Hervorhebungen der entscheidenden Elemente und vielen praktischen Beispielen, bietet der Band alles, was ein Unternehmen wissen muss, um **datenschutzkonform** zu arbeiten.

Die 6. Auflage

bringt den Band insgesamt auf den aktuellen Stand und berücksichtigt auch einige neue Themen, wie beispielsweise den **Datenschutz** bei **KI-Anwendungen.**

Beck im dtv

Erhältlich im Buchhandel oder bei:
beck-shop.de | Verlag C.H.Beck GmbH & Co. KG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 178648

Regeln für mächtige Systeme

KI-VO

Verordnung über künstliche Intelligenz
Kommentar

Hrsg. von **Dr. Silvio Andrae**, Senior Experte für KI-Regulierung, und **Jan Pohle**, Rechtsanwalt
2026, XXXVI, 1.440 Seiten, fester Einband,
€ 220,–. ISBN 978-3-503-24201-6
eBook: € 220,–. ISBN 978-3-503-24202-3
Berliner Kommentare

Der Kommentar analysiert die komplexen Anforderungen der **KI-Verordnung (EU) 2024/1689** systematisch und interdisziplinär – aus **rechtlicher, technischer und ethischer Perspektive**. Er verbindet dogmatische Präzision mit regulatorischer Einordnung und praktischer Umsetzbarkeit und bietet Orientierung für Unternehmen, Behörden, Beraterinnen und Berater sowie Entwickler bei der rechtssicheren Umsetzung.

Online informieren
und versandkostenfrei bestellen:
www.ESV.info/24201

ESV ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-265 · Fax (030) 25 00 85-275
ESV@ESVmedien.de · www.ESV.info

Legal AI – powered by Human Intelligence

Beck-Noxtua revolutioniert den juristischen Workflow – von der Recherche über die Analyse bis zur Dokumentenerstellung. Dafür sorgen Agentic AI, ein fachlich trainiertes KI-System und das Wissen der Autorinnen und Autoren im Verlag C.H.BECK. Zu dieser gebündelten Intelligenz und zu rund 60 Millionen Dokumenten hat DIE RECHTS-KI exklusiven Zugang über beck-online.

Zertifiziert & rechtskonform

Beck-Noxtua verfügt als einziger Legal AI Workspace über die sicherheitsrelevanten Zertifikate ISO/IEC 27018, BSI C5 und ISO/IEC 42001. Darüber hinaus erfüllt Beck-Noxtua die Anforderungen von DSGVO, § 43a und § 43e BRAO sowie § 203 StGB.

Souveräne Rechts-KI

Beck-Noxtua setzt bewusst auf die Serverinfrastruktur deutscher Anbieter (IONOS und Telekom Cloud). Die Server werden innerhalb der EU betrieben und befinden sich ausschließlich in deutscher bzw. europäischer Hand. Der Legal AI Workspace ist souverän von der KI über die Server bis zum Cloud-Speicher. Exklusiv mit dem Noxtua-KI-System.

In C.H.BECK-Qualität

Beck-Noxtua ist der einzige Legal AI Workspace, der exklusiven Zugriff auf Inhalte von beck-online bietet und Ergebnisse mit beck-online-Fundstellen liefert – etwa aus Kommentaren und weiterer Fachliteratur.

Beck-Noxtua
DIE RECHTS-KI

beck-noxtua.de