„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

# infobrief recht DEN

3 / 2024
März 2024


## Die Daten sind frei?

Ein Überblick über die rechtliche Zuordnung von maschinengenerierten Daten und deren Neuregelung durch den Data Act

## Ja, wer hat denn nun gewonnen?

Nach zahlreichen Entscheidungen zur Schadensersatzhaftung nach Art. 82 DSGVO hat der EuGH nun erstmals zur Bußgeldhaftung nach Art. 83 DSGVO geurteilt

## Datenschutz ist (noch immer) nicht Tatenschutz!

Videoaufzeichnungen eines Arbeitszeitbetruges sind regelmäßig als Beweismittel verwertbar

## Kurzbeitrag: Bewölkt mit Aussicht auf Souveränität

Neues europäisches Cloud-Großprojekt zur Sicherung der digitalen Souveränität in Europa

# Die Daten sind frei?

## Ein Überblick über die rechtliche Zuordnung von maschinengenerierten Daten und deren Neuregelung durch den Data Act

*von Johannes Müller*

Daten aus Internet of Things (IoT)-Geräten haben einen enormen wirtschaftlichen Wert. Von besonderer Bedeutung ist daher, wem die Rechtsordnung die Verfügungsgewalt über die Daten zuordnet. Nach bisherigem Recht wurde in erster Linie die Herrschaft desjenigen geschützt, der die faktische Kontrolle über die Daten hat. Der Data Act nimmt eine Neuzuordnung der Daten vor, insbesondere soll die Stellung des Gerätenutzers gestärkt werden.[1]

## I. Der Wert maschinengenerierter Daten für die europäische Wirtschaft

Eine Vielzahl von physischen Geräten erzeugt heutzutage große Datenmengen. Die Anwendungsmöglichkeiten dieser Geräte sind nahezu unbegrenzt. Smart-Home-Geräte wie intelligente Kühlschränke oder Thermostate, aber auch Autos können große Mengen an Informationen aufzeichnen und digital speichern. Auch in der Industrie oder Landwirtschaft liefern vernetzte Maschinen wertvolle Informationen. Aufgrund der nahezu kostenlosen Reproduzierbarkeit der Daten kann theoretisch eine unbegrenzte Anzahl von Personen von den Daten der IoT-Geräte profitieren. Damit haben sie einen enormen wirtschaftlichen Wert und das Potenzial, die wirtschaftliche Produktivität zu steigern. Gleichzeitig stehen der freien Verfügbarkeit der Daten eine Vielzahl faktischer und technischer Hindernisse entgegen.

## II. Die faktische Herrschaft des Geräteherstellers

Regelmäßig hat der Hersteller der Geräte die faktische Herrschaft über die Daten. Er entscheidet, auf welchem physischen Medium die generierten Daten verarbeitet und gesichert werden. Üblicherweise werden die Daten über das Internet auf den Servern des Geräteherstellers gespeichert, der damit den technischen Zugriff auf die Daten hat. So kann er andere von der Nutzung ausschließen oder die Daten nur unter bestimmten Bedingungen und gegen Entgelt zur Verfügung stellen. Wird anderen Personen Zugang zu den Daten gewährt, kann etwa die Weitergabe an Dritte vertraglich ausgeschlossen werden.

## III. Der rechtliche Schutz der faktischen Herrschaft über die Daten

Die Entscheidungsgewalt des Geräteherstellers findet nicht allein auf tatsächlicher Ebene statt. Das Recht schützt die faktische Herrschaft über die Daten durch verschiedene Regelungsmechanismen, die die Entscheidungsgewalt über die Verwendung der Daten sichern.

### 1. Geschäftsgeheimnisschutz

Einen umfangreichen Schutz der faktischen Herrschaft über die Daten eröffnet das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Als Geschäftsgeheimnis schützt es gemäß § 2 GeschGehG Informationen, die nicht der Allgemeinheit bekannt oder ohne Weiteres zugänglich sind und daher einen wirtschaftlichen Wert aufweisen, die Gegenstand von angemessenen Geheimhaltungsmaßnahmen sind und bei denen ein berechtigtes Interesse an der Geheimhaltung

1 Die Verordnung 2023/2854 (Data Act) ist am 11. Januar 2024 in Kraft getreten und wird ab dem 12. September 2025 direkt anwendbares Recht. Der Gesetzestext ist unter folgendem Link abrufbar https://bmdv.bund.de/SharedDocs/DE/Anlage/DG/Digitales/eu-data-act-deutsche-fassung-22-12-23.pdf?__blob=publicationFile (zuletzt abgerufen am 13.02.2024).

besteht. Unveröffentlichte Datensammlungen fallen regelmäßig unter diese Definition, so dass maschinengenerierte Daten Geschäftsgeheimnisse darstellen können. Geschützt wird durch das Geheimnisrecht der Inhaber des Geschäftsgeheimnisses. Dies ist nach § 2 Nr. 2 GeschGehG derjenige, der die rechtliche Herrschaft über das Geschäftsgeheimnis ausübt. Durch die Anknüpfung an das Merkmal der Herrschaft schützt das Geheimnisrecht denjenigen, der die faktische Herrschaft über die Daten hat, bei maschinengenerierten Daten also regelmäßig den Hersteller der Maschine. Das Geheimhaltungsrecht schützt den Inhaber des Geschäftsgeheimnisses vor unbefugtem Zugang zu den Daten, vor unbefugter Nutzung und vor unbefugter Offenlegung der Daten. Es sieht Beseitigungs-, Unterlassungs-, Löschungs- und Schadensersatzansprüche vor, wenn sich ein Dritter unbefugt Zugang zu den Daten verschafft, etwa in Form eines Datendiebstahls im Rahmen eines Hackerangriffs. Gleichzeitig stehen dem Inhaber des Geschäftsgeheimnisses Abwehransprüche zu, wenn er die Daten einem Dritten überlässt und dieser die Daten entgegen einer mit dem Geheimnisinhaber getroffenen Vereinbarung an einen Dritten weitergibt. Sofern der Dritte wusste, dass die Weitergabe der Daten unbefugt erfolgte, kann auch er Anspruchsgegner sein. Die vorsätzliche Verletzung des Geheimnisschutzes stellt zudem eine Straftat nach § 23 GeschGehG dar, wenn der unbefugte Zugang oder die unbefugte Verwendung der Daten in der Absicht erfolgt, den eigenen oder fremden Wettbewerb zu fördern oder den Inhaber des Geschäftsgeheimnisses zu schädigen.

### 2. Strafrecht

Das Strafgesetzbuch (StGB) kennt weitere Strafvorschriften, die die faktische Herrschaft über Daten sichern. Nach § 202a StGB ist das Ausspähen von Daten verboten. Ein verbotenes Ausspähen von Daten liegt vor, wenn jemand sich oder einem anderen unbefugt Zugang zu Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Ebenso stellt § 303a StGB die Datenveränderung unter Strafe, die vorliegt, wenn Daten rechtswidrig gelöscht, unterdrückt, unbrauchbar gemacht oder verändert werden.

## IV. Zuordnung der Datenherrschaft durch das Urheberrecht

Das Geheimhaltungsrecht und die dargestellten strafrechtlichen Bestimmungen sagen nur wenig darüber aus, wem die Herrschaft über die Daten zusteht. Sie schützen vielmehr denjenigen, der bereits die Herrschaft über die Daten hat. Die dargestellten Regelungen sichern somit den Status quo. Aus dem Urheberrecht lassen sich hingegen Aussagen darüber ableiten, wem die Datenherrschaft zukommen soll. Soweit das Urheberrecht Daten einer bestimmten Person zuordnet, stehen dieser Person umfassende Verwertungsrechte an den Daten zu, auch wenn sie nicht die alleinige faktische Herrschaft über die Daten hat. Nach §§ 15 ff. UrhG ist grundsätzlich nur der Urheber berechtigt, ein Werk zu vervielfältigen oder öffentlich zugänglich zu machen. Die Zuordnung eines Werkes kann im Urheberrecht nach verschiedenen Kriterien erfolgen.

### 1. Persönliche geistige Schöpfung

Das Urheberrecht schützt den Schöpfer eines Werkes, den es als Urheber bezeichnet (§ 7 UrhG).

Der Schöpfer eines Werkes wird als sein Urheber geschützt, sofern das Werk eine persönliche, geistige Schöpfung darstellt (§ 2 Abs. 2 UrhG). Eine persönliche, geistige Schöpfung liegt nur vor, wenn das Werk ein hinreichendes Maß an Individualität aufweist und Ausdruck eines individuellen, menschlichen Geistes ist. Maschinengenerierte Daten weisen diese Merkmale nicht auf, sie sind nicht die schöpferische, individuelle Leistung eines Menschen.

### 2. Wesentliche Investition bei Datenbanken

Den Hersteller einer Datenbank schützt das Urheberrecht, losgelöst von der Frage, ob die Datenbank selbst das Ergebnis einer persönlichen, geistigen Schöpfung ist. Eine Datenbank ist gemäß § 87a UrhG eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich ist. Datenbanken werden geschützt, sofern ihre Beschaffung, Überprüfung oder Darstellung eine wesentliche Investition erforderte (§ 87a Abs. 1 UrhG). Als Datenbankhersteller schützt das Urheberrecht gemäß § 87a Abs. 2 UrhG

denjenigen, der die Investition getätigt hat. Damit erscheint es zunächst naheliegend, dass ein Satz maschinengenerierter Daten als Datenbank urheberrechtlich geschützt sein kann, sofern beispielsweise die Entwicklung der Maschine eine wesentliche Investition bedurfte. Nach einer Entscheidung des EuGHs vom 9. November 2024 (Rs. C-203/02, ECLI:EU:C:2004:695) sollen jedoch nur Investitionen in die Beschaffung des Datenbankinhalts geschützt werden. Soweit eine erhebliche Investition für die Erzeugung – und nicht für die Beschaffung – der Daten erforderlich war, reicht dies für das Entstehen des Urheberrechtsschutzes nicht aus. Wird jedoch im Zusammenhang mit maschinengenerierten Daten eine wesentliche Investition getätigt, so bezieht sich diese auf die Generierung der Daten. Eine Sammlung maschinengenerierter Daten genießt daher zunächst keinen urheberrechtlichen Schutz, es sei denn, sie wurde zu einem späteren Zeitpunkt aufwendig aufbereitet.

## V. Zwischenfazit: Schutz maschinengenerierten Daten (vor dem Data Act)

Dem geltenden Recht lassen sich wenig Wertungen entnehmen, welcher Person die Nutzung von durch Geräte erzeugten Daten zusteht. Damit hat in der Regel der Maschinenhersteller die Verfügungsgewalt über die Daten. Er bestimmt den Speicherort und hat die faktische Kontrolle. Diese faktische Kontrolle wird von der Rechtsordnung durch das Geheimnisrecht und einigen strafrechtlichen Vorschriften geschützt.

## VI. Die Regelung der Datenherrschaft durch den Data Act

Eine neue Zuordnung über die Herrschaft von Daten trifft der Data Act (DA).[2] Der Data Act gilt ab dem 12. September 2025. Er bezieht sich insbesondere auf Daten von „vernetzten Produkten". Dies sind Daten, die durch die Nutzung eines physischen Geräts erlangt, generiert oder erhoben werden – also klassische iOT-Daten. Der Data Act erkennt, dass in der bisherigen Praxis regelmäßig der Hersteller des Geräts die faktische Kontrolle über die Daten hat und entscheiden kann, wem diese Daten zur Nutzung zur Verfügung gestellt werden. Diese Person bezeichnet der DA selbst als Dateninhaber. In der Regel ist dies der Gerätehersteller, im Einzelfall kann jedoch auch eine andere Person die faktische Kontrolle über die Daten haben. Die Stellung des Dateninhabers versucht der DA in Teilen aufzubrechen und stattdessen die Position des Nutzers des Geräts zu stärken.

### 1. Datennutzung nur bei Vertrag

Eine – zumindest formal – erhebliche Stärkung des Gerätenutzers erfolgt durch Art. 4 Abs. 13 DA. Dieser bestimmt, dass der Dateninhaber, also in der Regel der Hersteller, verfügbare Daten nur auf der Grundlage eines Vertrages mit dem Nutzer nutzen darf. Damit wird die Position des Dateninhabers theoretisch stark eingeschränkt. Trotz faktischer Kontrolle über die Daten darf er von dieser keinen Gebrauch machen, sofern er hierzu nicht die vertragliche Zustimmung vom Nutzer erhält. In der Praxis werden zahlreiche Produkthersteller ihre Produkte jedoch nur unter der Bedingung verkaufen oder nutzbar machen, dass der Nutzer des Produktes der Datenverwendung durch den Dateninhaber zustimmt. Handelt es sich bei dem Nutzer um einen Verbraucher, kann nicht davon ausgegangen werden, dass er die Vertragsbedingungen selbst bestimmen kann und daher zur Zustimmung „gezwungen" ist, wenn er das Gerät auch tatsächlich nutzen möchte. Handelt es sich bei dem Nutzer des Geräts selbst um einen Unternehmer, für den das Gerät etwa individuell angefertigt wurde, ist die Wahrscheinlichkeit deutlich höher, dass der Vertrag auf Augenhöhe ausgehandelt wird.

### 2. Zugangsrecht des Nutzers

Der DA schwächt nicht nur die Position des Dateninhabers, indem er ihm die Nutzung der Daten nur auf vertraglicher Grundlage erlaubt. Gleichzeitig soll der Nutzer Zugriff auf die Daten erhalten, die durch seine Nutzung des Geräts anfallen. Hierzu bestimmt Art. 3 Abs. 1 DA, dass das vernetzte Produkt so gestaltet sein muss, dass die Daten für den Nutzer einfach, sicher und in einem gängigen Format zugänglich sind. Beim Verkauf des Geräts muss der Verkäufer den Nutzer gemäß Art. 3 Abs. 2 DA umfassend darüber informieren, welche Daten das Gerät erzeugt und wie der Nutzer auf diese Daten zugreifen kann. Sofern der Nutzer nicht über das Gerät selbst auf die

2 Vgl. zur Übersicht über die verschiedenen Regelungsinhalte im Verordnungsentwurf des DA, Schaller, Data Act: Mehr Daten für alle – check!, DFN-Infobrief Recht 06/2022.

Daten zugreifen kann, muss ihm der Dateninhaber die Daten auf Anfrage unverzüglich zur Verfügung stellen (Art. 4 DA). Der Data Act differenziert hierbei nicht zwischen Daten mit und ohne Personenbezug.[3] Das Verhältnis zwischen dem Data Act und der DSGVO ist noch weitestgehend ungeklärt. Insbesondere ist die höchstrichterliche Rechtsprechung des EuGHs hierzu in den nächsten Jahren mit Spannung zu erwarten.

### 3. Faktische Datenkontrolle durch den Datennutzer

Indem der Dateninhaber verpflichtet wird, dem Nutzer Zugang zu den Daten zu gewähren, soll dieser eine faktische Kontrolle über die Daten erhalten. Der Gerätehersteller kann nicht mehr frei entscheiden, ob er Zugang zu den Daten gewährt oder nicht. Der Datennutzer ist grundsätzlich frei, über die Verwendung der nun unter seiner Kontrolle stehenden Daten zu entscheiden. Insbesondere steht es ihm frei, die Daten auch an Dritte weiterzugeben. Indem dritte Unternehmen die Daten vom Nutzer kaufen können, erhalten sie neue Möglichkeiten, an für sie wertvolle Daten zu gelangen, die sie nicht selbst generieren. Nach Art. 4 Abs. 10 DA darf der Nutzer die Daten jedoch nicht an einen Dritten weitergeben, wenn dieser die Daten für die Entwicklung eines Produkts verwenden würde, das mit dem genutzten Gerät im Wettbewerb steht. Ebenso ist der Nutzer selbst nicht berechtigt, die Daten für die Entwicklung eines Produkts zu verwenden, das mit dem Produkt des Dateninhabers konkurriert. Gemäß Art. 5 Abs. 1 DA kann der Nutzer vom Dateninhaber auch verlangen, dass dieser selbst die Daten einem Dritten in einem gängigen Format zur Verfügung stellt. Hierfür kann der Dateninhaber jedoch gemäß Art. 9 Abs. 1 DA vom Datenempfänger ein Entgelt verlangen.

## VII. Relevanz für wissenschaftliche Einrichtungen

Für wissenschaftliche Einrichtungen ergeben sich durch den Data Act neue Möglichkeiten, an Daten zu gelangen, die für ihre Forschung essentiell sein können. Wenn Forschungseinrichtungen selbst vernetzte Geräte verwenden, die Daten aufzeichnen, haben sie nun direkte Zugriffsrechte auf diese Daten. Gleichzeitig eröffnet der nutzerzentrierte Ansatz des Data Acts neue Möglichkeiten, an Daten zu gelangen, die bisher unter der ausschließlichen Kontrolle eines einzelnen Unternehmens standen, das diese Daten nicht (auch nicht gegen Entgelt) anderen zur Verfügung stellen wollte. Wissenschaftliche Einrichtungen können die Daten nur direkt von den Nutzern oder von dem betreffenden Unternehmen erhalten, wenn die Nutzer die Herausgabe der Daten an die Forschungseinrichtung verlangen. Darüber hinaus sollten die weiteren Regelungen des Data Acts im Blick behalten werden, die nicht Gegenstand dieses Infobriefs sind. Art 23-31 DA sollen etwa einen vereinfachten Wechsel zwischen Cloud-Anbietern ermöglichen, von denen auch wissenschaftliche Einrichtungen profitieren können.

3 Vgl. hierzu, Tech, Bist du ein personenbezogenes Datum?, DFN-Infobrief Recht 01/2024.

# Ja, wer hat denn nun gewonnen?

## Nach zahlreichen Entscheidungen zur Schadensersatzhaftung nach Art. 82 DSGVO hat der EuGH nun erstmals zur Bußgeldhaftung nach Art. 83 DSGVO geurteilt

*von Ole-Christian Tech*

Der Europäische Gerichtshof (EuGH) hat im lang ersehnten Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" dringende Fragen zur Bußgeldhaftung nach Art. 83 DSGVO beantwortet. Aber ist dadurch auch tatsächlich Rechtssicherheit gewonnen? Beide Parteien – die Deutsche Wohnen SE und die Berliner Staatsanwaltschaft – sehen sich als Sieger in dem Verfahren. Doch wie so oft, wenn sich zwei Boxer im Ring als Punktsieger sehen, steckt der Teufel im Detail.

## I. Die Ausgangslage

Die Deutsche Wohnen SE ist eine börsennotierte Immobiliengesellschaft mit Sitz in Berlin.
Das operative Geschäft der Deutsche Wohnen wird durch Tochtergesellschaften, sogenannten Besitzgesellschaften, geführt. Diese sind zugleich Eigentümer der Wohneinheiten, während die Deutsche Wohnen die übergeordnete Leitung des Konzerns wahrnimmt. Kerngeschäft des Konzerns ist die Vermietung von Wohn- und Gewerbeeinheiten, welche von konzernangehörigen Servicegesellschaften verwaltet werden.
Hierbei verarbeitet die Deutsche Wohnen gemeinsam mit den Tochtergesellschaften personenbezogene Daten sämtlicher Mieterinnen und Mieter. Zu den pesonenbezogenen Daten gehören etwa Identitätsnachweise, Steuer , Sozial- und Krankenversicherungsdaten sowie Angaben zu Vormietverhältnissen.
Nach einer Vor-Ort-Kontrolle wies die Berliner Beauftragte für Datenschutz die Deutsche Wohnen bereits am 23. Juni 2017 darauf hin, dass durch die Speicherung personenbezogener Daten von Mieterinnen und Mieter in einem elektronischen Archivsystem die Gewährleistung der Löschung nicht mehr erforderlicher Daten nicht gegeben sei und nicht nachvollzogen werden könne, ob die Speicherung erforderlich sei.
Die Aufsichtsbehörde forderte die Deutsche Wohnen auf, diese Dokumente bis zum Jahresende 2017 zu löschen. Die Deutsche Wohnen antwortete daraufhin, dass die Löschung aus technischen und rechtlichen Gründen nicht möglich sei.
Am 5. März 2019 führte die Aufsichtsbehörde eine erneute Prüfung in der Zentrale des Konzerns durch und setzte mit Bescheid vom 30. Oktober 2019 eine Geldbuße in Höhe von 14.385.000 Euro wegen des vorsätzlichen Verstoßes gegen Art. 5 Abs. 1 Buchst. a, c und e sowie Art. 25 Abs. 1 Datenschutzgrundverordnung (DSGVO) fest. Hinzu kamen 15 weitere Geldbußen in Höhe von 3.000 bis 17.000 Euro wegen Verstößen gegen Art. 6 Abs. 1 DSGVO.
Der Vorwurf der Datenschutzbeauftragten lautete, dass die Deutsche Wohnen es vorsätzlich unterlassen habe, die notwendigen Maßnahmen zur Ermöglichung der regelmäßigen Löschung nicht mehr benötigter oder aus sonstigen Gründen zu Unrecht gespeicherter personenbezogener Daten von Mieterinnen und Mietern zu treffen.
Hiergegen legte die Deutsche Wohnen Einspruch beim Landgericht Berlin ein. Dieses stellte das Verfahren ein, da der Bußgeldbescheid unter so gravierenden Mängeln leide, dass er nicht als Grundlage für die Festsetzung einer Geldbuße dienen könne.
Nach Auffassung des Landgerichts sei die Verhängung einer Geldbuße gegen eine juristische Person in § 30 Gesetz über Ordnungswidrigkeiten (OWiG) abschließend geregelt, der über § 41 Abs. 1 Bundesdatenschutzgesetz (BDSG) auch auf DSGVO-Verstöße nach Art. 83 Abs. 4 bis 6 DSGVO Anwendung finde. Gemäß § 30 OWiG könne eine Ordnungswidrigkeit aber nur von einer natürlichen Person und nicht von einer juristischen Person begangen werden. Der juristischen Person könnte nur ein Handeln ihrer Organmitglieder oder Repräsentanten zugerechnet werden. Nach § 41 BDSG i.V.m. § 69 Abs. 3 S. 1 OWiG ist nach dem Einspruch die Staatsanwaltschaft Berlin zuständig, die den Beschluss des Landgerichts beim Kammergericht Berlin mit einer sofortigen Beschwerde anfocht.

Das Kammergericht stellte sich sodann die Fragen, ob

1. nach Art. 83 DSGVO die Möglichkeit bestehen muss, eine Geldbuße gegen eine juristische Person zu verhängen, ohne dass der Verstoß gegen die DSGVO zuvor einer bestimmten identifizierten natürlichen Person zugerechnet wird. Insbesondere möchte es wissen, welche Relevanz der Begriff „Unternehmen" im Sinne von Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat, und

2. sollte der EuGH der Auffassung sein, dass die Möglichkeit bestehen muss, eine Geldbuße unmittelbar gegen eine juristische Person zu verhängen, welche Kriterien für die Feststellung heranzuziehen sind, dass eine juristische Person als Unternehmen für einen Verstoß gegen die DSGVO verantwortlich ist. Insbesondere möchte es wissen, ob nach Art. 83 DSGVO eine Geldbuße gegen eine juristische Person verhängt werden kann, ohne dass nachgewiesen ist, dass der ihr zugerechnete Verstoß gegen die DSGVO schuldhaft begangen wurde.

## II. Das Urteil des EuGHs

**Entscheidung und Begründung**

Das vorliegende Urteil ist aus gleich zwei Gründen hochgradig relevant. Nach einer Vielzahl von Entscheidungen zur zivilrechtlichen Schadensersatzhaftung[1] nach Art. 82 DSGVO hat der EuGH nun erstmals zur Bußgeldhaftung nach Art. 83 DSGVO geurteilt. Zum einen ist nun die Frage beantwortet, **unter welchen Voraussetzungen** der Verantwortliche haftet, das heißt, welche Ermittlungsergebnisse die Behörden erreichen müssen, um ein Bußgeld zu verhängen. Dies ist besonders angesichts des Effektivitätsgrundsatzes im Unionsrecht erheblich, da stark divergierende nationale Regelungen eine einheitliche Bußgeldpraxis und damit einen effektiven Datenschutz behindern.[2]

Zum anderen ist nun aber auch die Frage beantwortet, **wer** haftet. Das ist gerade bei komplexen multinationalen Konzernstrukturen entscheidend, da die Verhängung eines Bußgelds gegen eine mittellose Briefkastenniederlassung kaum Abschreckung für den Gesamtkonzern entfaltet.

**Juristische Person als Bußgeldadressat**

Die erste – zugegeben sehr technisch anmutende – Vorlagefrage lautet im Grunde, ob und unter welchen Umständen verantwortliche Unternehmen als juristische Person überhaupt Bußgeldadressat sein können.

Angesichts der enorm hohen Haftungssummen nach Art. 83 Abs. 4 und 5 DSGVO von 10 Millionen bis 20 Millionen Euro bzw. 2 bis 4 Prozent des weltweit erzielten Jahresumsatzes ist diese Frage nicht gerade trivial.

Die Abschreckungswirkung einer Strafe hängt schließlich von ihrem Erwartungswert ab: Wenn die drohende Strafe zwar drakonisch hoch ist, das Risiko, dass das Fehlverhalten tatsächlich bestraft wird aber verschwindend gering ist, ist der Abschreckungseffekt dahin. Aus einem scharfen Schwert des Rechtsstaats wird somit schnell ein zahnloser Tiger.

Die Vorschrift des Art. 83 DSGVO lässt das Verfahrensrecht der Mitgliedstaaten unberührt, es bleibt bei der Verfahrensautonomie der Mitgliedstaaten hinsichtlich der Verhängung von Bußgeldern.[3]

Der Begriff „Strafe" ist in der kontinentaleuropäischen Rechtsdogmatik maßgeblich von Hugo Grotius[4] geprägt und meint die Zufügung eines Übels zur Vergeltung eines Übels.

Nach traditionellem (deutschem) Rechtsverständnis setzt die Bestrafung die Handlungs- und Schuldfähigkeit des zu Bestrafenden voraus. Eine Handlung einer juristischen Person ist jedoch nur durch ihre Organe möglich. Dieser Gedanke kommt in § 30 OWiG zum Ausdruck, wonach eine juristische Person dann für das Verhalten ihrer Mitarbeiterinnen und Mitarbeiter handelt, wenn es sich bei diesen um leitende Angestellte oder Teilhaber der Gesellschaft handelt.[5]

In Deutschland erklärt § 41 Abs. 1 S. 1 BDSG einen Großteil der Vorschriften des OWiG für entsprechend anwendbar, darunter nach Auffassung des Berliner Kammergerichts auch § 30 OWiG. Somit wäre stets ein Verstoß durch Leitungspersonal erforderlich.

---

1 Hierzu bereits ausführlich Müller, Schaden oder kein Schaden, das ist hier die Frage in DFN-Infobrief Recht 03/2023, S. 10.

2 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 40.

3 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 36.

4 Geb.1583 in Delft, gest. 1645 in Rostock, einflussreicher Philosoph, Theologe und Jurist.

5 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 30.

Der EuGH führt hierzu aus, dass die DSGVO in Art. 4 Nr. 7, Art. 83 und Art. 58 Abs. 2 lit. i DSGVO zwar ausdrücklich erklärt, dass auch eine juristische Person Bußgeldadressat sein kann, jedoch gerade keine Bestimmung enthält, nach der die Verhängung einer Geldbuße gegen eine juristische Person als Verantwortliche davon abhängig wäre, dass dieser Verstoß von einem leitenden Angestellten oder einer identifizierten natürlichen Person begangen wurde.[6]
Zudem unterscheidet der Gerichtshof präzise zwischen der Autonomie der Mitgliedstaaten hinsichtlich des Verfahrensrechts, das ausdrücklich angemessene Verfahrensgarantien wie wirksame gerichtliche Rechtsbehelfe und ein ordnungsgemäßes Verfahren regeln soll, und den materiell-rechtlichen Anforderungen an das Bußgeld, für das den Mitgliedstaaten in Art. 58 Abs. 2 lit. i DSGVO gerade kein Spielraum eingeräumt wird.[7]

Bezüglich des § 30 OWiG wird der EuGH also deutlich: Die Regelung des § 30 OWiG, wonach eine Haftung nur für Verstöße durch leitendes Personal besteht, ist keine Frage des Verfahrensrechts, sondern schafft eine materielle Voraussetzung.[8] Das ist mit dem Ziel der DSGVO und dem Effektivitätsgrundsatz unvereinbar, somit ist § 30 OWiG nicht anwendbar, wenn deutsche Aufsichtsbehörden DSGVO-Bußgelder verhängen.[9]
Dies ist auch kohärent mit dem Konzept der Verantwortlichkeit nach der DSGVO. Auch da ist die Zurechnung des Verhaltens von Angestellten auf den Verantwortlichen begrenzt auf Tätigkeiten im Interesse des Verantwortlichen: Eine Zurechnung für weisungswidriges Verhalten der Mitarbeiterinnen und Mitarbeiter besteht regelmäßig nicht, wobei eine rechtssichere und trennscharfe Abgrenzung, wann eine Datenverarbeitung weisungswidrig erfolgte, im Einzelfall schwierig sein kann und ein Unternehmen auch dann für weisungswidrige Verarbeitungen haften kann, wenn es diese beispielsweise wissentlich duldet oder Anreize hierfür schafft.

Im Ergebnis haften Unternehmen somit nicht mehr nur für das Verhalten ihrer leitenden Mitarbeiterinnen und Mitarbeiter, sondern auch für jede andere Person, die im Rahmen der unternehmerischen Tätigkeit für das Unternehmen handelt.[10] Der EuGH etabliert somit eine Unternehmerhaftung, die deutlich über die Rechtslage des § 30 OWiG hinausgeht.
Des Weiteren beantwortet das Gericht, welche Stelle konkret Adressat des Bußgelds ist.
Hierfür verweist der EuGH auf seine bereits sehr feingliedrige Rechtsprechung zum europäischen Kartellrecht, genauer Art. 101 und 102 AEUV.
Der Unternehmensbegriff erfasst dort „jede eine wirtschaftliche Tätigkeit ausübende Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Er bezeichnet somit eine wirtschaftliche Einheit, auch wenn diese aus rechtlicher Sicht aus mehreren natürlichen oder juristischen Personen besteht. Diese wirtschaftliche Einheit besteht in einer einheitlichen Organisation persönlicher, materieller und immaterieller Mittel, die dauerhaft einen bestimmten wirtschaftlichen Zweck verfolgt“.[11]
Für die Bußgeldhaftung im Datenschutzrecht, die in ihrer Konzeption auch sonst stark an das Pendant im europäischen Kartellrecht angelehnt ist[12], wird somit ebenso auf einen weiten funktionalen Unternehmensbegriff verwiesen (sog. „single economic entity“). Damit ist es großen Konzernen auch nicht möglich, z. B. ihre Datenverarbeitungstätigkeit auf eine kleine mittellose Tochtergesellschaft auszugliedern, um im Haftungsfall den empfindlichen ökonomischen Konsequenzen zu entgehen. Außerdem ist für die Berechnung des Bußgelds (bis zu 2-4 % des gesamten weltweit erzielten Jahresumsatzes) ebenfalls das Konzernergebnis der gesamten wirtschaftlichen Einheit, ungeachtet der gesellschaftsrechtlichen Konzernstruktur, maßgeblich. [13]

Die erste Kernaussage des Urteils lässt sich also wie folgt zusammenfassen: Juristische Personen haften grundsätzlich für die Datenschutzverstöße ihrer Mitarbeiterinnen und Mitarbeiter, unabhängig von der hierarchischen Organisationsebene, auf

6 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 46.

7 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 45, 48.

8 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz.48.

9 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 50, 60.

10 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 44, 46.

11 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 56.

12 Siehe zum Vergleich VO Nr. 1/2003 Art. 23 für die Verhängung von kartellrechtlichen Geldbußen.

13 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen“ Rz. 59.

der diese beschäftigt sind. Dies gilt auch für Auftragnehmer. Erfasst ist also jeder, der im Namen der juristischen Person handelt und im Rahmen der geschäftlichen Tätigkeit aktiv wird. Im Umkehrschluss folgt daraus, dass Unternehmen nicht für das Handeln Dritter, etwa im Rahmen einer Cyber-Attacke, haften. Ein Verstoß des Unternehmens kann allerdings vorliegen, wenn nicht ausreichende Maßnahmen zur Verhinderung eines solchen Zugriffs getroffen wurden.

**Verschulden als Bußgeldvoraussetzung**

Die zweite Vorlagefrage betrifft letztlich den Verschuldensmaßstab im DSGVO Bußgeldregime. Es geht um die Unterscheidung zwischen verschuldensunabhängiger Haftung (strict liabilty) und einer Verschuldenshaftung.

Nach traditionellem deutschen Rechtsverständnis (sog. Schuldprinzip) setzt eine Bestrafung den Beweis der Schuld des Täters voraus.[14]
Gleichwohl kennen einzelne Mitgliedstaaten auch eine verschuldensunabhängige Haftung (sog. strict liability), bei der jeder objektive Verstoß eine Haftung nach sich zieht.[15]

Für die Bußgeldhaftung nach Art. 83 DSGVO hat der EuGH diese Frage nun eindeutig zugunsten des Schuldprinzips entschieden.[16] Es besteht aufgrund des Regelungsziels der Harmonisierung des europäischen Datenschutzes auch kein Raum für abweichende mitgliedstaatliche Haftungsregime.[17]

Dabei argumentiert das Gericht zunächst mit dem Wortlaut von Art. 83 Abs. 2 lit. b und Abs. 3 DSGVO, der Vorsatz und Fahrlässigkeit als Kriterium für die Bewertung der Schwere des Verstoßes nennt.[18] Es gibt im Text der DSGVO auch keinen konkreten Anhaltspunkt für eine verschuldensunabhängige Haftung.[18]

Auch hier greift der Gerichtshof auf seine kartellrechtliche Rechtsprechung zurück: Ein Verschulden liegt bereits vor, wenn sich der Verantwortliche über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, wobei ihm dabei nicht bewusst sein musste, dass er gegen die DSGVO verstößt.[19] Auch hier betont der EuGH noch einmal, dass Art. 83 DSGVO keine Handlung und nicht einmal eine Kenntnis eines Leitungsorgans des Unternehmens voraussetzt, vielmehr kommt es auf jede Mitarbeiterin oder jeden Mitarbeiter an.[20]

Die zweite Kernaussage des Urteils lässt sich also wie folgt zusammenfassen: Geldbußen nach Art. 83 DSGVO können nur bei Beweis von Vorsatz oder Fahrlässigkeit verhängt werden (keine strict liability). Die DSGVO erlaubt keine verschuldensunabhängige Bußgeldhaftung. Für die Zurechnung des Verschuldens kommt es auf die juristische Person als Verantwortliche insgesamt an. Das heißt auf jede einzelne Mitarbeiterin oder jeden einzelnen Mitarbeiter, unabhängig von der Managementebene. Ergibt sich aus den tatsächlichen Umständen, dass eine Mitarbeiterin oder ein Mitarbeiter Kenntnis von den wesentlichen Tatsachen des Verstoßes hatte, dann handelt die juristische Person vorsätzlich. Hätte die Mitarbeiterin oder der Mitarbeiter aufgrund der Unternehmensorganisation von den wesentlichen Tatsachen bzw. deren potentiell rechtswidriger Natur wissen müssen, liegt zumindest Fahrlässigkeit vor.

## III. Ausblick für die Praxis

Und wer hat nun gewonnen? Auf den ersten Blick wirkt das Urteil wie ein Unentschieden: Der EuGH stärkt mit der Antwort auf die erste Vorlagefrage die Aufsichtsbehörden und mit der Antwort auf die zweite die Unternehmen. Tatsächlich dürfte es sich aber als ein (deutlicher) Sieg nach Punkten für die Behörden darstellen.

Zwar ist dem verschuldensunabhängigen „strict liability"-Ansatz eine Absage erteilt worden, die Behörden müssen also dem Unternehmen einen vorsätzlich oder fahrlässig begangenen Verstoß nachweisen. Die Anforderungen an diesen Nachweis sind aber praktisch derart gering, dass es den Behörden regelmäßig

14 Siehe etwa Holländer in:BeckOK Datenschutzrecht, 46. Edition Rn. 18.

15 So bereits der EuGH, Urteil vom 09.02.2012 - C-210/10 „Urbán" Rz. 48.

16 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 78.

17 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 72.

18 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 66.

19 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 76.

20 EuGH, Urteil vom 5. Dezember 2023, Rs. C-807/21 „Deutsche Wohnen" Rz. 77.

keine größeren Probleme bereiten sollte, den Nachweis des Verschuldens zu führen.

So muss etwa nicht mehr ein Verschulden eines leitenden Angestellten vorliegen, sondern das Unternehmen wird für das Verhalten aller Mitarbeiterinnen und Mitarbeiter zu Verantwortung gezogen, die für das Unternehmen auftreten.
Etwas aufatmen können an dieser Stelle öffentliche Stellen wie (oftmals) Hochschulen und Forschungseinrichtungen als Anstalten oder Körperschaften des öffentlichen Rechts. Diese sind nach Art. 83 Abs. 7 DSGVO i.V.m. §§ 2 Abs. 1 und 43 Abs. 3 BDSG sowie der jeweiligen entsprechenden Regelung im Landesdatenschutzgesetz von einer Bußgeldhaftung befreit. Zu der Vollstreckung eines Bußgelds gegen diese Stellen wird es daher nach dem Urteil des EuGHs auch künftig nicht kommen. Doch schon aus Reputationsgründen ist dieses Urteil eine erneute Erinnerung an datenverarbeitende Stellen, das Thema DSGVO-Compliance mit Nachdruck anzugehen.

# Datenschutz ist (noch immer) nicht Tatenschutz!

## Videoaufzeichnungen eines Arbeitszeitbetruges sind regelmäßig als Beweismittel verwertbar

*Von Marc-Philipp Geiselmann*

In Fortsetzung des Urteils vom 23. August 2018 – Aktenzeichen: 2 AZR 133/18 bestätigt das Bundesarbeitsgericht (BAG), dass eine Videoaufzeichnung, die trotz Verstoßes gegen datenschutzrechtliche Bestimmungen aufgenommen wurde, ein zulässiges Beweismittel sein kann. Abzuwägen ist die Schwere des Eingriffs in die Privatsphäre des Mitarbeiters und das Interesse des Arbeitgebers.

## I. Einleitung

Ein Arbeitnehmer betritt das Werksgelände seines Arbeitgebers, einer Gießerei, am 2. Juni 2018, verlässt es aber vor Schichtbeginn wieder. Dabei wird er von einer gut sichtbaren Videokamera, auf die mittels eines Piktogramms hingewiesen wird, gefilmt. Die Arbeitsschicht lässt er sich dennoch vergüten. Der Arbeitgeber wertet, auf einen anonymen Hinweis hin, die Videoaufzeichnungen aus und kündigt dem Arbeitnehmer daraufhin außerordentlich fristlos und vier Tage später ordentlich. Der Arbeitnehmer erhebt dagegen Kündigungsschutzklage beim Arbeitsgericht. Er ist der Meinung, die Videoaufzeichnung unterläge einem Sachvortrags- und Beweisverwertungsverbot. Dem widersprach nun das Bundesarbeitsgericht (BAG) in seinem Urteil vom 29. Juni 2023 – Az.: 2 AZR 296/22.

## II. Entscheidung

In der Vorinstanz hat das Landesarbeitsgericht (LAG) Niedersachen die Wirksamkeit der außerordentlichen Kündigung abgelehnt. Es begründete sein Urteil (LAG Niedersachsen Urt. v. 06.07.2022 – 8 Sa 1149/20.) damit, dass der Beklagte Arbeitnehmer die Videoaufzeichnungen nicht als Beweismittel verwenden dürfe. Das BAG hat das Urteil des LAG aufgehoben und die Sache zurückverwiesen. In der Entscheidung stellt das BAG klar, dass der Kläger kein schutzwürdiges Interesse an der Nichtberücksichtigung der Videoaufzeichnung als Beweismittel habe.

Das BAG führte zunächst aus, dass auch die Gerichte selbst beim Fällen von Urteilen an Recht und Gesetz gebunden sind[1] und sich die Datenverarbeitung durch Gerichte auch nach der DSGVO beurteile. Sie ist rechtmäßig, wenn sie für die Erfüllung ihrer Aufgabe erforderlich ist, um die ihnen durch nationales Recht übertragene Aufgabe der Rechtsprechung zu erfüllen.[2] Werden Daten, die ursprünglich vom Arbeitgeber zu einem anderen Zweck erhoben wurden, durch das Gericht benutzt, liege darin eine Umnutzung der Daten. Diese sei zulässig, weil dadurch eine ordnungsgemäße Rechtspflege gewährleistet wird und zivilrechtliche Ansprüche durchgesetzt werden.[3]

Dies gelte sogar dann, wenn die ursprüngliche Erhebung der Daten, z. B. durch eine Videoaufzeichnung, selbst im Widerspruch zur DSGVO steht und damit rechtswidrig war.[4] Die Videoaufzeichnung erfolgte rechtswidrig, weil der Arbeitgeber mit dem Piktogramm

1 Art. 1 Abs. 3 GG.

2 Art. 6 Abs. 1 U Abs. 1 lit. e, Abs. 3 S. 1 und S. 4 DSGVO.

3 Art. 6 Abs. 4, 23 Abs. 1 lit. f und lit. j DSGVO.

4 Art. 17 Abs. 1 lit. d, Art. 4 Nr. 2 DSGVO.

lediglich auf das Vorhandensein von Kameras hinwies, nicht aber darauf, dass die Videoaufzeichnungen auch gespeichert werden. Er habe insoweit seine Informationspflichten verletzt, den Arbeitnehmer aber nicht in falscher Sicherheit gewiegt.
Nach der DSGVO sind personenbezogene Daten zu löschen, wenn deren Erhebung rechtswidrig war. Eine Ausnahme besteht jedoch, soweit die Datenverarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[5]

Das BAG zog in Betracht, ob hinsichtlich der Videoaufzeichnung ein Sachvortrags- und Beweiserhebungsverbot gilt. Dies kommt nach dem Urteil des BAG aber nur in Betracht, wenn das Beweismittel wegen einer durch Unionsrecht oder einer durch Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG geschützten Rechtsposition des Arbeitnehmers zwingend erforderlich ist. Bei einer vorsätzlich begangenen Pflichtverletzung des Arbeitnehmers, die von einer offenen Überwachungsmaßnahme erfasst wurde, sei dies nicht der Fall.[6]

Das BAG folgert zugunsten des Arbeitnehmers aus dem Recht auf effektiven gerichtlichen Rechtsschutz[7], dass das Merkmal der Erforderlichkeit in Art. 17 Abs. 3 lit. e DSGVO eine volle Verhältnismäßigkeitsprüfung durch die Gerichte erfordert. Art. 17 Abs. 3 lit. e DSGVO regelt den Ausnahmetatbestand des Rechts auf Löschung, soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Im vorliegenden Fall kann der Kläger sich daher nicht unmittelbar auf eine Löschung berufen. Dagegen hat im Rahmen einer Verhältnismäßigkeitsprüfung ein Abwägen der schützenswerten Grundrechte zu erfolgen. Nach dieser Prüfung kam das BAG zu dem Schluss, dass die Verwertung der Videoaufzeichnung durch ein Gericht nur dann unangemessen ist, wenn sie eine schwerwiegende Verletzung des Privatlebens und des Schutzes personenbezogener Daten wäre[8] und sonstige Sanktionsmöglichkeiten des Arbeitgebers zulänglich wären.

Das BAG zog auch in Betracht, dass sich für das Gericht das Verbot der Verwertung des Sachvortrags und des Beweismittels ergibt, wenn die Daten unter Verletzung des Rechts des Arbeitnehmers auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art 1 Abs. 1 GG) erhoben wurden. Dies nimmt das Gericht für den Fall an, dass der betroffene Schutzzweck des verletzten Grundrechts bei der Gewinnung der Daten auch der Verwertung entgegenstehe, sodass die Verwertung eine erneute Verletzung des Grundrechts wäre. Dies wäre beispielsweise der Fall, wenn eine Persönlichkeitsrechtsverletzung perpetuiert oder vertieft wird. Den Schutzzweck des Rechts auf informationelle Selbstbestimmung eines Arbeitnehmers vor einer offen durchgeführten Überwachungsmaßnahme sieht das BAG in der Verhaltenshemmung (psychischer Anpassungsdruck) und dem Entfaltungs-, Dokumentations- und Verbreitungsschutz. Der Arbeitnehmer hat sich im vorliegenden Fall jedoch, obwohl er von der Überwachung wusste, selbstbestimmt verhalten und das Werksgelände verlassen. Dass er dabei gefilmt wurde und für ihn somit die Gefahr der Verbreitung der Videoaufzeichnung vorhanden ist, hat er insoweit hinzunehmen, als dass der Arbeitgeber mit der Videoaufzeichnung sein rechtswidriges Verhalten – nämlich das Verlassen des Werksgeländes – nachweist, und dadurch ein schützenswerter Zweck aus dem eigenen Verhalten des Arbeitnehmers entfällt. Zudem ist die Überwachung offen geschehen. Andernfalls würde das Recht auf informationelle Selbstbestimmung dazu in Anspruch genommen werden, die Beweisführung zu unterlaufen und sich aus der Verantwortung für seine Tat zu stehlen. Das durch das Grundgesetz geschützte Recht auf informationelle Selbstbestimmung kann nicht zu dem Zweck, für vorsätzlich rechtswidriges Handeln keine Verantwortung übernehmen zu müssen, herangezogen werden. Ein Beweisverwertungsverbot käme nur bei einer schwerwiegenden Verletzung des Rechts auf informationelle Selbstbestimmung infrage, etwa bei einer dauernden offenen Überwachung oder bei Überwachung in Umkleideräumen.
Auch die bloße Möglichkeit, dass die Videoaufzeichnung kein Fehlverhalten des Arbeitnehmers zeigt, hindere nicht die Inaugenscheinnahme des Gerichts. Sollte sich dies aber tatsächlich bewahrheiten, so schulde der Arbeitgeber entweder eine Geldentschädigung[9] oder immateriellen Schadensersatz.[10]

---

5 Art. 17 Abs. 3 lit. e DSGVO.

6 Siehe auch Gielen, DFN-Infobrief 01/2019: Datenschutz ist nicht Tatenschutz.

7 Art. 47 Abs. 2 GRCh.

8 Art. 7 und 8 GRCh.

9 § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

10 Art. 82 DSGVO.

In der Folge hob das BAG das Urteil auf und verwies es an das LAG zurück. Damit gab sich das BAG aber nicht zufrieden, sondern sah sich veranlasst, für das anstehende Berufungsverfahren darauf hinzuweisen, dass auch der Abschluss einer Betriebsvereinbarung den Arbeitgeber nicht daran hindert, die Videoaufzeichnung als Beweismittel zu verwerten. Zur Begründung führt das BAG aus, dass die Parteien einer Betriebsvereinbarung zwar nicht auf die in § 88 BetrVG ausdrücklich aufgezählten Regelungsgegenstände beschränkt seien, ihnen jedoch die Befugnis fehle, Regelungen über das gerichtliche Verfahren zu treffen. Die Beweisverwertungsregeln sind in der Zivilprozessordnung (ZPO) geregelt und können nur durch den Gesetzgeber erweitert oder eingeschränkt werden.

## III. Fazit

Das BAG setzt seine arbeitgeberfreundliche Rechtsprechung aus dem Urteil vom 23. August 2018 – 2 AZR 133/18 fort, das im DFN-Infobrief Recht 01/2019 „Datenschutz ist nicht Tatenschutz“ von Nico Gielen bereits besprochen wurde. Es prüft auch die Verwertbarkeit durch die Gerichte am Maßstab der DSGVO. Bemerkenswert ist, dass das BAG am Merkmal der „Erforderlichkeit“ in Art. 17 Abs. 3 lit. e DSGVO eine volle Verhältnismäßigkeitsprüfung vornimmt.

Videoaufzeichnungen können demnach ein probates Beweismittel für Arbeitgeber in (Kündigungsschutz-) Prozessen sein. Das BAG lässt bei einer vorsätzlichen Pflichtverletzung durch den Arbeitnehmer nur wenige Ausnahmen zu wie schwerwiegende Eingriffe in die Privat- oder gar Intimsphäre, eine Totalüberwachung oder eine heimliche Überwachung.

Risikolos ist die Verwendung einer Videoaufzeichnung für den Arbeitgeber dennoch nicht. Sollte sich herausstellen, dass die Aufnahme keine Pflichtverletzung des Arbeitnehmers zeigt, schuldet der Arbeitgeber Geldentschädigung oder immateriellen Schadensersatz. Der Arbeitgeber sollte zunächst alle anderen Beweismittel wie Anhörungen oder Tätigkeitsprotokolle nutzen, bevor er eine Videoaufzeichnung als Beweis heranzieht. Selbst dann ist er gehalten, sorgfältig abzuwägen, ob sein Interesse an der Beweisführung höher wiegt als das Recht des Arbeitnehmers auf informationelle Selbstbestimmung.

# DFN Infobrief-Recht-Aktuell

## Urheberrecht: Klage der New York Times gegen OpenAI und Microsoft

Die New York Times klagt beim Bezirksgericht Manhatten gegen OpenAI und Microsoft. Hintergrund der Klage ist die unentgeltliche Nutzung urheberrechtlich geschützter Werke aus veröffentlichten Artikeln der New York Times zum Training automatischer Chatbots. Bereits am 03.08.2023 hatte die New York Times ihre Nutzungsbedingungen geändert. Aufgenommen wurde das Verbot der Nutzung von Inhalten aus der New York Times zu Zwecken des Trainings von KI-Anwendungen ohne Erlaubnis. Die Änderung beinhaltet auch die Aufnahme von Sanktionen wie Bußgelder bei Zuwiderhandlungen.

Eine weitere Klage wegen Urheberrechtsverletzungen wurde durch Getty Images gegen Stability AI erhoben. Begründet wurde die Klage ebenfalls damit, dass Stability AI Millionen von Bildern, Texten und Metadaten zur Verwendung des KI-Modells Stable Diffusion genutzt hat. Auch in Deutschland kam es inzwischen zu solchen Rechtsstreitigkeiten.

Nachfolgend erhalten Sie den Link zur Klage der New York Times gegen OpenAI und Microsoft:
https://nytco-assets.nytimes.com/2023/12/NYT_Complaint_Dec2023.pdf (zuletzt abgerufen am 19.02.2024).

## Medienrecht: European Media Freedom Act:

Einigung zum European Media Freedom Act erreicht: Der Europäische Rat und das Parlament haben im sog. Trilog-Verfahren zusammen mit der EU-Kommission am 15.12.2023 einen Kompromiss über den European Media Freedom Act (EMFA) der EU erreicht. Zum Schutz der Freiheit, des Pluralismus und der Unabhängigkeit der Medien soll eine neue Verordnung Journalistinnen und Journalisten und ihre Quellen stärken.

Hier erhalten Sie den Link zur vorläufigen Einigung:
https://www.consilium.europa.eu/de/press/press-releases/2023/12/15/council-and-parliament-strike-deal-on-new-rules-to-safeguard-media-freedom-media-pluralism-and-editorial-independence-in-the-eu (zuletzt abgerufen am 19.02.2024).

## Datenschutzrecht: Datenschutzkonformer Einsatz von KI:

Das Bayerische Landesamt für Datenschutzaufsicht veröffentlichte am 24.01.2024 eine Checkliste für Maßnahmen für die datenschutzkonforme Nutzung von KI in Unternehmen.

Hier erhalten Sie den Link zur Checkliste:
https://www.lda.bayern.de/media/ki_checkliste.pdf (zuletzt abgerufen am 19.02.2024).

# Kurzbeitrag: Bewölkt mit Aussicht auf Souveränität

## Neues europäisches Cloud-Großprojekt zur Sicherung der digitalen Souveränität in Europa

*von Johannes Müller*

Die Europäische Kommission hat am 05.12.2023 ein europäisches Cloud-Großprojekt mit Beihilfen von bis zu 1,2 Milliarden Euro genehmigt.[1] Durch das Projekt soll eine Cloud-Edge-Infrastruktur aufgebaut werden, die europäischen Werten entspricht.

## I. Digitale Souveränität durch europäisches Cloud-Computing

Datenverarbeitung wird zunehmend ausgelagert und findet auf Cloud Computing-Diensten statt. Die Anwender profitieren von der Flexibilität einer Cloud-Infrastruktur, die dynamisch an ihre Bedürfnisse angepasst werden kann und auf die über das Internet von jedem Gerät aus zugegriffen werden kann.[2] Aus der Perspektive der digitalen Souveränität birgt die Nutzung von Cloud-Infrastruktur jedoch auch beachtliche Risiken. Diese sind besonders ausgeprägt, wenn Unsicherheit darüber besteht, wer Zugriff auf die gespeicherten Daten hat. Befinden sich die Server etwa in den USA, kann ein Zugriff von staatlichen Sicherheitsbehörden nicht mit abschließender Sicherheit ausgeschlossen werden. Gleichzeitig besteht die Furcht vor privatem Datendiebstahl in Form von Hackerangriffen. Europäische Unternehmen profitieren daher von einer sicheren Cloud-Infrastruktur innerhalb der EU, deren Nutzung im Einklang mit dem europäischen Datenrecht steht.

## II. Genehmigung der IPCEI Cloud

Angesichts der Bedeutung des europäischen Cloud Computing für die digitale Souveränität ist es nicht verwunderlich, dass die Europäische Kommission den Wirtschaftsstandort Europa durch die Genehmigung und Förderung eines großen europäischen Cloud-Projekts stärken möchte. Es handelt sich dabei um das erste IPCEI (Important Project of Common European Interest) im Bereich Cloud und Edge Computing.[3] Ziel des Projekts ist der Aufbau einer Cloud-Edge-Infrastruktur der nächsten Generation, die den europäischen Werten entspricht. Die Europäische Kommission erwartet die Entstehung neuer, energieeffizienter, automatisierter und kombinierter Dienste, die heute noch nicht möglich sind. Die Entwicklung des ersten interoperablen und offen zugänglichen europäischen IT-Ökosystems, des „Multi-Provider-Cloud-to-Edge-Continuums“, soll so die digitale und technologische Souveränität Europas sichern und seine Wettbewerbsfähigkeit stärken. Gleichzeitig erhofft sich die Kommission die Förderung von CO2-reduzierenden Technologien und nachhaltigen Anwendungen im Bereich Cloud Computing.

---

1 Pressemitteilung der Europäischen Kommission, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246 (zuletzt abgerufen am 05.02.2024).

2 Vgl. Müller, Hie werden keine Daten gecloud, DFN-Infobrief Recht 08/2024.

3 Beim Edge Computing findet die Rechenleistung näher an dem Ort der Datenquelle, also näher an den Endgeräten oder Sensoren statt, an denen Daten erzeugt werden. Durch Kombination von Cloud- und Edge-Computing soll die Datenverarbeitung dort stattfinden, wo sie am günstigsten ist.

## III. Konkretes Vorhaben

Konkret werden die teilnehmenden Unternehmen eine Open-Source-Software entwickeln, die Echtzeitdienste durch verteilte Rechenressourcen in der Nähe des Benutzers ermöglicht, wodurch die Notwendigkeit der Übertragung großer Datenmengen zu zentralen Cloud-Servern verringert wird. Die einzelnen Projekte decken das gesamte Cloud-Edge-Kontinuum ab, von der Ebene der Basissoftware bis hin zu branchenspezifischen Anwendungen (z.B. im Energie-, Gesundheits- und maritimen Sektor). Unter der Co-Koordination von Deutschland und Frankreich beteiligen sich insgesamt 12 Mitgliedstaaten am IPCEI. Die Phasen Forschung, Entwicklung und erste industrielle Umsetzung werden zwischen 2023 und 2031 durchgeführt, wobei die Zeitpläne je nach Projekt und beteiligten Unternehmen variieren. Das erste innovative Ergebnis des IPCEI – eine Open-Source-Referenzinfrastruktur – wird für Ende 2027 erwartet. In diesen Phasen werden mindestens 1.000 direkte und indirekte hochqualifizierte Arbeitsplätze geschaffen, in der Kommerzialisierungsphase viele weitere.

## IV. Relevanz für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen stehen vor der Frage, ob sie Daten in Cloud-Infrastrukturen auslagern wollen und inwieweit Edge Computing zur nutzernahen Verarbeitung eingesetzt wird. Von einer innovativen europäischen Cloud-Infrastruktur, die im Einklang mit europäischem Recht steht und in der die Akteure selbst die Hoheit über ihre Daten behalten, könnten sie in Zukunft erheblich profitieren.

## Impressum

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

## Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

## Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster
Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de




### Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn