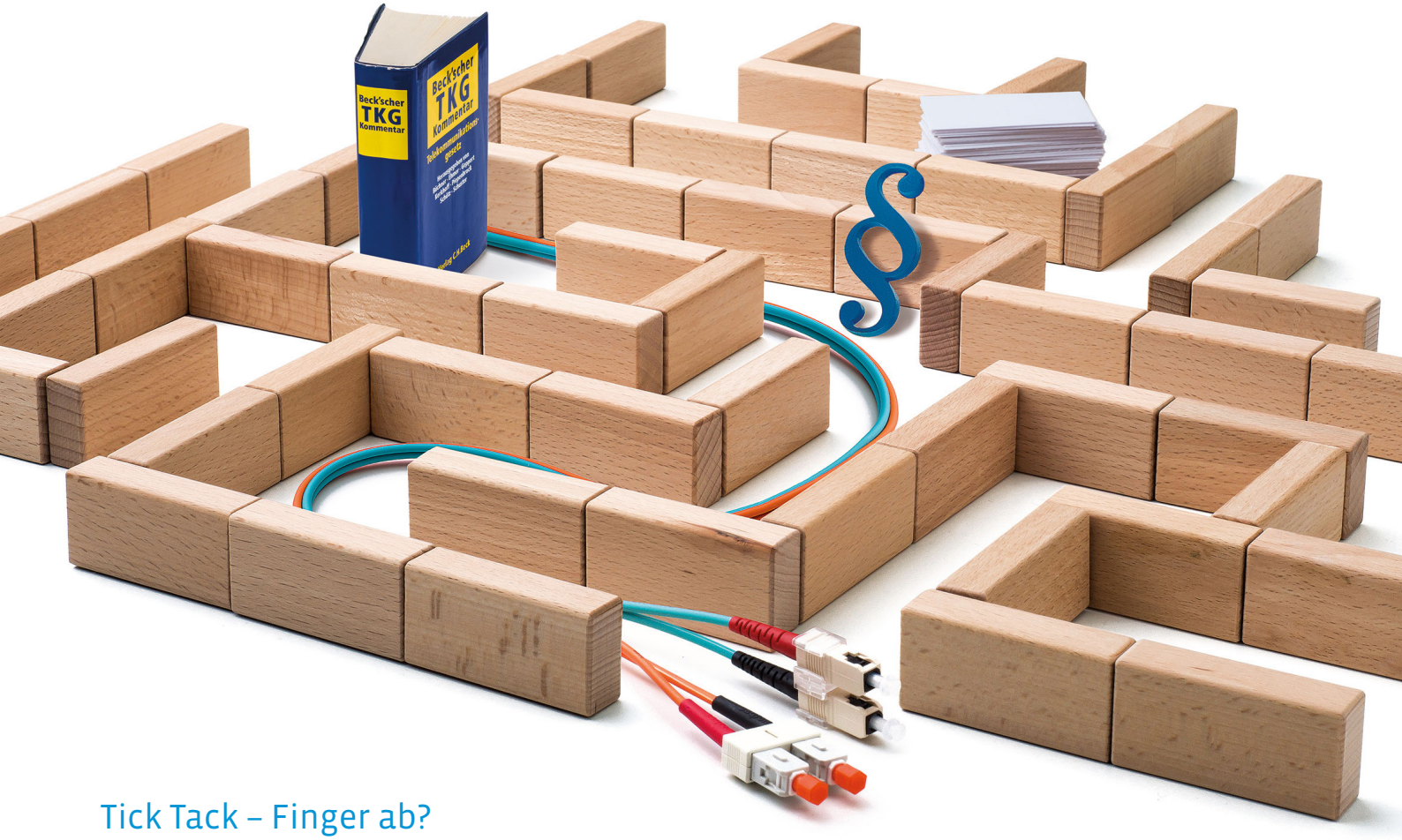
# infobrief recht

2 / 2020
Februar 2020




## Tick Tack – Finger ab?

Das Arbeitsgericht Berlin urteilt zur Zulässigkeit und Erforderlichkeit von Fingerprint Arbeitszeiterfassungssystemen ohne Einwilligung des Arbeitnehmers in die Datenverarbeitung

## Der Feind in meinem Netz – Teil 2

Die Melde- und Benachrichtigungspflichten aus Art. 33, 34 DSGVO im Zusammenhang mit Emotet-Angriffen

## Kann es Liebe sein?

LG Frankfurt am Main stuft den Versand eines Bildnisses per E-Mail als unerlaubte Nutzung ein

# Tick Tack – Finger ab?

## Das Arbeitsgericht Berlin urteilt zur Zulässigkeit und Erforderlichkeit von Fingerprint Arbeitszeiterfassungssystemen ohne Einwilligung des Arbeitnehmers in die Datenverarbeitung

*von Nicolas John*

Das Arbeitsgericht (ArbG) Berlin hat in seinem Urteil vom 16. Oktober 2019 (Az.: 29 Ca 5451/19) festgestellt, dass die Arbeitszeiterfassung durch ein Zeiterfassungssystem mittels Fingerprint nach den Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes nicht erforderlich ist. Damit ist eine Verwendung des Systems ohne Einwilligung des betroffenen Arbeitnehmers nicht zulässig und erfolgte Abmahnungen aufgrund der Weigerung des Arbeitnehmers, das System zu nutzen, müssen aus der Personalakte entfernt werden.

## I. Hintergrund

Arbeitszeiterfassungssysteme erfüllen mehrere Zwecke: Auf der einen Seite kann der Arbeitgeber kontrollieren, ob seine Angestellten ihre Stunden erfüllen, auf der anderen Seite wird der Arbeitnehmer durch ein funktionierendes System vor Überstunden geschützt. Die Ausgestaltung eines Zeiterfassungssystems kann auf verschiedene Arten geschehen. Die technischen Möglichkeiten reichen von der händischen Eintragung über eine Chipkarte, einer App auf dem Smartphone bis hin zum Fingerabdrucksensor. Doch je nach Ausgestaltung geraten Arbeitgeber und Arbeitnehmer in Konflikt, wenn eine der Parteien ihre Position gefährdet sieht. So wollen Arbeitgeber beispielsweise die Manipulationsmöglichkeiten minimieren, während Arbeitnehmer ihre höchstpersönlichen Daten nicht von jedem System verwenden lassen wollen.

Im Zusammenhang mit der Ausgestaltung eines Zeiterfassungssystems lenkte der Europäische Gerichtshof (EuGH) mit dem „Stechuhr-Urteil“ vom 14. Mai 2019 (Az.: C-55/18) die Aufmerksamkeit der Gewerkschaften und Arbeitgeberverbände auf die Systeme zur Arbeitszeiterfassung, indem er Arbeitgeber aufgrund der europäischen Arbeitszeitrichtlinie 2003/88 EG verpflichtete, verlässliche Systeme zu schaffen, mit denen „die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann“. Er stellte dabei fest, dass es sich dabei um ein „objektives, verlässliches und zugängliches System“ handeln muss, damit Höchstarbeitszeiten und Ruhepausen eingehalten werden und zum Schutz des Arbeitnehmers kontrolliert werden können. Die potentiellen Auswirkungen dieser Entscheidung wurden in den Medien kontrovers diskutiert. So begrüßten Gewerkschaften die Entscheidung, während Arbeitgeber und Berufsverbände überwiegend entsetzt und ablehnend reagierten. Letztendlich verlangt die Entscheidung nur die Einrichtung eines verlässlichen Systems. Aber es lässt offen, auf welche Weise diese Verlässlichkeit erreicht werden kann.
Die Entscheidung des ArbG Berlin fällt damit in ebendiese Thematik der zuverlässigen Arbeitszeiterfassungssysteme und sorgt damit für weiteren Diskussionsstoff rund um das Thema Zeiterfassung am Arbeitsplatz.

## II. Sachverhalt

Der Kläger ist seit Juni 2007 bei der Beklagten angestellt. Zum 1. August 2018 führte die Beklagte das Zeiterfassungssystem „ZEUS“ ein. Bis dahin trugen die Mitarbeiter der Beklagten ihre geleisteten Arbeitszeiten per Hand auf einem ausgedruckt ausliegenden Dienstplan ein. In der Regel wiesen die handschriftlich eingetragenen Arbeitszeiten auch geleistete Mehrarbeitsstunden aus. Eine Überprüfung der eingetragenen Zeiten fand nicht statt.

Durch eine Rundmail Ende Juli 2018 wurden die Mitarbeiter über die Einführung und Funktionsweise des neuen Systems aufgeklärt und die Nutzung ab August 2018 angeordnet. Im Übrigen wies die Beklagte ihre Mitarbeiter darauf hin, dass Eintragungen im schriftlichen Dienstplan nicht mehr anerkannt werden und ausschließlich die ermittelten Arbeitszeiten nach dem neuen Zeiterfassungssystem gelten.

Die Funktion des neuen Erfassungssystems basiert auf der Erkennung des Fingerprints eines Arbeitnehmers, wobei lediglich sogenannte „Minutien" (individuelle, nicht vererbbare Fingerverzweigungen) zur Erkennung erfasst werden. Eine Speicherung des vollständigen Fingerabdrucks ist nicht erforderlich, ebenso kann aus dem Minutiensatz der Fingerabdruck nicht mehr rekonstruiert werden.

Der Kläger verweigerte die Benutzung des Zeiterfassungssystems und erteilte hierzu keine Einwilligung. Seine Arbeitszeiterfassung nahm er weiterhin per Hand vor. Daraufhin mahnte die Beklagte den Kläger mehrfach ab. Der Kläger hielt die Abmahnungen für rechtswidrig und begehrte daher vor dem ArbG Berlin die Entfernung der Abmahnungen aus seiner Personalakte.

## III. Entscheidung des Arbeitsgerichts Berlin

Das ArbG Berlin verurteilte den Arbeitgeber, die Abmahnung aus der Personalakte zu entfernen. Datenschutzrechtlich sei die Verwendung der Daten des Arbeitnehmers ohne dessen Einwilligung unzulässig. Der Kläger sei nicht verpflichtet, das System zu nutzen und sei daher berechtigt, die Verwendung zu verweigern. Damit widerspricht das Gericht der Auffassung der Beklagten, dass die Verarbeitung der Daten zur Überwachung der Arbeitszeit erforderlich sei.

Das Gericht stellte zunächst fest, dass es sich bei dem Minutiendatensatz um biometrische Daten nach Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) und besondere Kategorien personenbezogener Daten im Sinne von § 26 Abs. 3 Bundesdatenschutzgesetzes (BDSG) handele. Bei diesen besonderen Kategorien kann es sich neben biometrischen Daten beispielsweise auch um Gesundheitsdaten oder Daten handeln, aus welchen die politische Meinung oder religiöse Überzeugung einer Person hervorgehen kann. Eine Verarbeitung dieser Daten könne die Privatsphäre des Mitarbeiters und damit das Recht auf informationelle Selbstbestimmung im besonderen Maße verletzen. Daher sei die Verarbeitung der Daten gemäß Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Allerdings eröffne Art. 9 Abs. 2 DSGVO verschiedene Erlaubnistatbestände, bei deren Vorliegen eine Verarbeitung (ausnahmsweise) doch zulässig sei. Diese könnten unter anderem die freiwillig erteilte Einwilligung gemäß § 26 Abs. 2 BDSG, die Erforderlichkeit der Datenverarbeitung gemäß § 26 Abs. 1 S. 1 BDSG oder eine die Verarbeitung erlaubende Kollektivvereinbarung gemäß § 26 Abs. 4 S. 1 BDSG (z. B. eine Betriebsvereinbarung) sein.

Im vorliegenden Fall lag weder eine Einwilligung vor, noch gab es eine Kollektivvereinbarung, welche eine Verarbeitung hätten erlauben können. Damit komme es maßgeblich auf die Erforderlichkeit der Datenverarbeitung zum Zwecke des Beschäftigtenverhältnisses an. Es sei daher eine umfassende Abwägung zwischen der Beeinträchtigung des Persönlichkeitsrechts des Arbeitnehmers durch das biometrische Verfahren auf der einen Seite und dem angestrebten Zweck der Datenverarbeitung auf der anderen Seite vorzunehmen. Je stärker der Eingriff, desto schwerer müsse der vom Arbeitgeber verfolgte konkrete Zweck wiegen. So stellte das ArbG fest, dass die Verwendung eines biometrischen Verfahrens bei Zugangskontrollen zu sensiblen Geschäftsbereichen gegenüber dem Persönlichkeitsrecht eher überwiege und daher eine Verwendung der biometrischen Daten hierbei angemessen sei.

Dagegen stelle die Zeiterfassung durch Fingerprint einen erheblichen Eingriff dar. Zwar könne es sein, dass es vereinzelt zum Missbrauch von Zeiterfassungssystemen durch Falscheintragungen oder durch „mitstempeln" durch Kollegen kommen könne, jedoch sei in der Regel davon auszugehen, dass sich die überwiegende Mehrheit der Arbeitnehmer rechtstreu verhalte. Daher gebe es keinen Anlass für diese Art des Kontrolleingriffs. Ein solcher könne lediglich begründet werden, wenn konkrete Umstände im Einzelfall diese Maßnahme verlangen und Nachweise über Missbräuche im erheblichen Umfang vorlägen. Jedoch hatte die Beklagte derartiges nicht vorgetragen. Weder mit Blick auf die Belegschaft läge eine solche Befürchtung des Missbrauchs vor, noch sei der Kläger in der Vergangenheit negativ aufgefallen.
Daher seien die Abmahnungen aus der Personalakte zu entfernen.

## IV. Fazit und Konsequenzen für die Hochschulen und Forschungseinrichtungen

Das Urteil des ArbG kommt nicht überraschend. Es spiegelt den aktuellen Meinungsstand der arbeitsrechtlichen Datenschützer wider und bestätigt die Auffassung, dass die Verwendung biometrischer Daten beim Zugang zu sensiblen Bereichen erlaubt ist, aber grundsätzlich nicht zur Arbeitszeiterfassung genutzt werden darf. Dennoch folgt daraus nicht, dass eine Zeiterfassung per Fingerabdruck generell unzulässig ist. Allerdings sind hier stets die Umstände des Einzelfalls maßgeblich. Zwar bestünde theoretisch die Möglichkeit ein solches System mit der Einwilligung des Arbeitnehmers einzuführen, jedoch stellen die hohen Anforderungen nach der DSGVO und dem BDSG an die Freiwilligkeit, die umfassenden Informationspflichten und die Form der Erklärung eine Hürde dar. Ebenfalls muss bei der Einwilligung bedacht werden, dass es dem Arbeitnehmer jederzeit offensteht, diese grundlos zu widerrufen. Ob dann wieder auf die Erlaubnisnorm des § 26 BDSG zurückgegriffen werden kann, ist umstritten.

In diesem Kontext wird es auch für die Wahl des Zeiterfassungssystems der Mitarbeiter an Hochschulen von Bedeutung sein, ob man unter den Gesichtspunkten der Erforderlichkeit zu einem fingerabdruckbasierten System greifen kann. Zwar ist für Hochschulen das BDSG nicht anwendbar, da sie als öffentliche Stellen der Länder gelten. Jedoch sind stattdessen die jeweiligen Landesdatenschutzgesetze (LDSG) anzuwenden. So finden sich beispielsweise in § 18 Abs. 3 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) oder in Art. 8 Abs. 1 Bayerisches Datenschutzgesetz (BayDSG) Vorschriften, welche ebenfalls die Erforderlichkeit der Verarbeitung der Daten fordern. Jedoch untersagen Länder wie beispielsweise Baden-Württemberg eine Verarbeitung biometrischer Daten, wenn diesbezüglich keine Einwilligung oder Kollektivvereinbarung vorliegen (vgl. § 15 Abs. 6 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW). Die Verarbeitung aufgrund einer Erforderlichkeit ist dann nicht möglich. Deshalb wird man an den Hochschulen und wissenschaftlichen Einrichtungen in jedem Fall vor der Entscheidung, eine fingerabdruckbasierte Zeiterfassung einzuführen, zunächst die Vorgaben des jeweils geltenden Landesdatenschutzgesetzes überprüfen und anschließend eine sorgfältige Einzelfallabwägung vornehmen müssen.

Auch das eingangs erwähnte Urteil des EuGH ändert wohl nichts an der Bewertung des zugrundeliegenden Urteils des ArbG Berlin, denn der EuGH lässt offen, auf welche Art das verlässliches System zur Zeiterfassung errichtet werden kann – und schreibt damit nicht eine Verwendung biometrischer Daten vor.

# Der Feind in meinem Netz – Teil 2

## Die Melde- und Benachrichtigungspflichten aus Art. 33, 34 DSGVO im Zusammenhang mit Emotet-Angriffen

*von Steffen Uphues*

Bei diesem Beitrag handelt es sich um eine Fortsetzung des Infobriefs „Der Feind in meinem Netz – Teil 1“ aus DFN Infobrief Recht 01/2020. Nachdem im ersten Teil beleuchtet wurde, wie sich ein Emotet-Angriff vollzieht und unter welchen Voraussetzungen eine Meldung nach Art. 33 DSGVO erfolgen muss, steht in diesem Teil im Vordergrund, wie die Meldung erfolgen sollte, wann die betroffene Person gemäß Art. 34 DSGVO zu benachrichtigen ist und welche Konsequenzen die Emotet-Angriffe für die Praxis wissenschaftlicher Einrichtungen bedeuten.

## I. Erfüllung der Meldepflichten

In Art. 33 Abs. 1 DSGVO wird ausgeführt, dass sich ein Verantwortlicher bei Bekanntwerden einer Schutzverletzung bei der zuständigen Aufsichtsbehörde melden muss, sofern diese Verletzung voraussichtlich zu einem Risiko für natürliche Personen führt. Zur Erinnerung: In Teil 1 wurde auf die Definition der Schutzverletzung in Art. 4 Nr. 12 DSGVO hingewiesen. Die Schutzverletzung meint – vereinfacht ausgedrückt – die Verletzung/Missachtung technischer Sicherheitsvorkehrungen. Im Folgenden soll erläutert werden, welche Angaben bei einer Meldung zu machen sind, in welcher Form und unter Beachtung welcher Frist diese stattzufinden hat sowie an welchen Adressaten sie zu richten ist.

### 1. Inhalt der Meldung

Der Inhalt der Meldung orientiert sich an Art. 33 Abs. 3 DSGVO. Der Aufsichtsbehörde sind Informationen zur Art der Verletzung (lit. a), zu einer möglichen Kontaktaufnahme zwecks weiterer Informationen (lit. b), zu den wahrscheinlichen Folgen der Verletzung (lit. c) sowie zu den geplanten bzw. schon umgesetzten Gegenmaßnahmen des Verantwortlichen mitzuteilen (lit. d).

Zur Einschätzung der Qualität der Schutzverletzung sind – sofern vorhanden – Angaben über die jeweilige Kategorie der Daten erforderlich. Gerade auch im Hinblick auf die wahrscheinlichen Folgen für die betroffene Person kann dies eine erhebliche Rolle spielen.

### 2. Form der Meldung

Die Erfüllung von Melde- und Informationspflichten ist oftmals an das Einhalten einer bestimmten Form geknüpft. Art. 12 Abs. 1 DSGVO äußert sich etwa dazu, in welcher Form der Verantwortliche den Informationspflichten aus Art. 13, 14 DSGVO nachzukommen hat. Eine vergleichbare Regelung existiert für Art. 33 DSGVO nicht. Somit steht es dem Verantwortlichen grundsätzlich offen, in welcher Form er seiner Meldepflicht nachkommt. Jeder Kommunikationskanal, den die zuständige Aufsichtsbehörde eröffnet hat, kann genutzt werden, wenngleich aufgrund der Komplexität der zu erteilenden Angaben eine mündliche Übermittlung per Telefon nicht zielführend erscheint. Aufgrund der Dringlichkeit der Meldung ist auch von einer schriftlichen Übermittlung per Post abzusehen. Nicht zuletzt aufgrund der Sicherheit der Übermittlung sollte – sofern möglich – auf die elektronischen Meldeformulare der Aufsichtsbehörden zurückgegriffen werden.

### 3. Fristwahrung

Die Meldung an die Aufsichtsbehörde hat nach Art. 33 Abs. 1 S.1 DSGVO unverzüglich und möglichst binnen 72 Stunden zu erfolgen. Für die Fristberechnung maßgeblich sind die Regelungen der Fristenverordnung (FristenVO). Nach Art. 3 Abs. 5 FristenVO muss jede Frist von zwei oder mehr Tagen – und somit auch die dreitägige Meldefrist aus Art. 33 Abs. 1 DSGVO – mindestens zwei Arbeitstage umfassen. Bezüglich der Meldung an die Aufsichtsbehörde hat der Verantwortliche somit für den Fall, dass Wochenend- oder Feiertage in den Zeitraum der Frist fallen, mitunter länger Zeit als die in Art. 33 Abs. 1 DSGVO genannten 72 Stunden.
Auch im Fall eines Fristversäumnisses kann die Pflichtwidrigkeit entfallen, wenn eine begründete Verzögerung nach Art. 33 Abs. 1 S. 2 DSGVO vorliegt. Die Anforderungen hinsichtlich der Ausführlichkeit der Begründung sind nicht näher bestimmt. Es erscheint sachgerecht, sich diesbezüglich am Zeitraum der Überziehung sowie an der Schwere der Schutzverletzung zu orientieren. Hinderungsgründe aus der privaten Sphäre – wie etwa Urlaub, ein Krankenhausaufenthalt oder ähnliches – bleiben unberücksichtigt. Für solche Fälle sind die innerbetrieblichen Prozesse schon im Vorfeld so zu gestalten, dass Vertreter tätig werden können. Hinsichtlich einer begründeten Verzögerung ist somit abzuwarten, unter welchen Konstellationen die Rechtsprechung eine solche annimmt.

### 4. Adressat der Meldung

Nach Art. 33 Abs. 1 S. 1 DSGVO ist die Meldung an die gemäß Art. 55 DSGVO zuständige Aufsichtsbehörde zu adressieren. In diesem Zusammenhang wird diskutiert, welche Folgen eine Meldung bei einer nicht zuständigen Aufsichtsbehörde hat. Aus den allgemeinen Pflichten der Aufsichtsbehörden ergibt sich, dass diese zumindest einen Hinweis auf ihre Unzuständigkeit geben muss. Nicht abschließend geklärt ist, ob eine unzuständige Aufsichtsbehörde die fälschlicherweise an sie gerichtete Meldung darüber hinaus an die zuständige Aufsichtsbehörde weiterleiten muss. Eine hierauf gerichtete Pflicht findet sich weder in den Regelungen zur Zusammenarbeit der Aufsichtsbehörden aus Art. 60 ff. DSGVO noch in den Regelungen zu Aufgaben und Befugnissen von Aufsichtsbehörden aus Art. 58, 59 DSGVO. Die hinter der Meldepflicht stehende Intention des Gesetzgebers könnte jedoch für eine solche Pflicht sprechen. Schließlich soll die Meldung des Verantwortlichen vor allem ermöglichen, dass die zuständige Aufsichtsbehörde geeignete Abhilfemaßnahmen ergreifen und einen bestmöglichen Schutz der betroffenen Person leisten kann. Vor diesem Hintergrund könnte man den Aufsichtsbehörden auferlegen, sich dieser Zielsetzung zu verpflichten und Meldungen bei fehlender Zuständigkeit an die zuständige Aufsichtsbehörde weiterzuleiten. Ebenfalls mit Blick auf diese Zielsetzung erscheint es jedoch wenig zweckmäßig, dem Verantwortlichen zugutekommen zu lassen, dass Aufsichtsbehörden dieser Pflicht im Einzelfall nicht nachkommen. Eine Meldung bei einer unzuständigen Aufsichtsbehörde sollte demnach nicht zu der Bewertung führen, dass der Verantwortliche seiner in Art. 33 Abs. 1 DSGVO normierten Pflicht nachgekommen ist.

## II. Dokumentationspflicht des Verantwortlichen

Art. 33 Abs. 5 DSGVO weist dem Verantwortlichen eine Dokumentationspflicht im Zusammenhang mit Schutzverletzungen zu. Bezüglich der Frage, in welchen Konstellationen eine Dokumentation anzustellen ist, erscheint eine Differenzierung angebracht: Liegt schon keine tatbestandliche Schutzverletzung vor, so sollten dem Verantwortlichen keine Dokumentationspflichten auferlegt werden. Hierfür streitet auch der Wortlaut aus Art. 33 Abs. 5 S. 1 DSGVO, der eine Verletzung voraussetzt. Liegt eine solche Verletzung vor, so hat der Verantwortliche dies zu dokumentieren – auch wenn er zum Schluss kommt, dass aus der Verletzung voraussichtlich kein Risiko resultiert. Die Einschätzung des Verantwortlichen ist schließlich eine subjektive Wertung, die für die Aufsichtsbehörde überprüfbar sein muss.

## III. Pflicht zur Benachrichtigung aus Art. 34 DSGVO

Sofern die einer Schutzverletzung folgende Risikoprognose ergibt, dass ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen vorliegt, hat der Verantwortliche nach Art. 34 Abs. 1 DSGVO die Pflicht, die betroffene Person zu benachrichtigen. Ein Unterschied zur Meldepflicht ergibt sich für den Verantwortlichen dergestalt, dass die Benachrichtigung unverzüglich erfolgen muss. Eine Höchstfrist von 72 Stunden gilt für Art. 34 DSGVO nicht. In formeller

Hinsicht hat die Benachrichtigung nach Art. 34 Abs. 2 DSGVO in klarer und einfacher Sprache zu erfolgen und muss die in Art. 33 Abs. 3 lit. b, c und d DSGVO genannten Informationen enthalten.
Als Ausnahmeregelungen bestimmt Art. 34 DSGVO drei Varianten, in denen eine Benachrichtigung trotz eines hohen Risikos nicht erfolgen muss. Zunächst ist eine Benachrichtigung entbehrlich, wenn im Vorfeld die von der Schutzverletzung betroffenen Daten mit technisch-organisatorischen Sicherheitsmaßnahmen versehen wurden (lit. a). Als eine geeignete Maßnahme erscheint hierbei vor allem die Verschlüsselung, wobei maßgeblich ist, ob die Verschlüsselung im Zeitpunkt der Schutzverletzung noch den technischen Standards im Bereich der IT-Sicherheit entspricht. Es kommen auch weitere Maßnahmen in Betracht, beispielsweise innerbetriebliche Anweisungen oder die Pseudonymisierung von Daten. Ob eine solche Sicherheitsvorkehrung geeignet ist, die Benachrichtigungspflicht entfallen zu lassen, ist im jeweiligen Einzelfall zu entscheiden.

Darüber hinaus besteht die Möglichkeit, im Nachhinein Maßnahmen zur Risikominimierung zu treffen, die etwa ein Übergreifen von bereits infizierten Systemteilen auf andere verhindern (lit. b). Ebenso entfällt die Benachrichtigungspflicht, sofern die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre (lit. c). Der Begriff des unverhältnismäßigen Aufwands wird in der DSGVO nicht näher erläutert; es scheint jedoch gerade bei einer Vielzahl an betroffenen Personen möglich, dass die individuelle Benachrichtigung aller Personen als unverhältnismäßig einzustufen ist. An die Stelle der Benachrichtigung tritt bei dieser Variante die öffentliche Bekanntmachung. Die nötigen Informationen können beispielsweise über die Webseite der Einrichtung, die Tagespresse oder auch in amtlichen Bekanntmachungen verbreitet werden.

## IV. Fazit und Konsequenzen für die Praxis wissenschaftlicher Einrichtungen

Wissenschaftliche Einrichtungen können in Bezug auf Infrastruktur und Organisation einige präventive Maßnahmen ergreifen, um sich gegen Emotet-Angriffe zu schützen. Daneben ist es von großer Bedeutung, im Fall einer Attacke schnell zu handeln und seiner Meldepflicht – sofern denn eine solche besteht – nachzukommen.

Zur Verhinderung eines Emotet-Angriffs kann eine Einrichtung an verschiedenen Stellschrauben drehen. Was die IT-Sicherheit anbelangt, sollten Sicherheits-Updates automatisiert eingespielt und Verschlüsselungstechniken genutzt werden. Admins können über Gruppenrichtlinien die Ausführung von Makros untersagen oder weitere Sicherheitsrichtlinien erlassen. Daneben sollten Maßnahmen zur Wiederherstellung angegriffener (Teil-)Systeme oder Meldewege für den Fall von Auffälligkeiten vorbereitet und getestet werden. Sollte ein Rechner infiziert worden sein, ist anzuraten, alle Passwörter, die auf diesem Rechner genutzt wurden, zu ändern. Generell ist ferner darauf hinzuweisen, dass dem Aspekt der Datensicherung – nicht nur in Bezug auf Emotet, sondern auch darüber hinaus – hohe Aufmerksamkeit gewidmet werden sollte.

Sobald ein erster Verdacht besteht, dass das System einer Einrichtung von einem Emotet-Angriff betroffen sein könnte, sollten Nachforschungen angestellt werden, ob eine Schutzverletzung vorliegt. In einem zweiten Schritt ist zu prüfen, ob diese meldepflichtig ist. Sofern eine solche Pflicht angenommen wird, sollte dieser schnellstmöglich – jedoch jedenfalls innerhalb der Frist – nachgekommen werden. Gemäß Art. 83 Abs. 4 lit. a DSGVO kann die zuständige Aufsichtsbehörde eine Verletzung der Meldepflicht mit einer Geldbuße sanktionieren. Für öffentliche Hochschulen und Forschungseinrichtungen ist die Frage nach einer etwaigen Geldbuße zwar kaum relevant, da gemäß Art. 83 Abs. 7 DSGVO, § 43 Abs. 3 BDSG gegen Behörden und sonstige öffentliche Stellen keine Geldbußen verhängt werden, sofern sie nicht als öffentlich-rechtliches Unternehmen am Wettbewerb teilnehmen. Es können im Zusammenhang mit Pflichtverletzungen jedoch Schadensersatzansprüche nach Art. 82 Abs. 1 DSGVO entstehen. Darüber hinaus können die Aufsichtsbehörden von weiteren Befugnissen aus Art. 58 DSGVO Gebrauch machen. Dies umfasst die Untersuchungsbefugnisse nach Abs. 1 (beispielsweise die Durchführung von Datenschutzüberprüfungen), die Abhilfebefugnisse nach Abs. 2 (beispielsweise die Anweisung, geltend gemachte Löschungsansprüche von betroffenen Personen umzusetzen) sowie die Genehmigungsbefugnisse nach Abs. 3.

# Kann es Liebe sein?

## LG Frankfurt am Main stuft den Versand eines Bildnisses per E-Mail als unerlaubte Nutzung ein

*von Maximilian Wellmann*

In einem kürzlich entschiedenen Rechtsstreit hat das Landgericht (LG) Frankfurt am Main geurteilt, dass der Versand eines Fotos per E-Mail ein unterlassungsbewährtes Verbreiten nach dem Kunsturhebergesetz (KUG) darstellt. Die Entscheidung enthält dabei einen bunten Strauß interessanter Fragestellungen, die vom Verhältnis des KUG zur Datenschutz-Grundverordnung (DSGVO), bis hin zu Fragen der Unterlassung im Immaterialgüterrecht reichen. Grund genug also das Urteil als Anlass zu nehmen, um einen Blick auf den aktuellen Stand im Stellungskrieg zwischen KUG und DSGVO zu werfen.

### I. Sachverhalt

In seinem Urteil vom 26.September 2019 (Az. 2-03 O 402/18), hatte das LG Frankfurt am Main konkret zu entscheiden, wie die Entnahme eines Profilbildes aus dem Karrierenetzwerk „XING“ und das anschließende Versenden dieses Bildnisses an einen Dritten via E-Mail rechtlich einzuordnen ist. Hintergrund der Versendung des Bildnisses an den Dritten war dabei die Klärung der Frage, ob es sich bei der abgebildeten Person um den Kläger in einem anderen Rechtsstreit handele. Die Versendung des Profilbildes erfolgte dabei nicht im Original, sondern in zugeschnittener Form. Die abgebildete Person, hier gleichzeitig der Kläger, mahnte den Verwender des Bildnisses ab und begehrte die Abgabe einer Unterlassungserklärung nach §§ 97 Abs. 1, 72, 23, 16 UrhG. Der Kläger führt hierzu aus, dass der Zuschnitt des Bildes durch den Verwender eine Bearbeitung i.S.v. § 23 UrhG und das Versenden des Profilbildes zudem eine Vervielfältigung i.S.v. § 16 UrhG darstelle. Schließlich sei er auch Urheber des Profilbildes, da es sich bei dem streitgegenständlichen Foto um ein durch ihn selbst angefertigtes „Selfie“ handelt. Sein Unterlassungsbegehren stützt der Kläger zudem auf eine Verletzung der Vorschriften des KUG und der DSGVO. Hierzu trägt er vor, dass die Versendung des Profilbildes ein Verstoß gegen §§ 22, 23 KUG und Art. 6 DSGVO sei, in die der Kläger nicht eingewilligt habe. Dieses Verhalten sei deshalb nach §§ 823, 1004 Bürgerliches Gesetzbuch (BGB) i.V.m. §§ 22 f. KUG, Art. 79 Abs. 1, 85 DSGVO bzw. §§ 823, 1004 BGB i.V.m. Art. 6 Abs. 1, 79 Abs. 1, 85 DSGVO unterlassungsbewährt. Der Beklagte bestreitet die rechtswidrige Verwendung des Bildnisses und zweifelt an, ob der Kläger überhaupt Urheber des streitbefangenen Profilbildes sei. Nach seiner Meinung weise das Bildnis seiner objektiven Erscheinung nach schon nicht die Merkmale eines selbständig angefertigten „Selfies“ auf. Dies verwehre dem Kläger mangels Stellung als Urheber einen Rückgriff auf den Unterlassungsanspruch aus § 97 Abs. 1 UrhG. Der Beklagte trägt zudem vor, dass sein berechtigtes Interesse an der Versendung des Bildes überwiege, was im Hinblick auf die Rechtswidrigkeit eines etwaigen Verstoßes zu würdigen sei.

### II. Entscheidung und Hintergrund

Das Gericht folgt in seinem Urteil der Rechtsansicht des Klägers und ordnet den Versand des Profilbildes per E-Mail als unerlaubte Nutzung ein. Der Beklagte habe das Profilbild durch die Versendung per E-Mail im Sinne des § 22 KUG verbreitet. Auf die Körperlichkeit der Verbreitung komme es insofern nicht an, weil auch die digitale, unverkörperte Versendung eines Bildes im Anhang einer E-Mail erfasst werde. Hier ist man zwar geneigt in dem Versenden eines Bildnisses per E-Mail an einen einzelnen Dritten keine Verbreitung zu erkennen. Dies ist jedoch ein Trugschluss, da bereits die Verbreitung an Ein-

zelpersonen zu einem der Kontrolle und dem Selbstbestimmungsrecht des Abgebildeten vorbehaltenen Übergang des Bildnisses in die Verfügungsgewalt eines anderen führt. Auch ein etwaiges Versenden eines Bildnisses über einen Messenger Dienst stellt daher ein Verbreiten im Sinne des KUG dar. Der Maßstab der Rechtmäßigkeit bestimme sich dabei nach dem abgestuften Schutzkonzept der §§ 22, 23 KUG. Hiernach dürfen Bildnisse einer Person grundsätzlich nur mit ihrer Einwilligung verbreitet werden. Ein Einwilligungserfordernis besteht allerdings nicht, wenn es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt (§ 23 Abs. 1 Nr. 1 KUG), für Bilder, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen (Nr. 2), für Bilder von Versammlungen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben (Nr. 3) sowie Bildnisse, deren Verbreitung oder Schaustellung einem höheren Interesse der Kunst dienen (Nr. 4).[1] Die Funktion des § 23 Abs. 1 KUG erschöpft sich dabei zugunsten der Informations- und Meinungsfreiheit die wichtigsten Ausnahmen vom allgemeinen Bildnisschutz nach § 22 KUG zu statuieren. An die Ausnahmetatbestände knüpft sich jedoch eine Rückausnahme an, wonach die Verbreitung eines Bildnisses trotzdem rechtswidrig ist, wenn die berechtigten Interessen des Abgebildeten überwiegen, die im Rahmen einer Interessenabwägung zu ermitteln sind. Das Überwiegen des berechtigten Interesses ist im Rahmen einer Einzelfallabwägung zu ermitteln und kommt zum Beispiel in Betracht, wenn durch die Verbreitung des Bildnisses die Intimsphäre des Betroffenen verletzt wird oder sein Interesse an der Wahrung der Privatsphäre gegenüber einer Verbreitung überwiegen.

Für den vorliegenden Fall lag eine Einwilligung des Klägers nach § 22 KUG in die Verbreitung nicht vor. Auch in dem Upload und dem Einstellen des Profilbildes auf die Homepage des Karrierenetzwerks „XING“ sieht die Rechtsprechung keine wirksame Einwilligung. Das Gericht führt sodann aus, dass die Verbreitung des Profilbildes auch in rechtswidriger Weise erfolgt sei. Die Abwägung der widerstreitenden Interessen zwischen den Interessen des Abgebildeten und denen des Beklagten als Versender des Fotos führe im konkreten Fall nicht zu einem Überwiegen der Interessen des Beklagten an einer Verbreitung des Profilbildes. Insbesondere liege keine Ausnahmen des § 23 Abs. 1 Nr. 1-4 KUG vor, die hier durch den Beklagten angeführt werden könne.

## III. Verhältnis zwischen DSGVO und KUG

Bis zum in Kraft treten der DSGVO am 25. Mai 2018 richtete sich die Verbreitung und Veröffentlichung von Personenbildern ausschließlich nach dem KUG. Mit der DSGVO hat der europäische Gesetzgeber nun aber ein Regelwerk geschaffen, das sich zwar nicht direkt auf Bildnisse bezieht, aber personenbezogene Daten im Allgemeinen betrifft. Da Personenbilder zugleich ein personenbezogenes Datum darstellen, das eine Identifizierung des Abgebildeten ermöglicht, ist der Anwendungsbereich der DSGVO grundsätzlich auch im Hinblick auf die Verbreitung und Veröffentlichung von Film- und Fotoaufnahmen eröffnet. Rechtsanwender, die ein Bildnis veröffentlichen, geraten daher grundsätzlich in den Anwendungsbereich beider Gesetze was die Frage ihres Verhältnisses zueinander aufwirft.

Kollisionsrechtlich ist dabei zu konstatieren, dass die DSGVO als europäischer Rechtsakt einen Anwendungsvorrang gegenüber dem nationalen KUG genießt. Konsequenz ist eine Verdrängung der nationalen Vorschriften im materiellen Anwendungsbereich der DSGVO. Der Anwendungsvorrang besteht aber nicht, wenn das KUG eine Ausnahmevorschrift im Sinne des Art. 85 Abs. 2 DSGVO ist. Art. 85 Abs. 2 DSGVO enthält eine Öffnungsklausel für die Ausübung der Meinungs- und Informationsfreiheit. Dies spiegelt insoweit auch den Schutzzweck des KUG wieder. Die Vorschrift eröffnet dem nationalen Gesetzgeber die Möglichkeit, Rechtsvorschriften zu erlassen, die für die Verarbeitung von personenbezogenen Daten zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken von der Verordnung abweichen oder Ausnahmen hierzu schaffen. Das Oberlandesgericht (OLG) Köln hat diesbezüglich in einer Entscheidung aus dem journalistischen Bereich entschieden, dass das nationale KUG den Anforderungen dieser Ausnahmevorschrift entspricht und daher weiter Anwendung finde.[2] Offen gelassen hat das Gericht aber die Frage, wie das Verhältnis des KUG und der DSGVO außerhalb der in Art. 85 Abs. 2 DSGVO beschrieben Regelungszwecke zu bewerten ist.

In der juristischen Diskussion ist diese Frage umstritten. Einerseits wird angenommen, dass Art. 85 Abs. 1 DSGVO eine weitere Öffnungsklausel enthält, die eine Ausnahme für Datenverar-

1 Siehe zu Einwilligung und Ausnahmetatbeständen des KUG: Klein, Das haben wir auf Band, DFN-Infobrief Recht 3/2015.

2 Zur Entscheidung des OLG Köln vom 18.06.2018 (Az.: 15 W 27/18) siehe Tiessen, Heißer gekocht als gegessen, DFN-Infobrief Recht 7/2018.

beitung zu anderen Zwecken als Absatz 2 zulässt. Andererseits wird angeführt, dass Art. 85 Abs. 1 DSGVO einen zwingenden durch die Mitgliedstaaten auszuübenden Regelungsauftrag enthalte, was in Bezug auf das KUG eine weitere Anwendung des KUG außerhalb der oben bezeichneten Zwecke ausschließen würde. Die Frage nach dem Verhältnis der beiden Regelwerke ist dabei kein Selbstzweck, da sich die Systematik der DSGVO und des KUG in Teilen deutlich voneinander unterscheiden.[3]

In der rechtlichen Beurteilung wirkt sich die skizzierte Kollision der Regelungswerke insbesondere dann aus, wenn eine Einwilligung fehlt. Das KUG statuiert hier über die Fallgruppen des § 23 Abs. 1 Nr. 1-4 KUG (vgl. II.) anders als die DSGVO mit Art. 6 Abs. 1 lit. f) Tatbestände, nach denen eine Einwilligung ausnahmsweise nicht erforderlich ist. Das KUG ist somit für den Rechtsanwender aufgrund der klar abgegrenzten Ausnahmetatbestände im Vergleich zu DSGVO anwenderfreundlicher. Dennoch findet auch im Rahmen des KUG eine nachgelagerte Interessenabwägung statt, die trotz des Vorliegens eines Ausnahmetatbestands dazu führen kann, dass der Abgebildete ein überwiegendes berechtigtes Interesse geltend macht und die Verarbeitung rechtswidrig wird. Diese wertungsoffene Interessenabwägung findet sich auch im Art. 6 Abs. 1 lit. f) DSGVO wieder, was die Rechtsprechung zu dem pragmatischen Schritt veranlasst die zu §§ 22 f. KUG entwickelten Grundsätze in die Interessenabwägung des Art. 6 Abs. 1 lit. f) DSGVO hineinzulesen und somit einen Gleichlauf in der Rechtsanwendung herzustellen. Allgemein folgen die Gerichte damit dem Postulat, was nach dem KUG früher verboten war, könne jetzt auch keine erlaubte Verarbeitung nach der DSGVO darstellen.

## IV. Rechtsansicht des LG Frankfurt am Main

Die vorliegende Entscheidung des LG Frankfurt am Main stützt sich allein auf die §§ 22 f. KUG i.V.m. Art. 85 DSGVO. Das Gericht nimmt damit scheinbar eine Fortgeltung des KUG auch außerhalb der Zwecke des Art. 85 Abs. 2 DSGVO an, da die Entnahme und Veröffentlichung eines Profilbildes von der Plattform „XING“ nicht einem künstlerischen, wissenschaftlichen, literarischen oder journalistischen Zwecke zuzuordnen ist. Damit scheint sich das Gericht derjenigen Meinung anzuschließen, die in Art. 85 Abs. 1 DSGVO eine weitere Öffnungsklausel zur Fortgeltung des KUG erkennt. Explizit äußert es sich zu dieser Frage jedoch nicht, sondern stellt vielmehr pragmatisch fest, dass „nachdem, wie oben dargelegt, die Tathandlung des „Verbreitens“ auf das KUG gestützt wurde […], kam es auf die datenschutzrechtlichen Ansprüche nicht mehr an, da das „Verbreiten“ bereits nach KUG zu untersagen war.“ Warum sich das Gericht jedoch mit dem Verhältnis zwischen KUG und der DSGVO in der vorliegenden Entscheidung nicht auseinandersetzt bleibt fraglich. Der Kläger hatte seinen Klageantrag auch maßgeblich auf eine Verletzung von Art. 6 Abs. 1 DSGVO gestützt. Nach dem generellen Anwendungsvorrang des europäischen Datenschutzrechts wäre hier eine Auseinandersetzung seitens des Gerichts zu fordern gewesen, warum außerhalb der in Art. 85 Abs. 2 DSGVO beschriebenen Zwecke über eine weitere Öffnungsklausel, Art. 85 Abs. 1 DSGVO, die Vorschriften des KUG fortgelten sollen.

Die Entscheidung überrascht insbesondere vor dem Hintergrund, dass das LG Frankfurt am Main in einer weiteren Entscheidung aus dem Jahr 2018 genau diese Frage thematisiert. Auch in dieser Entscheidung ging es um die Verletzung des Persönlichkeitsrechts durch eine Bildnisveröffentlichung.[4] Das Gericht stellte dabei fest, dass die Frage über das Verhältnis des KUG und der DSGVO außerhalb der Zwecke von Art. 85 Abs. 2 DSGVO offen bleiben könne, soweit nach den jeweiligen Voraussetzungen beider Gesetze eine Veröffentlichung rechtswidrig erfolgt sei. Der Kläger konnte im vorliegenden Fall daher einen Unterlassungsanspruch sowohl auf die Normen des KUG als auch auf die Vorschriften der DSGVO stützen, weil das Gericht einen Verstoß nach beiden Gesetzen bejahte. Dabei wendet das Gericht die §§ 22, 23 KUG und die dazu ergangene Rechtsprechung unter Berücksichtigung einer europarechtskonformen Auslegung als Gesichtspunkte, im Rahmen von Art. 6 Abs. 1 lit. f) DSGVO an, um hierüber die in der Vergangenheit entwickelten Grundsätze des KUG in die Interessenabwägung der DSGVO zu implementieren. Allgemein braucht es nach der Systematik der DSGVO einen Erlaubnistatbestand gemäß Art. 6 Abs. 1 DSGVO zur rechtmäßigen Verarbeitung von Daten. Art. 6 Abs. 1 lit. f DSGVO sieht in diesem System ebenfalls wie das KUG eine Interessenabwägung zwischen den berechtigten Interessen des Abgebildeten und denen des Verarbeiters vor. Im Rahmen dieser Abwägung gilt

3 Siehe hierzu ebenfalls Tiessen, Heißer gekocht als gegessen, DFN-Infobrief Recht 7/2018.

4 Vgl. LG Frankfurt am Main, Urteil vom 13.09.2018, Az.: 2-03 O 283/18.

es die Interessen der Parteien im Einzelfall zu ermitteln und zwar unbenommen von der Frage, ob es sich um ein rechtliches, wirtschaftliches oder ideelles Interesse handelt. Steht einem solchem Interesse des Verarbeiters ein überwiegendes Interesse des Abgebildeten gegenüber, insbesondere aufgrund einer Verletzung von Grundfreiheiten oder Grundrechten (z. B. die Verletzung des Allgemeinen Persönlichkeitsrechts) so wird die Interessenabwägung zulasten des Verarbeitenden ausfallen und die Verarbeitung des Bildnisses ist als rechtswidrig einzustufen. Die Entscheidung deutet darauf hin, dass das LG Frankfurt am Main auch hier das KUG als Ausnahmevorschrift im Sinne des Art. 85 Abs. 1 DSGVO anerkennt, da ansonsten eine Anwendung des KUG durch den Anwendungsvorrang der höherrangigen DSGVO gesperrt wäre.

## V. Fazit

Das Urteil lässt den Rechtsanwender etwas ratlos zurück. Zwar scheint das LG Frankfurt am Main eine Fortgeltung des KUG auch außerhalb der journalistischen, künstlerischen oder literarischen Zwecke über Art. 85 Abs. 1 DSGVO anzunehmen, begründet diese Rechtsanwendung jedoch nicht. Damit bleibt im Verhältnis zwischen dem KUG und der DSGVO weiter vieles im Unklaren. Zu beobachten ist allerdings die Tendenz, dass die Rechtsprechung die zu §§ 22 f. KUG entwickelten Grundsätze in die Interessenabwägung des Art. 6 Abs. 1 lit. f) DSGVO hineinliest, um eine kongruente Rechtsanwendung zwischen DSGVO und KUG zu gewährleisten. Dies folgt der Prämisse, dass ein Verbreiten das schon früher nach dem KUG verboten war, jetzt auch keine erlaubte Verarbeitung nach der DSGVO sein könne.

Die Unklarheiten im Hinblick auf das Verhältnis zwischen KUG und DSGVO sollen aber nicht den Blick darauf verstellen, dass die Entscheidung gleich in mehrfacher Hinsicht eine Relevanz für den Hochschulbetrieb entfaltet. Personenbilder werden im Wissenschaftsbetrieb sowohl zu Forschungszwecken, als auch zur Öffentlichkeitsarbeit der Hochschulen verwendet. Für Personenbildnisse, die zu wissenschaftlichen Zwecken genutzt werden, ist danach eine Fortgeltung des KUG anzunehmen. Die Feststellungen des OLG Köln über die Öffnungsklausel des Art. 85 Abs. 2 DSGVO das KUG für journalistische Zwecke weiter anzuwenden, dürften insoweit auch auf den Bereich der Wissenschaft, mithin die akademische Lehre und Forschung zu übertragen sein. Wenn von Mitarbeitern einer Hochschule oder Forschungseinrichtung allerdings Personenbildnisse zu administrativen Zwecken verarbeitet werden, ist nach derzeitigem Stand der Rechtslage nicht geklärt, ob im Rahmen dieser Verarbeitung nunmehr die Vorschriften des KUG weiterhin Anwendung finden oder allein die DSGVO anzuwenden ist. Klar ist insoweit nur, dass eine solche Verarbeitung nicht unter die Öffnungsklausel des Art. 85 Abs. 2 DSGVO fällt, da die Forschungsfreiheit nicht betroffen ist. Ob das KUG für die Öffentlichkeitsarbeit der Hochschulen und Forschungseinrichtungen anwendbar bleibt, richtet sich somit danach, ob in Art. 85 Abs. 1 DSGVO eine weitere Öffnungsklausel enthalten ist. Das LG Frankfurt am Main wendet in der vorliegenden und in der Entscheidung aus 2018 jeweils das KUG an, was auf eine Rechtsansicht des Gerichts hindeutet, das KUG als Ausnahmevorschrift im Sinne des Art. 85 Abs. 1 DSGVO einzuordnen. Dies führt aber zu der für das Gericht charmanten, für den Rechtsanwender allerdings eher problematischen Lösung, dass sofern die Voraussetzungen beider Gesetze vorliegen, sowohl die DSGVO als auch das KUG im Rahmen der Verbreitung von Bildnissen Anwendung finden können. Abhilfe wird hier absehbar nur der EuGH mit einer klärenden Entscheidung zur Auslegung des Art. 85 DSGVO liefern können.

Allgemein ruft die Entscheidung darüber hinaus zur Vorsicht beim Versand von Personenbildnissen auf, die aus öffentlichen zugänglichen Quellen, wie Karriereplattformen entnommen werden. Ein Betroffener kann hier aufgrund der unklaren Rechtslage eine unzulässige Verwendung eines Personenbildnisses unter Rückgriff auf die Vorschriften des KUG und/oder der DSGVO abmahnen und den Verarbeiter auf Unterlassung und ggf. Schadensersatz in Anspruch nehmen. Hierbei ist zu beachten, dass in dem Upload eines Personenbildnisses auf eine Plattform keine Einwilligung gesehen werden kann. Der insoweit rechtssichere Weg ist daher die Einholung einer Einwilligung des Betroffenen in die Verarbeitung (DSGVO) bzw. Verbreitung (KUG), die den Anforderungen beider Gesetze entspricht.

## Impressum

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

## Herausgeber

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

## Redaktion

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