DFN
infobrief recht

10 / 2020
Oktober 2020

Kontrolle ist gut, Vertrauen ist besser!

Zur Frage der datenschutzrechtlichen Zulässigkeit technischer Überprüfungs- und Kontrollmaßnahmen im Homeoffice

Schwamm drüber, Google

Neue Urteile zum Recht auf Vergessenwerden

Data Wars: Der Betroffene schlägt zurück

Das Arbeitsgericht Düsseldorf verurteilt Unternehmen zu Schadensersatz gemäß Art. 82 Abs. 1 DSGVO i.H.v. 5.000 Euro

Kontrolle ist gut, Vertrauen ist besser!

Zur Frage der datenschutzrechtlichen Zulässigkeit technischer Überprüfungs- und Kontrollmaßnahmen im Homeoffice

von Maximilian Wellmann

Eine der zentralen Lehren, der immer noch andauernden Coronavirus-Pandemie, ist die geradezu surreal anmutende rasante digitale Transformation der Arbeitswelt. Homeoffice, Telearbeit und Mobile Office haben in Pandemie Zeiten Hochkonjunktur, um den Betrieb am Laufen zu halten. Zu vermuten ist dabei, dass sich der Trend zum dezentralen Arbeiten noch weiter verstärken wird, wie auch die politische Debatte um ein „Recht auf Homeoffice" zeigt. Große Tech-Unternehmen wie z. B. Google sind da bereits weiter und haben angekündigt, dass ein Großteil ihrer Mitarbeiter bis Juli 2021 im Homeoffice verbringen wird. Auch Hochschulen und Forschungseinrichtungen bieten Mitarbeitern - nicht erst seit Ausbruch der Coronavirus-Pandemie - die Möglichkeit des Homeoffice. Dabei stellt sich für den Arbeitgeber regelmäßig die Frage, inwieweit eine Leistungs- und Verhaltenskontrolle der Mitarbeiter durch technische Kontrollmaßnahmen im Homeoffice möglich und ggf. zulässig ist. Hier trifft dann die Realität des technischen Möglichen auf die beschränkende Regulierung des Datenschutzrechts, die es in der Praxis aufzulösen gilt.

I. Vorfragen und notwendige Differenzierungen

Homeoffice, Telearbeit, Mobile Working, etc. spiegeln das begriffliche Potpourri und die damit einhergehenden mannigfaltigen Erscheinungsformen der digitalen Arbeitswelt wieder. Am weitaus geläufigsten ist dabei der Begriff des Homeoffice, der allerdings reichlich konturenlos daherkommt und keine allgemeingültige Definition kennt. Eine inhaltliche Annäherung ermöglicht insoweit § 2 Abs. 7 Arbeitsstättenverordnung (ArbStättV), der den Begriff der Telearbeit legaldefiniert und diesen annimmt, wenn „fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat." Ausgehend von der Prämisse, dass zwischen dem Arbeitgeber und dem Arbeitnehmer die Möglichkeit zum Homeoffice entweder arbeitsvertraglich vorgesehen ist, eine entsprechende „Homeoffice-Vereinbarung" besteht oder Homeoffice als betriebliche Übung geduldet wird, stellt sich für den Arbeitgeber schnell die Frage, wie er den seinerseits gewährten Vertrauensvorschuss durch eine effektive Leistungs- und Verhaltenskontrolle des Arbeitnehmers überprüfen kann. Datenschutzrechtlich sind dabei aufgrund des Schutzguts der informationellen Selbstbestimmung zwei Fallkonstellationen zu unterscheiden.

Zunächst ist dabei zu klären, ob im Rahmen des Homeoffice, mit Endgeräten des Arbeitgebers gearbeitet wird (Dienstlaptops, Diensthandys) oder eine sog. „Bring Your Own Device" (BYOD) Lösung zum Tragen kommt, bei der der Arbeitnehmer ein privates Endgerät zur Erfüllung seiner arbeitsvertraglichen Pflichten nutzt. Eine Leistungskontrolle im Rahmen des letztgenannten Modells kommt dabei nur unter sehr hohen Hürden in Betracht, da durch etwaige Kontrollmaßnahmen in die Privatsphäre des Arbeitnehmers und damit in den Kern der informationellen Selbstbestimmung eingegriffen wird. In Ausnahmefällen ist allein die Implementierung von sog. Container-Apps in Betracht zu ziehen, die die Daten so sortieren, dass der Zugriff auf den jeweiligen Bereich beschränkt wird. Damit lässt sich eine strikte Trennung zwischen dem privat genutzten Bereich und dem Arbeitsbereich auf dem Endgerät des Arbeitnehmers sicherstellen.

Im Regelfall stellt der Arbeitgeber dem Beschäftigten, auch aus datenschutzrechtlichen Erwägungen, ein Endgerät zur Verfügung.

II. Datenschutzrechtliche Grundlagen

Kontrollmaßnahmen gegenüber Mitarbeitern im Homeoffice stellen eine Verarbeitung personenbezogener Daten dar. Aus der Regelungssystematik der Datenschutz-Grundverordnung (DSGVO), die ein Verbot mit Erlaubnisvorbehalt vorsieht, ergibt sich die Notwendigkeit einer Rechtsgrundlage für den jeweiligen Verarbeitungsvorgang. Ist dabei die Privatnutzung eines zur Verfügung gestellten Dienstlaptops nicht erlaubt, richtet sich die Überprüfung und Kontrolle nach Art. 88 Abs. 2 DSGVO i.V.m. § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG).

Umgekehrt wird bei einer erlaubten Privatnutzung vertreten, dass auch die datenschutzrechtlichen Bestimmungen der §§ 91 ff. Telekommunikationsgesetz (TKG) anwendbar seien. Hierbei ist allerdings aufgrund der unklaren Rechtslage und in Ermangelung einer höchstrichterlichen Entscheidung umstritten, wie das genaue Verhältnis der beiden Regelungswerke zueinander ausgestaltet ist. Allerdings sollten wegen der bestehenden Rechtsunsicherheit die Regelungen des TKG weiterhin Beachtung finden, da im Anwendungsbereich des TKG immer Vorsicht geboten ist. So kann z. B. beim Herausfiltern oder unbefugten Öffnen von E-Mails ein unbefugter Eingriff in das Fernmeldegeheimnis vorliegen und damit auch potentiell Straftatbestände wie § 206 StGB erfüllt sein Oberlandesgericht (OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04).

Für die Mitarbeiter von Universitäten, Forschungseinrichtungen und andere öffentlichen Stellen kommen regelmäßig die Datenschutzgesetze der jeweiligen Länder (z. B. § 18 Abs. 1 Datenschutzgesetz NRW (DSG NRW) sowie § 26 Abs. 1 S. 1 BDSG zur Anwendung. Danach muss die Datenverarbeitung zum Zwecke der Begründung oder Durchführung des Beschäftigungsverhältnisses erforderlich sein. Dieses Erforderlichkeitsprinzip gilt selbstverständlich auch mit Blick auf die Implementierung einzelner Maßnahmen zur Kontrolle der Tätigkeit im Homeoffice.

III. Technische Überprüfungs- und Kontrollmaßnahmen und ihre datenschutzrechtliche Einordnung

Geht es nunmehr darum, einzelne Maßnahmen auf ihre datenschutzrechtliche Zulässigkeit zu prüfen, sind zunächst die rivalisierenden Interessenlagen zwischen Arbeitgebern und Arbeitnehmern zu betrachten. Seitens des Arbeitgebers besteht hierbei ein gesteigertes Interesse, den durch die Einräumung des Homeoffice gewährten Vertrauensvorschuss durch eine engmaschigere Verhaltens- und Leistungskontrolle des Mitarbeiters zu validieren. Auf der anderen Seite stehen einer ausufernden Anwendung solcher Maßnahmen die Schutzgüter des Datenschutzrechts und damit die Persönlichkeitsrechte des jeweiligen Mitarbeiters entgegen.

Betrachtet man einzelne Kontrollmaßnahmen en détail verbietet sich aber eine pauschale Einordnung. Dies gilt insbesondere mit Blick auf die Auswertung von Log-in Daten. Mithilfe dieser Log-in Daten kann der Arbeitgeber nachvollziehen, wann sich der Mitarbeiter am Endgerät mit seinen Benutzerdaten ein- und ausgeloggt hat.

Regelmäßig bringt dies dem Arbeitgeber jedoch nur einen geringen Erkenntnisgewinn. Der Einsatz von Logfiles oder umfangreicher Monitoring-Software sind hingegen weitergehender, da solche Programme theoretisch in der Lage sind die lückenlose Dokumentation des Verhaltens des Beschäftigten, z. B. über die Erfassung des Browserverlaufs oder die Überwachung der E-Mail-Kommunikation zu ermöglichen.[1] Auch der Einsatz von Software- oder Hardware basierten Keyloggern („Tasten-Protokollierer“), die sich zwischen Betriebssystem und Tastatur schalten und die Tastenanschläge an den Systemadministrator weitergeben sowie der Zugriff auf Webcams und Standortdaten wird oftmals arbeitgeberseitig zur effektiven Verhaltenskontrolle der Beschäftigten gewünscht.

Die Implementierung solcher Maßnahmen begegnet datenschutzrechtlich allerdings sehr großen Bedenken. Auch wenn ein legitimes Interesse des Arbeitgebers daran besteht, bei einem Verbot der Privatnutzung auf dem Dienstlaptop oder dem Diensthandy die Einhaltung dieses Verbots zu kontrollieren, darf dies nicht zu einer (Dauer-) überwachung der

1 Siehe hierzu, Gielen, Big Brother Is Watching You, DFN-Infobrief Recht, 05/2019.

Beschäftigten führen. Instanzgerichtlich hat ein Urteil des Landesarbeitsgerichts Köln (LAG Köln, Urt. v. 7.2.2020, 4 Sa 329/19) dabei bestätigt, dass eine Kontrolle der Verlaufsdaten oder der E-Mail-Kommunikation nach § 26 Abs. 1 S. 1 BDSG erforderlich sein kann. Die ständige Rechtsprechung des Bundesarbeitsgerichts (BAG) setzt dem allerdings klare Schranken, indem das Gericht feststellt, dass eine anlass- und lückenlose arbeitgeberseitige Überwachung nicht erfolgen darf. Denn eine lückenlose technische Überwachung ohne zweckgebundenen Anlass wird aufgrund des hohen Überwachungsdrucks, der schweren Persönlichkeitsrechtsbeeinträchtigung sowie eines massiven Eingriffs in das Recht auf informationelle Selbstbestimmung für den Arbeitgeber regelmäßig als rechtswidrig eingestuft Sollten dennoch einzelne rechtswidrige Überwachungsmaßnahmen seitens des Arbeitgebers ergriffen werden, so besteht die Gefahr mit diesen Handlungen in den Anwendungsbereich strafrechtlicher Normen, wie z. B. § 202a StGB zu geraten.

Eine Ausnahme von dem oben beschriebenen Verbot besteht allein dann, wenn ein konkreter Verdacht auf die Begehung einer Straftat im Rahmen des Beschäftigungsverhältnisses besteht. Dann können Überprüfungs- und Kontrollmaßnahmen im Einzelfall auf § 26 Abs. 1 S. 2 BDSG gestützt werden. Gleichwohl sollten hier regelmäßig zur Erreichung des Ziels (Aufdeckung einer Straftat) die mildesten Mittel, wie z. B. der Einsatz und die Auswertung von Logfiles, in Betracht kommen, sodass im Ergebnis die Ausforschung von Beschäftigten durch die Webcam nie in Betracht kommen wird. In jedem Fall muss für jede Einzelmaßnahme eine umfassende Verhältnismäßigkeitsprüfung stattfinden, um das mildeste und gleichzeitig effektivste Kontrollmittel zu identifizieren. Die Kontrolle sollte daher beispielsweise in Anwesenheit des Arbeitnehmers vollzogen werden, wenn diese Überprüfungsmaßnahme geeignet ist, den legitimen Zweck gleichwohl zu erreichen.

IV. Mitwirkung des Betriebs- oder Personalrats

Entscheidet sich der Arbeitgeber eine technische Leistungs-/oder Verhaltenskontrollen zur Überwachung der Beschäftigten zu ergreifen, muss in Unternehmen mit einem Betriebsrat, dieser den Maßnahmen, gem. § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) zustimmen. Eine äquivalente Bestimmung findet sich mit § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz (BPersVG) (und den entsprechenden Landesgesetzen) auch für Hochschulen und Forschungseinrichtungen mit einem Personalrat. Die Vorschrift ist dabei bewusst weit gefasst um der mit den fortschreitenden technischen Innovationen verbundenen Gefahr einer verstärkten potentiellen Beeinträchtigung der Persönlichkeitsrechte der Beschäftigten effektiv entgegenzutreten. Dem Mitbestimmungserfordernis des Personalrats unterliegen deshalb sämtliche technische Maßnahmen, die zur Aufgabe haben, unter Ausnutzung ihrer technischen Voraussetzungen das Verhalten und/oder die Leistung der Beschäftigten zu überwachen und zwar unabhängig davon, ob dies am Arbeitsplatz im Unternehmen geschehen soll oder im Homeoffice.

V. Fazit

Die Relevanz technischer Prüfungs- und Kontrollmaßnahmen im Homeoffice hat sich durch die Coronavirus-Pandemie noch einmal erheblich verstärkt. Hinzu kommt das aktuelle Urteil des Europäischen Gerichtshofs (EuGH, Urt. v. 14.5.2019, C-55/18), das den nationalen Gesetzgebern die Pflicht auferlegt, die Erfassung der Arbeitszeit von Beschäftigten künftig so zu regeln, dass diese genauer erfasst werden kann. Die Umsetzung dieser Vorgaben ist bisweilen jedoch noch nicht erfolgt. Es muss abgewartet werden, welche gesetzlichen Regelungen in Deutschland gelten werden. Für die Zukunft ist damit aber nicht auszuschließen, dass technische Systeme, die zumindest eine Zeiterfassung ermöglichen, weiter um sich greifen werden und damit verbundene datenschutzrechtliche Fragestellungen weiter an Relevanz gewinnen werden. Auch für Hochschulen und Forschungseinrichtungen ist die Thematik von besonderem Interesse. Aufgerufen sei aber zur Zurückhaltung, gilt doch, dass eine Implementierung technischer Prüfungs- und Kontrollmaßnahmen schnell an die Grenzen des datenschutzrechtlich Zulässigen gerät. Vielmehr gilt, dass eine ausufernde Überwachung im Homeoffice datenschutzrechtlich per se nicht möglich ist und punktuelle Überwachungsmaßnahmen nur dann getroffen werden können, wenn die Maßnahme nach einer Abwägung auch zur Durchführung des Arbeitsverhältnisses erforderlich ist.

Schwamm drüber, Google

Neue Urteile zum Recht auf Vergessenwerden

von Marten Tiessen

Das Internet ist wie ein Elefant, der nie vergisst. Einmal eingespeist, bleiben personenbezogene Daten länger abrufbar, als manch einem lieb ist. Die Datenschutzgrundverordnung (DSGVO) sichert zwar jedem das Recht auf Vergessenwerden zu, ab wann die Amnesie des digitalen Gedächtnisses eingefordert werden kann, ist aber nicht immer eindeutig bestimmbar. Auch ist es nicht immer einfach gegen denjenigen vorzugehen, der die Daten selbst hochgeladen hat. Daher bietet es sich manchmal an, stattdessen gegen Suchmaschinenbetreiber wie Google vorzugehen, welche die personenbezogenen Daten einem breiteren Publikum zuführen. Mehrere höchstrichterliche Urteile haben in jüngster Zeit darüber entschieden, ob ein Löschungsantrag gegenüber Google Erfolg hat.

I. Das Recht auf Vergessenwerden

Google Search ist meist die erste Anlaufstelle, um an Informationen im Internet zu gelangen. Dazu gehören auch personenbezogene Daten, deren Veröffentlichung nicht unbedingt im Interesse der Betroffenen liegt. Mitunter können die Daten sogar rechtswidrig veröffentlicht worden sein. Der Rechtsweg gegen die Webseitenbetreiber, die diese Informationen veröffentlichen, kann beschwerlich sein. Alternativ besteht daher die Möglichkeit, gegen den Suchmaschinenbetreiber, der den Zugang zu den Informationen vermittelt, vorzugehen.

Den rechtlichen Werkzeugkasten für einen solchen Anspruch bietet inzwischen die DSGVO. Sie bestimmt nicht nur, wann Daten erhoben und verarbeitet werden dürfen, sondern auch, wann diese Daten wieder gelöscht werden müssen. Der betroffenen Person sichert die Verordnung einen Anspruch auf Löschung seiner Daten zu – mit dem klangvollen Namen „Recht auf Vergessenwerden“.[1] Dieser in Art. 17 DSGVO festgelegte Anspruch fordert von dem Verantwortlichen die unverzügliche Löschung der Daten, wenn einer der dort aufgelisteten Gründe vorliegt. Der häufigste Anlass dürfte dafür sein, dass die Daten nicht mehr für den ursprünglichen Verarbeitungszweck benötigt werden. Darüber hinaus sind Daten insbesondere dann zu löschen, wenn für die Verarbeitung keine Rechtsgrundlage (mehr) besteht. Das ist unter anderem nach Art. 17 Abs. 1 lit. c DSGVO der Fall, wenn gegen deren Verarbeitung ein Widerspruch nach Art. 21 DSGVO eingelegt wurde. Der Widerspruch richtet sich gegen Datenverarbeitungen, die aufgrund des Art. 6 Abs. 1 lit. e oder f DSGVO erhoben wurden. Art. 6 Abs. 1 lit. e DSGVO erlaubt eine Datenverarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Art. 6 Abs. 1 lit. f DSGVO ermöglicht hingegen die Verarbeitung, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen und Rechte des Betroffenen überwiegen. In diese Kategorie fallen auch Datenverarbeitungen durch Suchmaschinenbetreiber. Sie werden in der Regel die Verarbeitung personenbezogener Daten nur auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO stützen können, da sie weder die Einwilligung des Betroffenen einholen, noch vertraglich mit ihm verbunden sind. Gegen eine solche Datenverarbeitung kann immer dann Widerspruch eingelegt werden, wenn die Verarbeitung ursprünglich erlaubt war, aber durch das Hinzutreten besonderer Umstände inzwischen nicht mehr

1 Zum Recht auf Löschung aus Art. 17 DSGVO siehe auch Leinemann, Vergiss mein nicht…, DFN-Infobrief Recht 08/2016.

rechtmäßig ist. Ein solcher Umstand kann unter anderem die Dauer der Speicherung sein. Eine Verarbeitung ist nicht länger rechtmäßig, wenn bei einer Abwägung die Rechte und Interessen des Verantwortlichen oder Dritter hinter den Rechten und Freiheiten des Betroffenen zurückstehen müssen.

Selbst wenn nach Art. 17 Abs. 1 DSGVO die Voraussetzungen für einen Löschungsanspruch vorliegen, muss der Betroffene zudem die Ausnahmen vom Löschungsanspruch in Art. 17 Abs. 3 DSGVO berücksichtigen. Besondere Bedeutung kommt vor allem der ersten Ausnahme zu: Das Recht auf Löschung gilt nicht, soweit die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist. Auch hier muss eine umfassende Abwägung im Einzelfall durchgeführt werden, die allerdings häufig schwerfallen dürfte, da sich eine schematische Lösung verbietet. Erwägungsgrund 153 S. 4 der DSGVO sieht zwar vor, dass die Mitgliedstaaten Gesetze erlassen können, die bei der Abwägung helfen, hiervon hat Deutschland bislang aber keinen Gebrauch gemacht. Hinweise, wie die sich widersprechende Rechtspositionen und Interessenlagen in Ausgleich gebracht werden können, gibt daher allein die Rechtsprechung. Die Frage, wann ein Löschungsanspruch gegenüber einem Suchmaschinenbetreiber durchgesetzt werden kann, ist in der Rechtsprechung keinesfalls neu. Bereits im Jahr 2014 beschäftigte sich der EuGH mit der Frage, ob ein generelles Recht auf Vergessenwerden gegenüber Google geltend gemacht werden könne.[2] Mit dem gleichen Problem beschäftigten sich in drei neueren Verfahren nun sowohl das Bundesverfassungsgericht (BVerfG) als auch der Bundesgerichtshof (BGH).

II. Urteil des BVerfG

Hintergrund des Verfahrens vor dem BVerfG (Beschluss vom 6.11.2019 – 1 BvR 276/17) war ein Interview, in dem die Beschwerdeführerin zur Kündigung einer ihrer Mitarbeiter befragt wurde. Dieses Interview erschien im NDR in der Sendung „Panorama“ als Teil eines Beitrags mit dem Titel „Kündigung: Die fiesen Tricks der Arbeitgeber“. Ein Transkript dieses Interviews wurde zudem auf die Internetseite des Senders geladen. Bei Eingabe des Namens der Beschwerdeführerin in die Suchmaske von Google erschien als eines der ersten Suchergebnisse ein Link zu besagter Website. Die Beschwerdeführerin begehrte von Google die Entfernung des Links. Sie berief sich dabei auf ihr allgemeines Persönlichkeitsrecht sowie ihr Grundrecht auf informationelle Selbstbestimmung.

Das BVerfG schloss sich weitestgehend der Rechtsauffassung der Vorinstanz an. Das namensbezogene Auffinden, Indexieren, vorübergehende Speichern und die Anzeige des Links durch Google stellen danach eine Verarbeitung personenbezogener Daten dar. Gegenüber dieser Verarbeitung könne der Betroffenen ein Löschungsanspruch zustehen. Die von der Beschwerdeführerin geltend gemachten Rechten müssen aber sowohl mit den Grundrechten des Suchmaschinenbetreibers als auch mit betroffenen Rechten Dritter abgewogen werden. Weil mit der DSGVO der Datenschutzstandard innerhalb der EU vereinheitlicht wurde, ging das BVerfG dabei von der alleinigen Anwendbarkeit des Unionsrechts aus und prüfte nur die Verletzung von Unionsgrundrechten. Diese gelten nicht nur im Verhältnis zwischen Staat und Bürgen, sondern finden auch in privatrechtlichen Streitigkeiten Anwendung.

Im Ergebnis hielt das Gericht die Klage jedoch für unbegründet. Zwar kann sich Google bei der Verbreitung von Suchnachweisen nicht auf die eigene Meinungsfreiheit berufen, da es lediglich fremde journalistische Beiträge in den Suchergebnissen anzeigt. Stattdessen muss aber die Meinungsfreiheit des NDR in die Abwägung der verschiedenen Rechtspositionen einbezogen werden. Diese würde durch ein Verbot der Verbreitung des Artikels über die Suchmaschine eingeschränkt. Dennoch ist die Frage nach der Rechtmäßigkeit der Verbreitung durch den Suchmaschinenbetreiber nicht identisch mit der Frage der Rechtmäßigkeit der Veröffentlichung durch den Inhalteanbieter, da durch beide Handlungen unterschiedliche Rechtspositionen betroffen sein können. So sei bei der ersten Frage unter anderem auch die unternehmerische Freiheit des Suchmaschinenbetreibers aus Art. 16 EU-Grundrechtecharta (GrCh) in die Abwägung einzubeziehen.

In der Abwägung berücksichtigten die Richter zudem, dass die Beschwerdeführerin freiwillig das Interview gegeben hatte sowie, dass der Inhalt des Gesprächs ein Thema von allgemeinem Interesse behandelt und nicht nur Informationen über das Privatleben der Beschwerdeführerin enthält. Entscheidend sei im Hinblick auf Art. 17 DSGVO auch, wieviel Zeit zwischen der ursprünglichen Veröffentlichung und dem späteren Nachweis durch die Suchmaschine vergangen sei. Die verstrichene Zeit

2 Siehe hierzu Thinius, Google, du musst mich vergessen!, DFN-Infobrief Recht 07/2014.

betrifft sowohl das Öffentlichkeitsinteresse als auch die Intensität der Grundrechtbeeinträchtigung. Auch wenn das Gericht im konkreten Fall davon ausging, dass weiterhin öffentliches Interesse an dem Artikel besteht, nahm es jedoch gleichfalls an, dass mit weiterem Zeitablauf, das Öffentlichkeitsinteresse hinter dem Löschungsinteresse der Betroffenen zurückstehen könnte und die Verbreitung dadurch unzulässig wird.

Auch wenn das BVerfG nur eine Verletzung der Unionsgrundrechte und nicht die tatbestandlichen Voraussetzungen des Art. 17 DSGVO geprüft hat, lassen sich die Argumente des BVerfG auf die Abwägung in Art. 17 DSGVO weitestgehend übertragen. Das verdeutlichen auch die aktuellen Entscheidungen des BGH, die starke inhaltliche Parallelen aufweisen.

III. Entscheidungen des BGH

In seinen beiden Entscheidungen vom 27. Juli 2020 hat der BGH ebenfalls Stellung zum Recht auf Vergessenwerden und dessen Durchsetzung gegenüber Suchmaschinenbetreibern genommen.[3] Im ersten Verfahren (VI ZR 405/18) sollte Google dazu verpflichtet werden, Presseartikel über den Kläger nicht länger in der Suchanzeige zu listen. Der Kläger war Geschäftsführer des Regionalverbands einer wohltätigen Organisation, der im Jahr 2011 ein Defizit von ca. einer Million Euro aufwies. Kurz zuvor meldete sich der Kläger krank. Über beide Umstände wurde in der Tagespresse berichtet. Diese Artikel wurden zudem in der Google-Suche aufgeführt. Der BGH entschied, dass dem Kläger kein Anspruch aus Art. 17 DSGVO auf Auslistung der Ergebnislinks zustand. Zu dem Ergebnis kam er nach einer umfassenden Abwägung zwischen Grundrechten des Klägers auf der einen Seite und den Grundrechten der Beklagten, den Interessen der Nutzer der Beklagten und der Öffentlichkeit sowie den Grundrechten des Anbieters der Presseartikel auf der anderen Seite. Der Kläger stehe zwar unter dem Schutz des Rechts auf Achtung des Privat- und Familienlebens nach Art. 7 GrCH und des Rechts auf Schutz personenbezogener Daten aus Art. 8 GrCh, müsse sich aber die Meinungsfreiheit des Inhalteanbieters entgegenhalten lassen. Dabei wird kein Vorrang der Schutzinteressen des Klägers pauschal vermutet, sondern beide in Rede stehenden Rechtsgüter stehen sich gleichberechtigt gegenüber. Daraus ergebe sich aber auch, dass der Suchmaschinenbetreiber nicht erst tätig werden muss, wenn er Kenntnis von einer offensichtlichen und auf den ersten Blick erkennbaren Rechtsverletzung erlangt. Davon ist der BGH bislang noch ausgegangen. Noch kurz vor Anwendbarkeit der DSGVO war er der Meinung, dass die Prüfpflichten des Suchmaschinenbetreibers schwächer als die des Hostproviders wären (Urteil vom 27.2.2018 – VI ZR 489/16). Trotz der verschärften Anforderungen, ging in diesem Fall die Abwägung zuungunsten des Klägers aus. Laut BGH überwiege hier die Meinungsfreiheit und die Interessen der anderen Betroffenen, so dass ein Anspruch auf Auslistung nicht besteht.

Auch im zweiten Verfahren (VI ZR 476/18) ging es um Löschungsansprüche gegenüber Google.[4] Ausgang waren auch hier Presseartikel, die auf einer Website über die Kläger veröffentlicht wurden. Beide Kläger sind in Gesellschaften tätig, die Finanzdienstleistungen erbringen. Die Beiträge setzten sich kritisch mit den Anlagemodellen dieser Gesellschaften auseinander und enthielten in einem Artikel auch Fotos der Kläger. Die Websitebetreiber stehen allerdings im Verdacht, Unternehmen zu erpressen, indem sie erst kritische Berichte veröffentlichen und danach gegen Zahlung anbieten, die Artikel zu löschen. Ein solcher Fall lag nach Meinung der Kläger auch hier vor. Sie verlangen, dass Google es unterlässt, die in Rede stehenden Artikel bei einer Namenssuche aufzulisten und ihre Fotos als Thumbnails anzuzeigen.

In diesem Verfahren kam es vorläufig noch zu keinem abschließenden Urteil. Der BGH hat sich hingegen dazu entscheiden, das Verfahren auszusetzen und zwei Fragen dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vorzulegen. Mit der ersten Frage möchte der Gerichtshof wissen, ob bei einer Abwägung der Rechte des Betroffenen mit denen des Suchdienstanbieters und Dritter nach Art. 17 Abs. 3 lit. a DSGVO darauf abgestellt werden kann, dass der Kläger, sofern er Recht hat, zunächst auf andere, zumutbare Art Rechtsschutz gegenüber dem Inhalteanbieter erlangen kann. Hintergrund ist die Behauptung der Kläger, dass die Tatsachenbehauptungen in dem verlinkten Artikel wahrheitswidrig und damit deren Veröffentlichung rechtswidrig seien. Diese Behauptung ließe sich in einem Verfahren gegen den Inhalteanbieter gerichtlich überprüfen. Der Suchmaschinenbetreiber kann dagegen selbst den Wahrheitsgehalt der verlinkten Inhalte nur eingeschränkt

3 Der Volltext der Urteile liegt zum Zeitpunkt der Bearbeitung noch nicht vor.

4 Zu diesem Verfahren bereits Baur, Google weiß, was Du letzten Sommer getan hast, DFN-Infobrief Recht 04/2019.

beurteilen. Mit seiner Frage möchte der BGH daher klären, ob in der Abwägung der widerstreitenden Interessen berücksichtigt werden kann, ob ein solches Vorverfahren stattgefunden hat und ob der Kläger somit von der Möglichkeit, seine Behauptungen gerichtlich überprüfen zu lassen, Gebrauch gemacht hat. Als zweites fragt der BGH, inwiefern der Kontext der ursprünglichen Veröffentlichung innerhalb der Abwägung nach Art. 17 Abs. 3 lit. a DSGVO zu berücksichtigen ist, wenn der Suchdienstanbieter nur ein Vorschaubild mit Link aber nicht den Titel der Website oder anderweitige Informationen der Ursprungsseite nennt. Beide Fragen drehen sich letztlich darum, inwieweit die Suchanzeige und die verlinkte Website rechtlich getrennt voneinander betrachtet werden können.

IV. Fazit und Praxishinweise

Hochschulen und Forschungseinrichtungen sind von den Urteilen zweifach betroffen. Zunächst sind sie selbst datenverarbeitende Stellen. Das Datenmanagement und der Datenschutz sind eine zunehmend komplexe und verantwortungsvolle Aufgabe, welche die Einrichtungen häufig an die Grenze der Belastbarkeit führt. Die Einführung der DSGVO hat diese Situation verschärft, indem sie für weitere Verunsicherung gesorgt hat. Abstrakte und teilweise schwammige Formulierungen sind nicht zuletzt dem großen Anwendungsbereich der DSGVO geschuldet. Es bedarf der Rechtsprechung, um diese Normen und ihre Voraussetzungen näher auszudifferenzieren. Gerade die Abwägung, wann das Recht auf Vergessenwerden Vorrang gegenüber den Interessen Dritter erhält, fällt schwer. Mit den Urteilen ist ein bisschen Licht in die Dunkelheit gekommen. Wird ein Löschungsanspruch geltend gemacht, kann sich die Einrichtung gegebenenfalls auf eine Ausnahme aus Art. 17 Abs. 3 DSGVO berufen. Gerade die Entscheidung, ob die Meinungsfreiheit oder Informationsfreiheit Vorrang gegenüber dem Datenschutz besitzt, kann nur nach einer umfassenden Einzelfallabwägung stattfinden. Dabei muss vor allem berücksichtigt werden, dass die Intensität des Eingriffes in die Persönlichkeitsrechte des Betroffenen mit der Dauer der Speicherung steigt. Relevant dürfte zudem die Ausnahme nach Art. 17 Abs. 3 lit. d DSGVO sein, wonach kein Löschungsanspruch besteht, wenn die Verarbeitung für wissenschaftliche Zwecke erforderlich ist.

Konkreteren Anwendungsbezug haben die Urteile vor allem dann, wenn personenbezogene Daten von Mitgliedern der Hochschulen und Forschungseinrichtungen auf Websites veröffentlicht und über Suchmaschinen verlinkt werden. Möchte die betroffene Person die Veröffentlichung ihrer Daten verhindern oder deren Verbreitung zumindest einschränken, ist ein direktes Vorgehen gegen den Suchmaschinenbetreiber möglich. Er ist selbst Verantwortlicher der von ihm durchgeführten Datenverarbeitung und somit potentieller Anspruchsgegner eines Löschungsanspruchs. Allerdings lässt sich auch mit dem Recht auf Vergessenwerden nicht jede unliebsame Berichterstattung aus dem Weg räumen. Einem Löschungsbegehren kann der Suchmaschinenbetreiber seine eigenen Rechte und Interessen, aber auch die seiner Nutzer, der Öffentlichkeit und des Inhalteanbieters entgegenhalten. Wichtige Fragen werden außerdem noch zukünftig vom EuGH zu klären sein. Dabei geht es insbesondere um die Frage, wie weit der Suchmaschinenbetreiber den Kontext der verlinkten Veröffentlichung zu berücksichtigen hat und ob der Betroffene bei einer rechtswidrigen Veröffentlichung zunächst Rechtsschutz gegenüber dem Betreiber der Website suchen muss.

Auch wenn die DSGVO jedem ein Recht auf Vergessen zusichert, wird die Reichweite des Rechts durch zahlreiche Ausnahmen und die Rechte anderer begrenzt. Wer durch die DSGVO auf mehr Anonymität im Netz hofft, wird durch die aktuelle Rechtsprechung vielleicht enttäuscht sein. Denn eines wird nach den Urteilen des BGH klar: So schnell vergisst das Internet auch zukünftig nicht.

Data Wars: Der Betroffene schlägt zurück

Das Arbeitsgericht Düsseldorf verurteilt Unternehmen zu Schadensersatz gemäß Art. 82 Abs. 1 DSGVO i.H.v. 5.000 Euro

von Nicolas John

Weil sie dem Auskunftsbegehren des ehemaligen Arbeitnehmers zu spät und unvollständig nachgekommen ist, verurteilte das Arbeitsgericht (ArbG) Düsseldorf in seiner Entscheidung (Urteil vom 5.3.2020, Az. 9 Ca 6557/18) die beklagte Arbeitgeberin zur Zahlung eines immateriellen Schadensersatzes in Höhe von 5.000 Euro. Im Zentrum der Entscheidung stand die Frage, wie weit der Begriff des Schadens auszulegen ist und ob hohe immaterielle Schadensersatzansprüche durch Art. 82 DSGVO der Verordnung zur effektiven Durchsetzung verhelfen.

I. Hintergrund

Art. 82 Datenschutz-Grundverordnung (DSVGO) sieht für betroffene Personen einen Anspruch auf materiellen und immateriellen Schadensersatz vor, wenn vom Verantwortlichen oder vom Auftragsverarbeiter gegen die Vorschriften der DSGVO verstoßen wird. Dabei kann jeder Verstoß gegen die DSGVO eine Schadensersatzpflicht begründen, insbesondere auch Verstöße gegen die Informations- und Auskunftspflichten aus Art. 12 ff. DSGVO. Diese Pflichten sehen vor, dass die betroffene Person über die Datenverarbeitungen zu informieren ist und sie erfahren kann, ob und welche personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO vom Verantwortlichen für welche Zwecke auf welche Weise verarbeitet werden.

Die im Urteil des ArbG Düsseldorf thematisierte Auskunftspflicht der Beklagten aus Art. 15 DSGVO gibt in einem detaillierten Katalog vor, in welchem Umfang die Auskunft zu erfolgen hat. Zudem ist dabei stets die Monatsfrist des Art. 12 Abs. 3 DSGVO für die Auskunftserteilung vom Verantwortlichen zu beachten.

II. Sachverhalt

Der Kläger war bei der Beklagten bis Januar 2018 zu einem Gehalt von nahezu 12.000 Euro brutto/Monat beschäftigt. Während des Beschäftigungsverhältnisses übersandte die Beklagte personenbezogene Daten des Klägers zumindest an zwei andere Unternehmen. Im Juni 2018 verlangte der Kläger schriftlich Auskunft über die ihn betreffenden personenbezogenen Daten gemäß Art. 15 Abs. 1 DSGVO und forderte Kopien hierüber an. Die Beklagte kam diesem Verlangen nicht nach, weshalb der Kläger das Begehren im November 2018 klageweise geltend machte. Daraufhin übermittelte die Beklagte dem Kläger im Dezember 2018 Unterlagen mit Informationen über die Verarbeitung seiner personenbezogenen Daten mitsamt einem Passwort für eine Online-Ressource, welches dem Kläger ermöglichen sollte, weitere personenbezogene Daten abzurufen. Doch erwies sich diese Auskunft als unvollständig und der Kläger erhielt eine vollständige Auskunft erst Monate später.

Der Kläger sah in diesem Sachverhalt sein Recht auf Erteilung einer vollständigen und fristgemäßen Auskunft über seine personenbezogenen Daten aus Art. 15 DSGVO verletzt und verlangte daher eine Entschädigung in Höhe von zwölf Bruttomonatsgehältern, also insgesamt 143.482,80 Euro.

III. Entscheidung des ArbG Düsseldorf

Das ArbG Düsseldorf gab dem Kläger im Grunde Recht und verurteilte die Beklagte zur Zahlung eines Schadensersatzes in Höhe von 5.000 Euro.

Das Arbeitsgericht stellte zunächst fest, dass die Beklagte den Vorgaben des Art. 15 Abs. 1 DSGVO nicht ausreichend nachgekommen sei. Eine Auskunftserteilung müsse in präziser, transparenter, verständlicher, leicht zugänglicher Form und in einer klaren und einfachen Sprache erfolgen. Maßgeblicher Datenbestand der Auskunftserteilung sei jener, welcher im Zeitpunkt des Auskunftsersuchens vorliege. Über ein Löschen dürfe sich der Verantwortliche nicht der Pflicht entziehen, jedoch müsse er auch nicht über Daten Auskunft erteilen, über welche er zum Zeitpunkt des Auskunftsverlangens nicht mehr verfüge. Die Angaben der Zwecke müssten zudem vollständig und so konkret sein, sodass sich die betroffene Person ein Bild davon machen könne, welche Datenverarbeitungen zu welchen Zwecken erfolgt seien. Dies sei mit der erfolgten Auskunft nicht der Fall gewesen. Die Beklagte sei ihrer Pflicht nicht ausreichend nachgekommen, indem sie in der Auskunft erklärt, „dass die Datenverarbeitung zum Zwecke des Beschäftigungsverhältnisses, namentlich zu dessen Abwicklung und Beendigung, zur Erfüllung bestehender rechtlicher Verpflichtungen und zur Wahrnehmung berechtigter Interessen“ erfolge. Damit gebe die Beklagte nach der Ansicht des Gerichts lediglich „pauschal und fast die ganze Bandbreite im Privatrechtsverkehr naheliegender Zwecke“ an, ohne konkrete Absichten zu nennen.

Darüber hinaus stellt das Gericht klar, dass die Pflicht der Beklagten nicht das Durchsuchen sämtlicher Server, Datenbanken, Web-Anwendungen, E-Mail-Postfächer, usw. umfasse, da dies im groben Missverhältnis zu dem Leistungsinteresse des Klägers stünde. Nach dem anwendbaren Grundsatz von Treu und Glauben gemäß Art. 8 Abs. 2 S. 1 Charta der Grundrechte der Europäischen Union (GRCh) dürfe dem Verantwortlichen kein unverhältnismäßiger Aufwand abverlangt werden. Nach Auffassung des Arbeitsgerichts besteht ein Anspruch auf Schadensersatz in Höhe von 5.000 Euro. Die Voraussetzungen des Art. 82 Abs. 1 DSGVO seien schon durch die nicht fristgerechte sowie unvollständige Beantwortung des Auskunftsantrages erfüllt. Durch die unvollständige Auskunftserteilung werde das zentrale Betroffenenrecht der DSGVO sowie das europäische Grundrecht aus Art. 8 Abs. 2 S. 2 GRCh, welches das Auskunftsrecht ausdrücklich gewährleiste, beeinträchtigt. Hierdurch werde dem Kläger die Kontrolle über seine personenbezogenen Daten erschwert und dieser im Ungewissen gelassen. Der Kläger habe daher einen immateriellen Schaden erlitten.

Mangels entsprechender Darlegung könne die Haftung der Beklagten auch nicht im Sinne des Art. 82 Abs. 3 DSGVO entfallen. Nach diesem Artikel kann sich der Verantwortliche oder der Auftragsverarbeiter von der Haftung befreien, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Zudem sei nach Ansicht des Gerichts die Schwere des immateriellen Schadens für die Begründung des Anspruchs irrelevant, dies wirke sich lediglich bei der Höhe des Anspruchs aus. Damit verneint das Gericht die Erforderlichkeit einer Bagatellgrenze. Zur Anspruchshöhe führt das Gericht aus, dass die Höhe der Vergütung des Klägers bei der Bemessung des Schadens keine Rolle spiele, wohl aber Kriterien wie Art, Schwere, Dauer des Verstoßes, Grad des Verschuldens, frühere einschlägige Verstöße sowie Kategorien der betroffenen Daten. Zudem müssen Verstöße nach der Auffassung des ArbG Düsseldorf effektiv sanktioniert werden, um der DSGVO zur Wirkung zu verhelfen. Die hierfür erforderliche abschreckende Wirkung des Schadensersatzes werde daher durch die Einbeziehung der Finanzkraft des Verantwortlichen in die Festsetzungserwägungen zur Anspruchshöhe erreicht.

IV. Fazit und Konsequenzen für die Hochschulpraxis

Das ArbG Düsseldorf setzt mit seinem Urteil die unionsrechtlichen Vorgaben aus der DSGVO folgerichtig um. Zwar mag die Begründung der Kammer mit dem Argument der Abschreckung zur Schadenshöhe zunächst überraschen, da das deutsche Schadensersatzrecht eine solche Art des „Strafschadensersatzes“ nicht kennt. Im Gegenteil zu Art. 83 Abs. 1 DSGVO, welcher die abschreckende Wirkung von Bußgeldern von Aufsichtsbehörden vorsieht, erwähnt der Wortlaut des Art. 82 DSGVO die abschreckende Wirkung des Schadensersatzes allerdings nicht ausdrücklich. Jedoch sehen neben dem ArbG Düsseldorf auch Teile der juristischen Literatur die Erforderlichkeit der abschreckenden Wirkung als gegeben an. So verlangt Erwägungsgrund 146 DSGVO, dass der Begriff des Schadens „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden [soll], die den Zielen dieser Verordnung in vollem Umfang entspricht“. Außerdem sollen „die betroffenen Personen […] einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten“. Im Kontext von Art. 4 Abs. 3 EUV argumentiert daher neben dem

Arbeitsgericht auch die Literatur, dass die Mitgliedsstaaten – und damit auch die entscheidende Kammer – angehalten sind, Verstöße wirksam zu sanktionieren. Für ebendiese Wirksamkeit der Sanktion sei daher die abschreckende Wirkung des Schadensersatzes erforderlich und insbesondere durch die Höhe zu erreichen.

An dieser Stelle bleibt abzuwarten, wie die nächste Instanz, das Landesarbeitsgericht (LAG) Düsseldorf, entscheiden wird, bei welchem die Berufung gegen das arbeitsgerichtliche Urteil nun anhängig ist. Auch mehren sich Stimmen gegen eine solche extensive Auslegung des Art. 82 DSGVO. Das abschließende Wort ist damit in dieser Sache noch nicht gesprochen und eine Korrektur insbesondere hinsichtlich der Höhe des Schadensersatzes erscheint weiterhin möglich.

Dennoch zeigt das Urteil eindrucksvoll, welche Konsequenzen sich auch aus kleinsten Verstößen gegen die DSGVO ergeben können. Da das Arbeitsgericht eine Bagatellgrenze beim Schaden dem Grunde nach nicht annimmt, kann jeder Datenschutzverstoß zu einer Schadensersatzpflicht führen. Um sich nicht schadensersatzpflichtig zu machen, haben auch Hochschulen und Forschungseinrichtungen bei der Verarbeitung personenbezogener Daten stets darauf zu achten, die Auskunftsbegehren von betroffenen Personen vollständig und fristgerecht zu erteilen. Aus diesem Grund sollten standardisierte Abläufe im Falle von Auskunftsverlangen eingerichtet sein, um keine Verschleppung der Sache herbeizuführen und die Monatsfrist zu verpassen. Der Umfang wird dabei je nach Einzelfall zu bestimmen sein. Eine Verweigerung der Auskunft wird in der Regel nicht verhältnismäßig sein.[1]

1 Siehe hierzu John, Mein Name ist Hase, ich weiß von nichts, DFN-Infobrief Recht 6/2020.

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