EINFÜHRUNGSBEITRÄGE UND CHECKLISTEN

WiJ-Interview

Rechtsanwalt Tim Wybitul, Frankfurt a.M.,
Dr. Markus Wünschelbaum, Hamburg, und
Rechtsanwalt Dr. Arne Klaas, Berlin

E-Mail-Auswertung bei internen Ermittlungen
Alles im Fluss? Fernmeldegeheimnis, Rechtsgrundlagen, Betroffenenrechte

Die E-Mail an die eigenen Kinder, der schnelle Nachrichtencheck oder den Frisörtermin online vereinbaren: die private Nutzung des Internets am Arbeitsplatz und des dienstlichen E-Mail-Accounts ist in vielen Unternehmen gelebte Praxis. Und für die Durchführung von internen Untersuchungen durchaus folgenreich: die deutschen Datenschutzaufsichtsbehörden stellten sich lange Zeit auf den Standpunkt, dass die Erlaubnis zur Privatnutzung den Arbeitgeber an das Fernmeldegeheimnis aus § 88 TKG a.F. (nun: § 3 TDDDG) bindet. Dabei bedarf es keiner expliziten Erlaubnis im Arbeitsvertrag oder einer Betriebsvereinbarung. Bereits das Tolerieren der Privatnutzung soll nach einer teilweise vertretenen Ansicht als betriebliche Übung den Arbeitgeber auf das Fernmeldegeheimnis verpflichten können. Die Konsequenz: die Auswertung der auch privat genutzten E-Mail-Postfächer soll nicht in den Anwendungsbereich der DSGVO und des BDSG fallen, sondern sich nach dem TDDDG richten. Danach wäre die Auswertung nicht oder nur unter sehr engen Grenzen möglich. Aber: ist das wirklich so?

Dr. Arne Klaas hat Tim Wybitul, RA bei Latham & Watkins LLP, und Dr. Markus Wünschelbaum, Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit[1], zum Gespräch eingeladen.

AK: Wir beginnen unser heutiges Gespräch mit einer kleinen Revolution aus Nordrhein-Westfalen. Im aktuellen Tätigkeitsbericht kehrt die Landesbeauftragte für Datenschutz und Informationsfreiheit von der bisher einheitlich vertretenen Position[2] der Aufsichtsbehörden ab: Das Fernmeldegeheimnis gelte nicht für Arbeitgeber.[3] Lass uns daher gleich mit Dir beginnen, lieber Markus. Wie ist die E-Mail-Auswertung durch Arbeitgeber mit § 3 TDDDG und § 206 StGB vereinbar? Ist das Fernmeldegeheimnis überhaupt auf Arbeitgeber anwendbar?

MW: In der Tat kommt etwas Bewegung in diesen ewigen Streit darum, ob Arbeitgeber zumindest teilweise Telekommunikationsdienste „geschäftsmäßig" anbieten. Die LDI NRW hat diese These damit begründet, dass es Arbeitgebern bei der erlaubten oder geduldeten Privatnutzung am Rechtsbindungswillen fehle: Sie treten gegenüber ihren Beschäftigten nicht als geschäftsmäßige Telekommunikationsdienstleister auf und wollen nicht, dass die für diese Dienstleister geltenden Rechtsnormen auf sie angewendet werden.

Diese Wende aus NRW begrüße ich vor allem auch, weil sich ein Abschied vom Fernmeldegeheimnis für Arbeitgeber als deutsche Sonderlocke harmonisch in das Unionsrechtsregime einfügt: Wenn wir uns die betriebliche Kommunikation ansehen, sei es per E-Mail oder Instant-Messaging, haben wir es fast immer mit personenbezogenen Daten zu tun. Mitarbeiter tauschen sich unter ihren echten Namen über ihre Aufgaben und Kollegen aus. Für solche Daten gilt vorrangig die DSGVO.

Nun kommt aber das TDDDG ins Spiel, genauer gesagt § 3 Abs. 3 TDDDG. Der verbietet dem Arbeitgeber als Dienstanbieter quasi jede Kenntnisnahme von Kommunikationsinhalten, es sei denn, es ist technisch notwendig. Ein solches Datenverarbeitungsverbot steht aber im Konflikt mit der DSGVO – es schließt die Verarbeitung aufgrund berechtigter Interessen nach Art. 6 Abs. 1 Satz 1 lit. f) DSGVO pauschal aus; solche Vorgaben hat der EuGH in der Vergangenheit bereits kassiert.

Der einzige Ausweg wären hier die Öffnungsklauseln aus Art. 88, 95 DSGVO. Doch die greifen nicht. Pauschale Datenverarbeitungsverbote sind von Art. 88 DSGVO nicht abgedeckt. Die Öffnungsklausel aus Art. 95 DSGVO für Regelungen der e-Privacy-RL kann man ebenfalls nicht fruchtbar machen; sie bezieht sich nur auf öffentlich zugängliche Dienste – dass betriebsinterne Kommunikation überhaupt vom Fernmeldegeheimnis erfasst sein könnte ist das Ergebnis einer überschießenden Umsetzung in Deutschland. Soweit reicht aber die Öffnungsklausel nicht. Was bedeutet das nun in der Praxis? Im Ergebnis muss man davon ausgehen, dass der Anwendungsvorrang der DSGVO gegenüber dem TDDDG-Fernmeldegeheimnis wirkt, wenn es um Arbeitgeber geht. Das heißt, der Zugriff auf Kommunikationsinhalte richtet sich nach den Regeln der DSGVO. Damit ist auch eine Strafbarkeit nach § 206 StGB ausgeschlossen – wenn eine Datenverarbeitung unional zulässig ist, gebietet der effet utile, dass dies nicht tatbestandsmäßig „unbefugt" ist.

AK: Tim, wie bewertest du diese Entwicklung aus NRW?

[1] Der Beitrag wurde nicht in dienstlicher Eigenschaft verfasst und gibt ausschließlich persönliche Auffassungen des Autoren wieder.
[2] Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz („Orientierungshilfe"), abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf (zuletzt abgerufen 17. August 2024).
[3] LDI NRW, 29. Tätigkeitsbericht 2024, S. 76 f.

TW: Ebenso wie Markus sehe ich diese Positionierung aus Nordrhein-Westfalen positiv. Meines Erachtens haben die deutschen Datenschutzbehörden hier in der Vergangenheit ohnehin eine fragwürdige Rechtsposition bezogen, die sich auf eine Argumentation stützte, die ich rechtlich schwer nachvollziehbar fand. Insofern wäre eine gesamtheitliche Abkehr der Behörden von dieser Position begrüßenswert. Soweit sind wir mit dieser einzelnen Behördenmeinung aus Nordrhein-Westfalen natürlich noch nicht. Aber sie bietet Anlass, eine auch in Bezug auf die von Markus genannten europarechtlichen Positionen fragwürdige Rechtsauffassung auf den Prüfstand zu stellen.

Auch wenn dies eine positive Entwicklung ist, würde ich sie aber nicht als kleine Revolution bezeichnen. Wir reden hier über Behördenmeinungen, die erst einmal vor Gericht Bestand haben müssten. Und deutsche Gerichte standen der genannten Rechtsauffassung der Behörden nach meiner Wahrnehmung bereits in der Vergangenheit ganz überwiegend sehr kritisch gegenüber. Mir persönlich ist – mit Ausnahme des jedoch etwas anders gelagerten Falls des OLG Karlsruhe vor bald 20 Jahren[4] – nicht ein einziger Fall bekannt, in dem ein Arbeitgeber oder seine Vertreter deswegen von der Staatsanwaltschaft angeklagt oder gar von einem Strafgericht wegen Verletzung des Fernmeldegeheimnisses verurteilt worden wären, weil sie auf betriebliche E-Mail-Kommunikation ihrer Mitarbeiter zugegriffen hätten. In diesem viel zitierten Beschluss des OLG Karlsruhe ging es um eine Universität, die Zugänge nicht nur für Beschäftigte, sondern auch für Studierende, Lehrbeauftragte, Externe und sonstige Dritte angeboten hatte.

Inhaltlich teile ich Markus Argumente. Zudem fallen mir noch einige weitere Argumente gegen die Einordnung des Arbeitgebers als Anbieter von Telekommunikationsdiensten gegenüber seinen Beschäftigten ein. Die habe ich aber schon so häufig in Veröffentlichungen aufgeschrieben, dass ich uns diese Wiederholung hier erspare.

AK: Hat dieses Verständnis Auswirkungen darauf, wer für die Aufsicht über die Auswertung von auch privat genutzten E-Mail-Postfächern zuständig ist?

MW: Grundsätzlich ist für die Einhaltung des Fernmeldegeheimnisses nur eine Datenschutzaufsichtsbehörde zuständig – die BfDI. Das begründet sich mit dem eigentlichen Adressaten des Fernmeldegeheimnisses: große Telekommunikationsdienstleister die bundesweit einheitlich ihre Dienstleistungen anbieten. Wenn das Fernmeldegeheimnis für Arbeitgeber nicht gelten würde, fiele diese Zuständigkeit weg und die Landesdatenschutzaufsichtsbehörden würden im Rahmen ihrer DSGVO-Zuständigkeit tätig. Auch hieran lässt sich übrigens erkennen, dass der Arbeitgeber als Diensteanbieter ein Fremdkörper in der TK-Regulierung darstellt: Die Auswertung privat genutzter E-Mails findet innerhalb des Unternehmens statt und betrifft die Mitarbeiter vor Ort. Die Auswirkungen sind somit auf lokaler Ebene spürbar – sei es in Bezug auf die Arbeitsbedingungen, das Betriebsklima oder mögliche arbeitsrechtliche Konsequenzen. Warum sollte die Auswertung von E-Mails im Gegensatz zu den sonstigen Beschäftigtendaten auf einem Dienstrechner auf einmal von einer anderen Behörde beaufsichtigt werden? Die Lösung ist für mich deshalb auch von der Governance-Struktur her sinnvoll: Die BfDI bleibt zuständig für die Aufsicht über die „echten" geschäftsmäßigen Telekommunikationsanbieter, während die Landesbehörden – wie auch sonst – die Überwachung von Mitarbeitern mittels datenverarbeitender Systeme regulieren, auch bei der Auswertung privat genutzter E-Mail-Postfächer. Die bisherige Lösung droht, einheitliche Lebenssachverhalte auseinanderzureißen.

AK: Sind damit der Auswertung von E-Mail-Postfächern jetzt keine Grenzen mehr gesetzt? Was muss – auch nach einer Abkehr vom betrieblichen Fernmeldegeheimnis – beachtet werden?

TW: Nein. Man kann nicht davon sprechen, dass es jetzt hier keine Grenzen gäbe. Ganz im Gegenteil. Die DSGVO stellt eine ganze Reihe strenger Anforderungen an die Auswertung von E-Mail-Postfächern auf, etwa im Rahmen interner Untersuchungen, aber auch in anderen Zusammenhängen.

Zunächst einmal muss sich jede Durchsicht des E-Mail-Postfachs auf einen Erlaubnistatbestand stützen. Bei der Auswahl der in Frage kommenden Rechtsgrundlagen kommt es darauf an, welche Art von Fehlverhalten im Raum steht. Hier müssen wir differenzieren zwischen Straftaten, Ordnungswidrigkeiten und bloß rechts- oder vertragswidrigem Verhalten. Daneben kommt es darauf an, welche Rolle der Postfachinhaber spielt: wird er verdächtigt oder ist er ein potentieller Zeuge?

Während bei Verdacht auf Straftaten § 26 Abs. 1 Satz 2 BDSG als spezielle Rechtsgrundlage in Frage kommt, müssen wir bei weniger schwerwiegenden Verstößen und bei potentiellen Zeugen auf Art. 6 Abs. 1 Satz 1 lit. b) oder f) DSGVO zurückgreifen. § 26 Abs. 1 Satz 1 BDSG wurde durch den EuGH faktisch zur Makulatur erklärt.[5] Hier die BAG-Rechtsprechung auf die unionale Ebene zu übertragen kann vorschnell sein – Stand jetzt fehlt uns im Beschäftigtenkontext hinreichend konkrete EuGH-Rechtsprechung, um die Grenzen von Art. 6 Abs. 1 Satz 1 lit. b) DSGVO aufzuzeigen. Gleichzeitig ist es schwierig, im Vorfeld von Aufklärungsmaßnahmen zu erkennen, ob schlussendlich eine grobe Pflichtverletzung, eine Ordnungswidrigkeit oder eine Straftat nach § 26 Abs. 1 Satz 2 BDSG vorliegen wird.

Dabei muss immer auch im Blick behalten werden, ob sich besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO im Postfach befinden. In diesen Fällen kommen Verarbeitungen etwa auf der Grundlage von Art. 9 Abs. 2 lit. f) DSGVO in Betracht.

[4] OLG Karlsruhe, Beschluss vom 10.1.2005 - 1 Ws 152/04 .
[5] EuGH, NZA 2023, 487 (491 Rn. 81).

Gerade bei (auch) privat genutzten E-Mail-Postfächern sind mit Blick auf den Erforderlichkeitsgrundsatz entsprechende Vorkehrungen und Regelungen zu treffen, damit den Beschäftigten klar und transparent kommuniziert wird, mit welchen Verarbeitungen personenbezogener Daten ihrer betrieblichen Emails sie rechnen müssen. Bewährt hat sich in der Praxis bspw. das klare Verbot der privaten Nutzung betrieblicher Kommunikationssysteme. Hier sind entsprechende interne Nutzungsregeln und entsprechende Datenschutzhinweise nach Art. 13, 14 DSGVO wichtig. Letztere sollten auch darauf hinweisen, dass Unternehmen gehalten sind, Indizien für interne Regelverstöße aufzuklären. Viele unserer Mandanten verwenden entsprechende Datenschutzerklärungen, die spezifisch die Themen Compliance- und Aufsichtsmaßnahmen, interne Ermittlungen und Hinweisgebersysteme abdecken. Das kann auch in arbeitsrechtlicher Hinsicht sehr sinnvoll sein, weil Beschäftigte dann kaum argumentieren, dass sie mit zuvor kommunizierten Überwachungsmaßnahmen nicht rechnen mussten, wenn sie hierüber zuvor transparent informiert wurden. Und natürlich schließt eine solche allgemeine Datenschutzinformation eine konkrete, anlassbezogene Unterrichtung im Einzelfall nicht aus.

AK: Welche Maßnahmen empfehlt ihr beide, wenn ein Unternehmen seinen Mitarbeitern die Privatnutzung – zumindest in einem angemessenen Rahmen – ermöglichen möchte?

MW: Auf jeden Fall darf die IT-Policy nicht nur für die Schublade geschrieben werden, sondern sollte/muss den Mitarbeitern als wirksame Richtlinie dienen. Deshalb sollte sie den Umfang der Privatnutzung genau definieren und durch griffige Beispiele anschaulich machen. Genauso präzise sollte beschrieben werden, welche Nutzungen diesen Rahmen überschreiten. Auf technischer Ebene können zudem ähnliche Lösungen wie in gemeinsamen Ordnerstrukturen implementiert werden, indem separate private Ordner zur Abtrennung solcher Nachrichten angelegt werden.

TW: Das stimmt.

AK: Apropos – das Eingrenzen des zu untersuchenden E-Mail-Datenbestands ist ja auch unter dem Grundsatz der Datenminimierung geboten. Markus, gibt es hier eine sinnvolle Richtschnur, an der sich Unternehmen orientieren können?

MW: Klar – zunächst einmal klingen Datenminimierung und das Ziel einer umfassenden Aufklärung wie ein Widerspruch. Aber hier kann Compliance-Management und Ermittlungseffizienz Hand in Hand gehen. Ein guter Ansatz ist eine Negativabgrenzung ex ante. Das bedeutet, das Unternehmen definiert im Vorfeld, welche Bereiche oder Arten von E-Mails für die Untersuchung nicht relevant sein werden. Gleichzeitig sollten wir klar zwischen „nice to know" und „need to know" unterscheiden. Nur die Informationen, die wirklich notwendig sind, um den fraglichen Sachverhalt aufzuklären, sollten in den Umfang der Auswertung fallen.

Hier kommt die Einbindung von Fachabteilungen ins Spiel. Statt alle E-Mails der gesamten Abteilung zu durchsuchen, können relevante Schlüsselpersonen, Zeiträume und Suchbegriffe die Auswertung von Anfang an eingrenzen.

Um dieses Dilemma in der Praxis zu lösen, sollte stufenweise vorgegangen werden: Man beginnt die Untersuchung auf Basis von Art. 6 Abs. 1 Satz 1 lit. b) oder f) DSGVO mit einem eng begrenzten Umfang. Wenn die erste, eng begrenzte Untersuchung keine Erkenntnisse liefert, aber der ursprüngliche Verdacht weiterhin besteht, kann eine vorsichtige Ausweitung des Suchumfangs denkbar sein, etwa durch Einbeziehung eines größeren Zeitraums oder weiterer potenziell relevanter Personen. Wichtig ist, dass dieser Prozess transparent gestaltet wird und klare Abbruchkriterien definiert sind, um eine unangemessene Ausweitung der Untersuchung zu verhindern. Sollten sich im Laufe der Ermittlungen keine konkreten Anhaltspunkte für eine Straftat ergeben, kann nicht trotzdem unter Berufung auf § 26 Abs. 1 Satz 2 BDSG weiter gemacht werden.

AK: Tim, ist das in der Praxis umsetzbar? Wie gehst du damit um, dass Sachverhalt und einschlägige Rechtsgrundlage zu Beginn der Ermittlung häufig schwer zu fassen sind?

TW: Man muss halt mit dem Sachverhalt arbeiten, den man hat. Diesen Sachverhalt muss man ordentlich analysieren und dokumentieren. Auf dieser Basis prüft man die in Betracht kommenden Rechtsgrundlagen und entscheidet sich für die entsprechenden Maßnahmen und sonstigen Schritte. Wenn sich der Sachverhalt ändert – und das tut er sehr häufig im Rahmen laufender Untersuchungen – ändert sich oft auch die datenschutzrechtliche Bewertung. Daher ist eine interne Untersuchung in aller Regel ein sehr dynamischer Prozess, der vielen Veränderungen unterworfen ist. Datenschutzrechtlich ist das eine durchaus komplexe Aufgabe, bei der man viele Fehler machen kann. Solche Fehler lassen sich durch eine gründliche Planung und ein präzises rechtliches Vorgehen in der Praxis vermeiden.

AK: Tim, Du hast es gerade bereits angerissen: Transparenzpflichten. Grundsätzlich sind alle betroffenen Personen vor der Auswertung des E-Mail-Postfachs nach Art. 13, 14 DSGVO zu informieren. Das können mitunter ganz schön viele Stakeholder sein – man denke bspw. an ausufernde .cc-Adresszeilen mit einer Vielzahl an Externen. Tim, wie sieht ein gutes Informationskonzept aus? Und wie können sich Unternehmen bereits im Vorfeld gut aufstellen?

TW: Wie bereits angesprochen, sollten Unternehmen im Idealfall bereits im Vorfeld – und damit etwa bei der erstmaligen Erhebung – bereits entsprechende Zwecke antizipieren und darüber informieren. Damit vermeiden sie im Ernstfall auch das Risiko einer möglichen zweckändernden Verarbeitung, die ihrerseits wieder gesonderte Informationspflichten auslösen kann, Art. 13 Abs. 3 DSGVO und Art. 14 Abs. 4 DSGVO.

AK: Aus der Praxis wissen wir, dass nicht immer jeder mögliche Zweck antizipiert werden kann. Vor diesem Hintergrund besteht ein gewisses Bedürfnis auf abstraktere Zweckumschreibungen zuzugreifen. Die DSGVO fordert jedoch die Festlegung „eindeutiger" Zwecke. Markus, ist Dir der Zugriff auf das E-Mail-Postfach zur „Gewährleistung der Unternehmensintegrität" eindeutig genug? Und wenn nein: wie machen Unternehmen es besser?

MW: Die Formulierung „Gewährleistung der Unternehmensintegrität" bei einem konkreten Zugriff auf ein E-Mail-Postfach finde ich zu uneindeutig. Die Formulierung unterscheidet sich kaum von allgemeinen Datenschutzhinweisen bzgl. Aufsichtsmaßnahmen, Compliance und Hinweisgebersystemen wie Tim sie dargestellt hat. Da kann man Unternehmen schon mehr abverlangen, ohne dass sie an Flexibilität einbüßen oder das Ermittlungsziel gefährden. Denkbar wäre etwa, dass eine Kategorie aus den allgemeinen Datenschutzhinweisen aufgegriffen und beispielhaft konkretisiert wird. So könnte man den Zugriff zur Aufdeckung von Compliance-Verstoßen benennen und erklären, dass unter den Begriff der Compliance beispielsweise Datenschutzverletzungen oder Korruptionsvorwürfe fallen. Klar ist aber auch, dass selbst solche informatorischen Aussagen im Einzelfall eine Warnwirkung beinhalten können. Am Ende wird es auf eine ordentliche Dokumentation der Ermittlung ankommen, um die Entscheidungen über die Zwecke und den Umfang der Informationen nachvollziehbar darstellen zu können.

AK: Guter Punkt. Je nach Untersuchungsgegenstand und -situation kann einer vorherigen Information von betroffenen Personen eine unerwünschte Warnwirkung zukommen. Muss der Untersuchungsführer in jedem Fall informieren oder kommen ggf. auch Ausnahmetatbestände in Betracht?

TW: Ob in der jeweiligen Situation eine gesonderte Unterrichtung geboten ist, ist stets eine Frage des Einzelfalles. Allein schon aufgrund der unklaren Definition der Zwecke in der DSGVO und der Frage, ob eine der in der DSGVO oder im BDSG geregelten Ausnahmen von der Unterrichtungspflicht vorliegt. In jedem Fall ist darauf zu achten, ob die personenbezogenen Daten direkt bei der betroffenen Person oder aber bei Dritten erhoben wurden. Für beide Erhebungsmöglichkeiten kommen unterschiedliche Ausnahmetatbestände in Betracht. Drohen bspw. „Verdunklungsmaßnahmen" durch Dritte kann eine Information gem. § 29 Abs. 1 Satz 1 BDSG unterbleiben. Wie auch sonst bei datenschutzrechtlichen Vorgängen – und insbesondere bei internen Untersuchungen – muss man hier bei der datenschutzrechtlichen Bewertung präzise und gründlich arbeiten und dokumentieren. Denn gerade bei internen Untersuchungen gibt es ja eine erhebliche Wahrscheinlichkeit, dass die vom Unternehmen ergriffenen Maßnahmen später einmal durch eine Behörde bzw. ein Gericht überprüft werden.

AK: Gehen wir mal einen Schritt weiter: Wie sollte man mit Betroffenenrechten während einer laufenden internen Ermittlung umgehen, insbesondere mit dem im betrieblichen Kontext beliebten Auskunftsrecht?

MW: Der EuGH hat in den letzten Jahren den Auskunftsanspruch kontinuierlich gestärkt und ausgeweitet. Das Grundprinzip dabei ist, dass alles von der Auskunft erfasst sein muss, was für die betroffene Person unerlässlich ist, um ihre Rechte wirksam ausüben zu können.

Besonders relevant für interne Ermittlungen ist hier der S-Pannki Fall. In diesem Fall hat der EuGH die Ausnahme vom Auskunftsrecht zum Schutz der Rechte Dritter sehr eng ausgelegt. Ein ehemaliger Bankmitarbeiter wollte wissen, welche Mitarbeiter auf sein Konto zugegriffen hatten, weil er unrechtmäßige Zugriffe vermutete. Der EuGH gab ihm Recht und argumentierte, dass diese Information unerlässlich sei, um zu beurteilen, ob die Zugriffe im Rahmen eines Berechtigungskonzepts rechtmäßig erfolgten.

Übertragen wir das auf interne Ermittlungen, bedeutet dies, dass wir nach Abschluss der Ermittlungen von sehr umfassenden Auskunftsrechten ausgehen müssen. Die betroffene Person hat ein Recht darauf zu erfahren, wer auf ihre Daten zugegriffen hat und warum, sofern das Ermittlungsergebnis dadurch nicht gefährdet wird.

Während laufender Ermittlungen sehe ich jedoch gute Argumente dafür, den Auskunftsanspruch insoweit einzuschränken, wie er sich auf aktuelle Ermittlungsgegenstände bezieht. Dies dient dem Schutz der Integrität der Untersuchung.

Ein weiterer interessanter Aspekt aus dem EuGH-Urteil ist, dass der Umfang des Auskunftsanspruchs durch die Begründung des Antragstellers erweitert oder präzisiert werden kann. Je konkreter die Anfrage und je detaillierter die Befürchtungen oder Zwecke dargelegt werden, desto tiefgehender kann die Auskunft ausfallen. Dies bedeutet zwar keine Konkretisierungspflicht für den Betroffenen, eröffnet aber die Möglichkeit für einen differenzierteren Dialog.

Gerade im betrieblichen Kontext ist das Risiko eines Auskunftsanspruchs bei einer denkbaren Änderung des Arbeitsverhältnisses absehbar. Wenn man dieses Risiko ernst nimmt, muss schon am Anfang der internen Ermittlung ein Prozess feststehen, der es erlaubt, die Erfüllung von etwaigen Auskunftsansprüchen zu ermöglichen, Zugriffe bei der E-Mail-Auswertung sorgfältig zu dokumentieren und abzuwägen, welche Informationen ohne Gefährdung der Untersuchung offengelegt werden können. Nach Abschluss der Ermittlungen sollte dann eine möglichst umfassende Auskunft erteilt werden.

AK: Wie verstehst Du die Rechtsprechung des EuGH dazu, Tim?

TW: Die Übertragung der Rechtsprechung des EuGH in die betriebliche Realität der Unternehmen ist oft eine erhebliche Herausforderung. Letztlich entscheidet der EuGH anhand

von Einzelfällen über die Auslegung europarechtlicher Normen. Zu mehr ist er nach Art. 267 AEUV in Vorlageverfahren auch gar nicht befugt. Daher werden die Entscheidungen des EuGH in solchen Verfahren häufig auch stark durch die entsprechenden Vorlagebeschlüsse der nationalen Gerichte geprägt. Dies führt häufig dazu, dass sich Wertungen und Aussagen des EuGH zu einem Sachverhalt nur schwer auf andere Sachverhalte übertragen lassen. Insgesamt würde ich mir gerade im Datenschutz häufig ein mehr an der Praxis orientiertes Vorgehen des höchsten europäischen Gerichts wünschen. Das wäre ja auch aus europarechtlicher Sicht im Hinblick auf den Verhältnismäßigkeitsgrundsatz geboten. Insofern würde ich mich sehr freuen, wenn der EuGH beim Auslegen der DSGVO und andere europarechtlicher Vorgaben einmal etwas mehr auf die Frage der tatsächlichen Umsetzbarkeit blicken würde. Wirklich optimistisch bin ich hier aber für die kommenden Jahre nicht.

Wo wir aber gerade bei dem Thema sind – ich glaube, dass es auch im Sinne des Datenschutzes viel zweckmäßiger wäre, wenn Datenschutzbehörden, nationale Gerichte und EuGH die DSGVO auf eine Art und Weise auslegen, dass Unternehmen und sonstige datenschutzrechtlich Verantwortliche dies in der Praxis auch gut umsetzen können. Wenn ein Unternehmen dann nicht bereit ist, die Anforderungen der DSGVO in einer solchen praxisorientierten Auslegung umzusetzen, sollte es auch mit einiger Wahrscheinlichkeit mit konkreten Sanktionen rechnen müssen. Derzeit habe ich häufig eher den Eindruck, dass aufgrund überzogener Auslegungen der unklaren Vorgaben der DSGVO oft schwer umsetzbare Anforderungen aufgestellt werden, die aber in der Praxis kaum ein Unternehmen einmal umsetzt. Das führt dann zu einer wenig flächendeckenden Umsetzung datenschutzrechtlicher Vorgaben und zu einer eher zufallsbezogenen Ahndung von Einzelfällen.

Was die konkrete Auslegung der Vorgaben der DSGVO angeht, kann ich gerne einige Beispiele liefern. Beispielsweise wäre sehr zweckmäßig, Daten nur dann als personenbezogen zu bewerten (und sie damit den umfassenden Anforderungen der DSGVO zu unterstellen), wenn tatsächlich eine realistische Möglichkeit besteht, dass diese Daten einzelnen Person zugeordnet werden können. Diese Frage spielt gerade bei internen Untersuchungen in der Praxis häufig eine entscheidende Rolle. Aber auch für die Entwicklung und den Einsatz von künstlicher Intelligenz. Die Hamburger Behörde hat hierzu kürzlich eine sehr durchdachte und lesenswerte Stellungnahme veröffentlicht.

Ein anderes gutes Beispiel für eine überzogene Auslegung der DSGVO ist das datenschutzrechtliche Auskunftsrecht. Hier wäre es meines Erachtens zweckmäßig, sich an den in Art. 15 Abs. 1 lit. a) bis lit. h) DSGVO genannten Vorgaben zu orientieren und nicht über die ansonsten recht schwammige Formulierung dieser Vorschrift ein all umfassendes Auskunftsrecht zu schaffen.

AK: Ganz herzlichen Dank Euch Beiden für das aufschlussreiche Gespräch.

WiJ-Checklisten

Rechtsanwalt Tim Wybitul, Frankfurt a.M.,
Dr. Markus Wünschelbaum, Hamburg, und
Rechtsanwalt Dr. Arne Klaas, Berlin

Checkliste für E-Mail-Auswertungen bei internen Ermittlungen

1. Ermittlungsumfang definieren

- Konkreten Verdacht dokumentieren
- Ermittlungsziel präzise formulieren
- Zeitraum und Inhalte der zu untersuchenden E-Mails festlegen
- Betroffene Personen/Abteilungen identifizieren und Rolle definieren

2. Rechtsgrundlagen prüfen

- Privatnutzung erlaubt oder geduldet? Gründe für (Un-)Beachtlichkeit des Fernmeldegeheimnisses dokumentieren (§ 3 TDDDG, § 206 StGB)
- Datenschutzrechtliche Rechtsgrundlagen identifizieren (§ 26 Abs. 1 Satz 2, Abs. 3 BDSG, Art. 6, 9 DSGVO), Betriebsvereinbarungen, IT-Policies
- Unterscheidung zwischen Straftaten, OWis und Vertragsverletzungen beachten
- Prüfung der Notwendigkeit einer DSFA

3. Verarbeitungszwecke prüfen und ggf. festlegen

- Zu welchen Zwecken wurden die in den Postfächern gespeicherten pD erhoben?