Handlungsempfehlung zur Öffnung von E-Mail-Accounts und Benutzerkonten

Inhalt

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung (EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.
Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.
Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

A. Zusammenfassung

Vielfach besteht das Bedürfnis für Hochschulen und Forschungseinrichtungen, auf Daten ihrer Mitarbeiter oder der Nutzer ihrer Kommunikationsinfrastruktur zugreifen zu können. Die Gründe können dabei unterschiedlichster Natur sein. Vom wichtigen Dokument im E-Mail-Account, das wegen eines Krankheitsfalles nicht vom Mitarbeiter selbst zur Verfügung gestellt werden kann, bis hin zur Optimierung des Gesamtsystems in Bezug auf Störungsfälle bieten sich verschiedenste Anlässe. Die folgende Handlungsempfehlung soll dazu dienen, die möglichen rechtlichen Risiken bei einem solchen Vorgehen aufzuzeigen und sich der rechtlichen „Stolperfallen“ bewusst zu werden.

Dazu wird zum einen zwischen den Mitarbeitern der Hochschule und den Nutzern des Kommunikationsnetzes und zum anderen zwischen den verschiedenen Situationen und den einzelnen, dabei potentiell betroffenen Rechtspositionen unterschieden.

Wenn ein *Mitarbeiter* nicht mehr ansprechbar oder sogar verstorben ist, stellt sich die Frage, ob Vorgesetzte oder Mitarbeiter Einsicht in seine E-Mails oder sein Benutzerkonto nehmen dürfen. Lebt der Mitarbeiter noch bzw. ist nur kurzfristig erkrankt und liegen die E-Mails noch auf einem zentralen Server, unterliegen sie dem Fernmeldegeheimnis nach Art. 10 GG. Neben dem Fernmeldegeheimnis gilt es auch datenschutzrechtliche Aspekte zu beachten. Dies wird gerade beim, grundsätzlich nicht vom Fernmeldegeheimnis erfassten, Benutzerkonto relevant. Die Möglichkeit der Einsichtnahme kann indes nur für dienstliche Sachverhalte, deren Kenntnis zwingend erforderlich ist, um die Aufgaben der Hochschule fortzuführen (z. B. Verwaltung, Durchführung von Lehrveranstaltungen, Prüfungen etc.) bestehen. Stets sind die Interessen der Hochschule mit denen des Mitarbeiters abzuwägen und nach Möglichkeit in Einklang zu bringen. Die Erlaubnis von Privatnutzung kann im Übrigen von bestimmten Voraussetzungen und der Einwilligung in stichprobenartige Kontrollen abhängig gemacht werden. Im Zuge solcher Kontrollen ist es von großer Bedeutung, transparent zu handeln. Jedem Mitarbeiter sollten die Voraussetzungen und das mögliche Ausmaß der Kontrollen erkennbar sein. Ist der Mitarbeiter verstorben, so sind zwar das Fernmeldegeheimnis des Verstorbenen und das Datenschutzrecht für ihn nicht mehr relevant, dennoch gilt es, das postmortale Persönlichkeitsrecht zu beachten. Ob und inwieweit ein Zugriff erleichtert möglich ist, hängt dabei vom Einzelfall ab.

Für den Zugriff auf E-Mail-Account oder Benutzerkonto von *Nutzern (insb. Studierende)*, die nicht erreichbar oder verstorben sind, zeichnet sich ein vergleichbares Bild.

Bei jedweder Situation einer Einsichtnahme sollte stets der Datenschutzbeauftragte der Hochschule hinzugezogen und ein Protokoll über das konkrete Vorgehen angefertigt werden. Eine präventive Auseinandersetzung mit den sich ergebenden Problemen von fehlender Erreichbarkeit bzw. Versterben von Mitarbeitern oder Nutzern ist zu empfehlen.

Seinen Mitarbeitern zu erlauben, ihren dienstlichen Anschluss auch in geregelten Maßen privat zu nutzen, ermöglicht es dem Arbeitgeber festzulegen, welche Art von Nutzung genau gestattet ist. Insbesondere kann im Rahmen dieser Regelung festgelegt werden, dass private Mails auch als solche zu kennzeichnen sind. Daneben sollte ausdrücklich klargestellt werden, dass jede Form der ordnungswidrigen und strafbaren Nutzung untersagt ist. Gerade bei Arbeitnehmern könnte insofern individualvertraglich vereinbart werden, dass im Falle der Unerreichbarkeit oder des Versterbens eine Einsicht durch den Arbeitgeber erfolgen darf. Diese Vereinbarung bedarf der Schriftform und einer ausdrücklichen Regelung. Es gilt festgehalten, unter welchen genauen Voraussetzungen eine angemessene Einsichtnahme erfolgen darf. Es ist anzuraten, die Einwilligung im Rahmen einer, vom Arbeitsvertrag unabhängigen, Vereinbarung einzuholen. Darüber hinaus sollte die Einsichtnahme auf die explizit konkretisierten Fälle beschränkt werden. Die Erlaubnis zur (eingeschränkten) Privatnutzung kann von der Einwilligung abhängig gemacht werden, denn es besteht keine Pflicht zur Einräumung der Nutzungsmöglichkeit durch den Arbeitgeber. Grundsätzlich sollte vor der Einsichtnahme des Arbeitgebers, auch wenn eine Einwilligung und deren Voraussetzungen vorliegen, immer der betriebliche Datenschutzbeauftragte und etwaige Rechtsrat hinzugezogen werden.

B. Rechtliche Bewertung

Im Folgenden wird die rechtliche Ausgangslage, die bei einer Einsichtnahme in E-Mail-Accounts und Benutzerkonten besteht, dargestellt. Dazu wird zwischen Mitarbeitern auf der einen, und Nutzern auf der anderen Seite differenziert.

I. Mitarbeiter

Wie sich eine solche Einsichtnahme in Bezug auf die Mitarbeiter der Hochschule auswirkt, ist, je nach Sachlage, unterschiedlich. Es wird zwischen dem Fall der fehlenden Ansprechbarkeit und dem Versterben des Mitarbeiters differenziert.

1. Mitarbeiter nicht ansprechbar

Für den Fall, dass der Mitarbeiter, in dessen Konten Einsicht genommen werden soll, nicht ansprechbar ist, ergibt sich folgendes Bild:

a) E-Mail-Account

Besteht die Absicht in den E-Mail-Account eines Mitarbeiters, der für eine etwaige Rückfrage nicht erreichbar/ansprechbar ist, Einsicht zu nehmen, sind verschiedene rechtliche Aspekte zu beachten.

aa) Fernmeldegeheimnis, Art. 10 GG

In Bezug auf die Nutzung von E-Mail-Diensten kann das in Art. 10 Grundgesetz (GG) verankerte Fernmeldegeheimnis einschlägig sein. Die Hochschule hat als Arbeitgeberin das Fernmeldegeheimnis zu beachten, wenn sie ihren Mitarbeitern die Nutzung dienstlicher TK-Ressourcen zu privaten Zwecken erlaubt. Sie wird damit zum Diensteanbieter i.S.d. TKG und hat dieser Pflicht gem. § 88 Abs. 2 TKG nachzukommen. Damit ist sich dem immer noch überwiegenden Teil der Literatur und insbesondere unverändert den Landesdatenschutzbeauftragten anzuschließen (https://www.datenschutz-mv.de/datenschutz/publikationen/informat/internet/oh-internet-arbeitsplatz.pdf).[1]
Der Schutz des Fernmeldegeheimnisses erstreckt sich dabei auf die Vertraulichkeit der ausgetauschten Informationen und soll vor allem den Kommunikationsinhalt vor unbefugter Kenntniserlangung durch Dritte bewahren. Dadurch wird vermieden, dass der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen unterbleibt, weil die Beteiligten damit rechnen müssen, dass sich staatliche Stellen (oder der TK-Diensteanbieter) in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder -inhalte gewinnen. Maßgeblich für das Bestehen des Schutzes ist der andauernde Kommunikationsvorgang, denn die Beteiligten sollen weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwesenden stünden. Für E-Mail-Konten ist insbesondere relevant, mit welchen Verfahren operiert wird. Der Schutz des Fernmeldegeheimnisses endet grundsätzlich in dem Augenblick, in dem die Nachricht beim Empfänger angekommen und der Übertragungsvorgang abgeschlossen ist. Soweit die Kommunikationsteilnehmer von E-Mails Kenntnis nehmen, diese aber dann weiter auf dem Mailserver eines Providers gespeichert bleiben, bleibt das Fernmeldegeheimnis jedoch einschlägig. Dieser Fall ist vom Schutzbereich des Fernmeldegeheimnisses erfasst, da die spezifische Gefährdungslage und der Zweck dieser Freiheitsverbürgung weiter bestehen. Durch die Endspeicherung wird der Kommunikationsinhalt auf einem vom Provider bereit gestellten Speicherplatz und damit in einer Sphäre abgelegt, die von den Kommunikationsteilnehmern nicht beherrschbar ist (BVerfG). Gerade bei der Nutzung von IMAP ist zu beachten, dass eine Speicherung auf dem Server des Providers (hier meist das Rechenzentrum der Hochschule) bestehen bleibt.

Bei der Öffnung/Einsichtnahme in den E-Mail-Account eines Mitarbeiters, dem die Privatnutzung von Internet und E-Mail erlaubt ist, hat die Hochschule damit die Anforderungen des Fernmeldegeheimnisses zu beachten. Die Anforderungen an eine Rechtfertigung einer solchen Einsichtnahme orientieren sich grundsätzlich an den §§ 88 Abs. 3 S. 3 TKG und kann nur unter den dort genannten Voraussetzungen erfolgen.

– Eingriffshandlung –

Öffnet die Hochschule das E-Mail-Konto des Mitarbeiters und nimmt Einsicht, so stellt dies einen unmittelbaren Eingriff in das Fernmeldegeheimnis dar. Das erhöhte Schutzbedürfnis des Betroffenen ergibt sich aus dem Umstand, dass er auf den Kommunikationsanbieter zur Umsetzung des Kommunikationsvorgangs angewiesen ist. Für den Anbieter besteht eine erleichterte Zugriffsmöglichkeit auf die Kommunikationsinhalte, weil er den Übertragungsvorgang beherrscht.

[1] Dieser Ansicht folgend stellt die Erlaubnis der Privatnutzung ein „Angebot an Dritte“ gem. § 3 Nr. 10 TKG dar.

Vor dieser erleichterten Zugriffsmöglichkeit eines Dritten, die sich aus der fehlenden Beherrschbarkeit des Übertragungsvorgangs ergibt, ist der Betroffene indes zu schützen.
Im Arbeitsverhältnis bestehen noch weitergehende Möglichkeiten des Zugriffs.

Kennzeichnend für Arbeitsverhältnisse ist das faktische Ungleichgewicht der Parteien. In der Situation des Arbeitgebers als TK-Diensteanbieter ergibt sich eine erleichterte Zugriffsmöglichkeit einerseits aus der TK-Leistung (also der Übertragung). Andererseits hat er aber auch noch die Möglichkeit, direkt mithilfe von Administratorenrechten über den Desktop-PC des Arbeitnehmers Einsicht zu nehmen und so auf Kommunikationsvorgänge zuzugreifen. Der Arbeitgeber hat damit eine doppelte Machtstellung. Auch diese zweite Zugriffsmöglichkeit unterliegt dem Schutz des Fernmeldegeheimnisses, obwohl hierbei nicht unmittelbar die überlegene Position als TK-Dienstleister ausgenutzt wird, denn ist der Arbeitgeber als Diensteanbieter zur Beachtung des Fernmeldegeheimnisses verpflichtet, dann darf er dies nicht umgehen können, indem er eine weitere, sich aus dem Ungleichgewicht der Parteien ergebende Möglichkeit des Zugriffs nutzt, obwohl die Informationen nach dem Willen des Gesetzgebers geschützt sein sollen. Im Ergebnis wäre es widersprüchlich, wenn der Arbeitgeber sich durch seine besonders beherrschende Stellung nicht nach § 88 TKG an das Fernmeldegeheimnis halten müsste, nur weil für ihn die Möglichkeit besteht, auch anderweitig Zugriff auf den Kommunikationsinhalt zu erlangen. Sinn von Art. 10 GG ist der Schutz des Fernmeldegeheimnisses und dieser Schutz darf nicht umgangen werden.

- Grundrechtsverzicht der Beteiligten –

Erklären alle an der Kommunikation Beteiligten ihr Einverständnis mit der Kenntnisnahme der Kommunikation, liegt kein Eingriff in das Fernmeldegeheimnis vor. Ein Einverständnis nur einzelner Kommunikationsteilnehmer reicht jedoch nicht aus, da diese nicht über die kommunikative Selbstbestimmung anderer Kommunikationsteilnehmer verfügen können. Der Gebrauch einer beruflichen E-Mail-Adresse respektive die Versendung an eine solche wird nicht zugleich als Verzicht auf den Grundrechtsschutz gewertet werden können. Gerade unter dem Aspekt, dass viele Arbeitgeber ihren Mitarbeitern bewusst erlauben, ihren E-Mail-Account auch zu privaten Zwecken zu nutzen, wird der bloße Versand an eine solche E-Mail-Adresse in der Regel nicht ausreichend sein, um darin einen konkludenten Verzicht auf den Schutz des Kommunikationsinhaltes zu sehen. Denn dass der Arbeitgeber definitiv die E-Mails kontrolliert, muss dem Nutzenden und dem Versendenden nicht klar sein. Entsprechend fehlt ihnen das Bewusstsein, auf ihren Grundrechtsschutz zu verzichten. Das bloße Bewusstsein, dass der Arbeitgeber auf die Kommunikation zugreifen könnte, ersetzt auch in diesem Verhältnis keinen bewussten Verzicht auf den Schutz des Fernmeldegeheimnisses.

- Rechtfertigung –

Auch ohne Einverständnis der Kommunikationsteilnehmer kann eine Rechtfertigung für einen Eingriff in das Fernmeldegeheimnis bestehen. Diese bedarf allerdings einer einfach-gesetzlichen Regelung, die den Eingriff gestattet und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht, § 88 Abs. 3 S. 3 TKG.

Eine solche Norm existiert für die Öffnung/Einsichtnahme in E-Mail-Accounts nicht. In Extremfällen, wenn die Aufrechterhaltung des Betriebs gefährdet ist und die Interessen des Arbeitgebers stark

überwiegen, könnte möglicherweise eine Rechtfertigung aus kollidierendem Verfassungsrecht (sog. verfassungsimmanente Schranke), namentlich durch das grundrechtlich in Art. 14 GG geschützte Eigentum, in Betracht kommen.

Ob eine solche Rechtfertigung möglich ist, ist in Rechtsprechung und Fachliteratur bis dato ungeklärt und daher mit entsprechender Rechtsunsicherheit verbunden.

Art. 14 GG würde hier sowohl das Eigentum an den genutzten Ressourcen (Computer) selbst, als auch die Gesamtheit des eingerichteten und ausgeübten Gewerbebetriebs betreffen. Diese Rechte umfassen zum Beispiel die Regelung der Verwendung von Arbeitsmitteln wie Telefon, Computer und Internetzugang für private Zwecke.
Welche Anforderungen genau erfüllt sein müssen, damit in diesen Fällen die Öffnung des dienstlichen E-Mail-Accounts zulässig wäre, ist höchstrichterlich bisher nicht entschieden. Klar bleibt lediglich, dass es immer einer Abwägung des Interesses des Arbeitgebers am ungestörten Arbeitsablauf (Art. 14 GG) mit dem Interesse des Arbeitnehmers am Unterbleiben des Zugriffs bedarf. Die Interessen des Arbeitnehmers am Schutz seiner Kommunikation sind im Falle einer Einsichtnahme stets und umfassend zu berücksichtigen. Es sollte mehrfach und nachweislich versucht werden, den Arbeitnehmer telefonisch zu erreichen, um dessen Einverständnis einzuholen. Vor dem eigentlichen Zugriff sind der ggf. vorhandene Betriebs-/Personalrat sowie der Datenschutzbeauftragte zu informieren, so dass die Möglichkeit der Hinzuziehung einer Vertrauensperson seitens des Arbeitnehmers besteht. Die Öffnung des Postfachs sollte dem Arbeitnehmer in jedem Fall rechtzeitig vorher angekündigt werden. Die konkrete Einsichtnahme in die einzelnen E-Mails selbst hat sich ausschließlich auf dienstliche E-Mails zu beschränken. Die Vertrauensperson/der Datenschutzbeauftragte sollte eine derartige Differenzierung anhand des Absenders und der (eindeutigen) Betreffzeile vornehmen, wobei im Zweifel von einem privaten Charakter und unterbleibender inhaltlicher Durchsicht auszugehen ist. Nicht zuletzt sollte stets ein entsprechendes Protokoll zur Beweissicherung und Gedächtnisstütze für ein etwaig nachfolgendes Gerichtsverfahren angefertigt werden.

bb) Datenschutzrecht

Neben dem Fernmeldegeheimnis ist in jedem Fall der besondere Schutz personenbezogener Daten zu beachten. Da die E-Mail zumindest Informationen über Sender und Empfänger enthält, sind personenbezogene Daten (vgl. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)) gegeben. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG).

Der Regelungsrahmen ergibt sich aus den §§ 91 ff. TKG, soweit das Fernmeldegeheimnis einschlägig ist und im Übrigen aus den jeweiligen Landesdatenschutzgesetzen (exemplarisch erfolgt die Darstellung anhand des LDSG NRW – entsprechende Regelungen finden sich indes auch in den Datenschutzgesetzen der anderen Bundesländer). Für die Anwendbarkeit der Vorschriften des jeweils einschlägigen Landesdatenschutzgesetzes ist danach zu differenzieren, ob Privatnutzung erlaubt ist oder nicht.

Hochschulen sind bei Gestattung oder qualifizierter Duldung privater Nutzung als Diensteanbieter nach dem TKG anzusehen (s.o.). In diesem Fall sind im Rahmen einer Einsichtnahme in den E-Mail-Account des Mitarbeiters aus datenschutzrechtlicher Sicht die Anforderungen der §§ 91 ff. TKG zu beachten.

Ist eine Nutzung zu privaten Zwecken untersagt oder ist das Fernmeldegeheimnis aus sachlicher Sicht nicht einschlägig, greifen für die Hochschulen die Vorschriften des Landesdatenschutzgesetzes ein. Personenbezogene Daten dürfen nur mit der Einwilligung des Betroffenen erhoben werden. Ohne eine Einwilligung ist die Erhebung nur gestattet, wenn diese durch eine gesetzliche Regelung erlaubt wird. Indes kann die Einwilligung nur ausdrücklich erklärt werden. Mutmaßliche Einwilligungen des Nutzers reichen nicht aus.
Für die Erhebung personenbezogener Daten sind die §§ 12 Abs. 1, 13 Abs. 2 Datenschutzgesetz NRW gesetzliche Erlaubnisnormen. Voraussetzung einer zulässigen Datenerhebung ist, dass sie zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Dem Grundsatz der Datensparsamkeit folgend ist diese Vorschrift eng auszulegen. Insofern ist die Erforderlichkeit erst dann gegeben, wenn alle anderen Wege, insbesondere die Kontaktierung des Mitarbeiters, ausgeschöpft sind. Die Erforderlichkeit ist (nach Ausschöpfung der Möglichkeiten) z.B. gegeben, wenn es ohne die Kenntnis nicht möglich ist, wichtige Lehrveranstaltungen oder Forschungsvorhaben durchzuführen. Eben dann kann für den Zugriff auf den E-Mail-Account eine datenschutzrechtliche Rechtfertigung durch die o.g. Vorschriften gegeben sein.

Indes ist eine Abwägung im konkreten Einzelfall grundlegende Voraussetzung eines jeden Zugriffs. Darin ist zu prüfen, ob die Durchführung des Vorhabens Vorrang vor dem Recht auf informationelle Selbstbestimmung des betroffenen Mitarbeiters hat. Daher muss der Vorgesetzte oder Mitarbeiter die Relevanz der Einsichtnahme für die Realisierung der jeweiligen Aufgabenerfüllung detailliert darlegen. Insbesondere sollte stets versucht werden, die Anwesenheit einer entsprechenden Vertrauensperson (des Betroffenen) zu ermöglichen.

Ist also die private Nutzung nicht gestattet (und damit das Fernmeldegeheimnis nicht zu beachten) und ist es im Einzelfall für die Erfüllung der jeweiligen Aufgaben erforderlich, so könnte grundsätzlich eine solche Einsichtnahme in E-Mail-Accounts von Mitarbeitern erfolgen. Dennoch sind bei der Einsichtnahme nur die geschäftlichen E-Mails zu öffnen. Sollten sich also, entgegen der arbeitsrechtlichen Anweisung, private E-Mails im E-Mail-Account befinden, so ist deren Öffnung nicht gestattet. Wird der E-Mail-Account unberechtigterweise geöffnet, können sich Schadensersatzansprüche des Betroffenen aus § 20 Abs. 1 DSG NRW ergeben.

cc) Arbeitsrecht

Bei der Einsichtnahme in E-Mail-Accounts von Mitarbeitern sind schließlich noch arbeitsrechtliche Aspekte zu beachten. Aus dem Arbeitsverhältnis ergeben sich gegenseitige Schutz- bzw. Nebenpflichten mit der Folge, dass auf die Interessen und Rechtsgüter des anderen Teils Rücksicht zu nehmen ist. Diese Pflicht könnte durch rechtswidrige Einsichtnahme in E-Mail-Accounts verletzt werden. Dies könnte dann sowohl Beseitigungs- und Unterlassungsansprüche als auch Schadensersatzansprüche nach sich ziehen.

b) Benutzerkonto

Benutzerkonten sind zum einen durch Zugriffsrechte auf Daten und (Sub-) Systeme gekennzeichnet, zum anderen bieten sie die Möglichkeit, persönliche (Stamm- und Bewegungs-) Daten, sowie Konfigurationseinstellungen des jeweiligen Nutzers zu speichern.

Bei Zugriff auf Benutzerkonten wird mangels bestehender Kommunikation in der Regel das Fernmeldegeheimnis nicht betroffen sein. Damit entfällt bei Einsichtnahme in ein Benutzerkonto grundsätzlich Art. 10 GG als Maßstab einer rechtlichen Bewertung. Ebenso werden im Regelfall die §§ 91 ff. TKG nicht zur Anwendung kommen. Anders sieht dies aus, wenn zum einen die Eigenschaft als Diensteanbieter zu bejahen ist und zum anderen die Daten, die im Benutzerkonto einsehbar sind, einen Telekommunikationsbezug i.S.v. § 91 Abs. 1 S. 1 TKG aufweisen.

Im Übrigen ist aber auf die oben gemachten Ausführungen zu verweisen. Insbesondere sind damit regelmäßig die datenschutzrechtlichen Maßstäbe des jeweiligen Landesdatenschutzgesetzes zu beachten.

Es ist neben der Erforderlichkeit zur Erfüllung der Aufgaben auch notwendig, dass die im spezifischen Einzelfall betroffenen Interessen gegeneinander abgewogen werden. Gerade im Rahmen dieser Verhältnismäßigkeitsprüfung bzgl. des Vorgehens bei der konkreten Einsichtnahme können sich spezifische (ggf. auch erhöhte) Maßstäbe für ein rechtmäßiges Verhalten ergeben.

Es ist insofern stets zu empfehlen, bei der Öffnung des Benutzerkontos zu versuchen, die Anwesenheit einer Vertrauensperson zu ermöglichen, um eine Heimlichkeit der Maßnahme zu verhindern, zumindest jedoch den betrieblichen Datenschutzbeauftragten hinzuzuziehen und eine entsprechend detaillierte Dokumentation des Vorgangs anzufertigen.

2. Mitarbeiter verstorben

Sollen Konten von verstorbenen Mitarbeitern eingesehen werden, ergeben sich einige Besonderheiten im Vergleich zu nicht ansprechbaren Mitarbeitern, da die Rechtsordnung für Verstorbene ein geringeres Schutzniveau vorsieht.

a) E-Mail-Account

Auch hier ist zwischen dem E-Mail-Account und dem Benutzerkonto zu differenzieren.

aa) Fernmeldegeheimnis

Die Einsichtnahme in E-Mail-Konten unterliegt unter dem Gesichtspunkt des persönlichen Schutzbereichs auch dann dem Schutz des Fernmeldegeheimnisses, wenn einer der Beteiligten verstorben ist. Ist die Hochschule als Diensteanbieter i.S.d. TKG zu qualifizieren (s.o.) und ist der Kommunikationsvorgang noch nicht abgeschlossen, so greift das Fernmeldegeheimnis auch aus sachlicher Sicht ein (s.o.). Obwohl ein verstorbener Mitarbeiter nicht dem persönlichen

Schutzbereich des Fernmeldegeheimnisses unterfällt, ist auch in diesem Fall das Fernmeldegeheimnis zu beachten. Grundrechtsfähig sind natürliche Personen. Mit dem Tod eines Menschen endet dessen Grundrechtsfähigkeit (BVerfG). Bei Kommunikationsvorgängen sind dagegen Besonderheiten zu beachten. Jede natürliche Person, die an einer privaten Fernkommunikation beteiligt ist, kann sich auf den Schutz des Grundrechts aus Art. 10 GG berufen, so der (Ab-)Sender und Anrufer wie auch der Empfänger und Angerufene. Insofern ist der Schutzanspruch des Kommunikationspartners zu beachten. Damit ist das Fernmeldegeheimnis durch die Hochschule bzw. den Arbeitgeber zu beachten, auch wenn der Verstorbene selbst nicht mehr den Schutz des Fernmeldegeheimnisses genießt.

bb) Datenschutzrecht

Anstelle des Datenschutzrechts ist als Maßstab eines Zugriffs außerhalb des Fernmeldegeheimnisses das Postmortale Persönlichkeitsrecht zu beachten. Wenn und soweit schon unter den Voraussetzungen der Datenschutzgesetze auf Daten des (lebenden) Betroffenen zugegriffen werden darf, so gilt dies erst recht, wenn nur der schwächere Schutz des postmortalen Persönlichkeitsrechts besteht. Wie im Fall des nicht ansprechbaren Mitarbeiters ist damit auch beim verstorbenen Mitarbeiter für die rechtliche Bewertung entscheidend, ob das Fernmeldegeheimnis und damit die §§ 91 ff. TKG eingreifen, soweit Daten mit Telekommunikationsbezug vorliegen.

Ist dies nicht der Fall, so ergeben sich aus datenschutzrechtlichen Aspekten Besonderheiten.

Ziel des Datenschutzrechts ist es, den Zugriff auf personenbezogene Daten zu reglementieren. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG). Geschützt sind aber nach herrschender Meinung in der Rechtswissenschaft nur die Daten lebender Personen, sodass die Datenschutzgesetze auf Daten Verstorbener nicht anwendbar sind. Stattdessen ist hier das sogenannte postmortale Persönlichkeitsrecht zu beachten, welches im Wesentlichen eine Interessenabwägung erfordert.

Für die Einsichtnahme in E-Mail-Accounts folgt daraus, dass ein Zugriff in bestimmten Fällen möglich sein muss.

Dennoch ist ein unbegrenzter Zugriff nicht möglich. Da auch in diesen Fällen das postmortale Persönlichkeitsrecht betroffen sein kann, hat eine Abwägung der widerstreitenden Interessen zu erfolgen. Dabei können im Einzelfall geringere Anforderungen an die Erforderlichkeitsschwelle zu stellen sein. Ein Zugriff auf dienstliche E-Mails sollte insoweit, unter den o.g. Voraussetzungen, möglich sein.

cc) Arbeitsrecht

Die Erben treten in die Rechtsposition des Erblassers ein. Dies umfasst auch Vertragsverhältnisse.

Das Arbeitsverhältnis endet jedoch regelmäßig mit dem Tod des Arbeitnehmers, da die geschuldete Arbeitsleistung nach § 613 Satz 1 BGB im Zweifel in eigener Person zu erbringen ist. Arbeitsrechtliche Aspekte sind insoweit nicht mehr zu beachten.

b) Benutzerkonto

Im Rahmen der Einsichtnahme in Benutzerkonten greift das Fernmeldegeheimnis regelmäßig (und unabhängig von dem Versterben des Nutzers) nicht ein (s.o.).

Bzgl. des Datenschutzrechts gelten die zum E-Mail-Account gemachten Ausführungen, auf die auch im Übrigen zu verweisen ist.

3. Einwilligung des Mitarbeiters in die Einsichtnahme

a) Fernmeldegeheimnis

Für einen Verzicht auf den grundrechtlich gewährleisteten Schutz des Art. 10 GG ist es, wie oben beschrieben, erforderlich, dass beide Kommunikationsteilnehmer diesen gegenüber dem Zugreifenden erklären. Bei der Einwilligung des Arbeitnehmers wäre dies nicht der Fall. Anzumerken bleibt jedoch, dass das Fernmeldegeheimnis keinem der Gesprächspartner verwehrt, auf seiner Seite, auch ohne Einverständnis des Partners, einen Dritten in den Kommunikationsvorgang einzubeziehen und ihn aktiv oder auch passiv daran teilhaben zu lassen. Dies folgt daraus, dass das Fernmeldegeheimnis zwischen den Kommunikationspartnern nicht gilt. Es begründet in ihrem Verhältnis zueinander keine Ansprüche auf Vertraulichkeit oder Geheimhaltung und schützt damit keinen Beteiligten vor Handlungen, mit denen der andere den sonst geschlossenen Bereich ihrer Kommunikation öffnet. Art. 10 Abs. 1 GG schützt nur die Vertraulichkeit des zur Nachrichtenübermittlung eingesetzten Übertragungsmediums. Dieser Gewährleistungsbereich wird aber nicht beeinträchtigt, wenn ein Gesprächspartner in seinem Einfluss- und Verantwortungsbereich einem Dritten den Zugriff auf die Telekommunikationseinrichtung, hier durch normale Einsichtnahme in den E-Mail-Account ermöglicht. Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg (z.B. durch Eingabe von Benutzernamen und Passwort), so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist.

Ein Eingriff in Art. 10 Abs. 1 GG ist zu verneinen, wenn z.B. ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung gestellt hat und die Behörde in der Folge diesen Zugang nutzt (BVerfG - Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07). Diese Situation entspricht der Einsichtnahme in den E-Mail-Account unter Nutzung des Passworts des Mitarbeiters mit dessen Zustimmung. Darin verwirklicht sich nicht die spezifische Gefährdungslage, die aus der Abhängigkeit von technischen Kommunikationsdienstleisternfolgt, sondern das immer gegebene zwischenmenschliche Risiko, dass das personengebundene Vertrauen in den Kommunikationspartner enttäuscht wird. In dieser Konstellation besteht bereits kein Eingriff in das Fernmeldegeheimnis der Kommunikationsteilnehmer, sodass es auf eine Rechtfertigung nicht ankommt.

b) Datenschutzrecht

Unter datenschutzrechtlichen Aspekten sind die Anforderungen an eine Einwilligung zuletzt durch das Bundesarbeitsgericht weiter konkretisiert worden. Demnach ist eine freiwillige Einwilligung im Arbeitsverhältnis möglich und zulässig. Sie muss jedoch schriftlich erfolgen, anlassbezogen sein und Umstände und Ausmaß der geplanten Einsichtnahme aufzeigen. Darüber hinaus sollte eine solche Einwilligung nicht zusammen mit anderen Erklärungen erteilt werden. Der Arbeitnehmer muss sich „frei entscheiden“ können und darf nicht durch Druck oder Zwang zur Abgabe von Erklärungen gedrängt werden. Besteht für ihn die Möglichkeit, diese „freie Entscheidung“ treffen zu können, so steht der Freiwilligkeit und damit letztendlich einer Einwilligung nicht die grundlegende Tatsache einer abhängigen Beschäftigung oder das Weisungsrecht des Arbeitgebers (§ 106 GewO) entgegen. Insgesamt sollte Wert darauf gelegt werden, einen möglichst hohen Grad an Transparenz bzgl. etwaiger Kontrollen zu erreichen. Im Einzelfall kann es auch sinnvoll oder erforderlich sein, den Betriebs- oder Personalrat bei der Ausarbeitung der Voraussetzungen mit einzubeziehen.

II. Studierende

Die rechtliche Bewertung ändert sich, wenn in die Konten eines Studierenden als Nutzer des Kommunikationsnetzes Einsicht genommen werden soll. Dennoch kann für viele Fälle auf die oben gemachten Ausführungen verwiesen werden.

1. Studierender nicht ansprechbar

In den meisten Fällen bieten Hochschulen ihren Studierenden an, einen hochschuleigenen E-Mail-Account zu nutzen. Oftmals wird ein solcher bereits mit Immatrikulation automatisch erstellt. Daneben können Studierende meist das Internetnetz der Hochschule durch ihr persönliches Passwort nutzen und haben ihr persönliches Benutzerkonto auf den Hochschulservern. Ein Zugriff auf Nutzerdaten ist von verschiedenen Blickwinkeln zu beleuchten. Dabei ist zwischen einer Einsichtnahme in den E-Mail-Account, der damit verbundenen Relevanz des Fernmeldegeheimnisses und dem potentiellen Zugriff auf das Benutzerkonto zu differenzieren.

a) Fernmeldegeheimnis

Bietet die Hochschule ihren Studierenden die Nutzung ihres Hochschulnetzes zu Forschungs- und Studienzwecken an, so ist sie grundsätzlich Diensteanbieter i.S.d. TKG. Werden das Internet und/oder E-Mail-Accounts bereitgestellt, hat die Hochschule gem. § 88 Abs. 2 TKG das Fernmeldegeheimnis zu beachten. Insofern besteht bei andauerndem Kommunikationsvorgang insbesondere bzgl. E-Mail-Accounts, der besondere Schutz des Fernmeldegeheimnisses, wodurch eine Einsichtnahme in die E-Mail-Konten von Studierenden in aller Regel ausgeschlossen ist.

Zwar sind Studierende nach den meisten Landeshochschulgesetzen Mitglieder der Hochschule (vgl. z.B. § 9 Abs. 1 HG NRW, § 32 Abs. 1 HG Hessen), dennoch ist ihre Rolle gegenüber der Hochschule anders zu bewerten als die des Mitarbeiters gegenüber seinem Arbeitgeber, der besondere arbeitsvertragliche Verpflichtungen hat.

Studierende besuchen die Hochschule, um ihrer Ausbildung selbstständig nachzugehen. Sie tragen weder zur Abwicklung der Aufgabenerfüllung bei, noch werden sie entlohnt. Vielmehr sind sie das erforderliche Gegenstück des Lehrauftrages der Hochschule und ihrer Mitarbeiter.

Sie sind insofern nicht als Teil der Hochschule selbst, sondern immer auch in einer außerhalb der Hochschule befindlichen Rechtsposition berührt. Das TKG fordert insoweit für die Einordnung als Dritter i.S.d. § 3 Nr. 10 TKG nur eine gewisse Außenwirkung. Wird der Internetzugang durch die Hochschule bewusst so zur Verfügung gestellt, dass er nicht ausschließlich zur Erfüllung der eigenen wissenschaftlichen Tätigkeit, sondern darüber hinaus genutzt werden kann, wird sie entsprechend als Diensteanbieter i.S.d. TKG anzusehen sein.
Zwar sieht § 100 Abs. 1 TKG vor, dass der Diensteanbieter (Hochschule) im Rahmen des Erforderlichen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden darf, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können (vgl. § 100 Abs. 1 TKG). Allerdings wird sich damit kaum eine inhaltliche Einsichtnahme rechtfertigen lassen, da die Kommunikationsinhalte nicht zu den Bestands- oder Verkehrsdaten gehören und es zudem meist an der Erforderlichkeit mangeln wird.

b) Datenschutzrecht

Im Übrigen ist auf die Regelungen des Datenschutzes Rücksicht zu nehmen. Insofern gelten erneut die §§ 91 ff. TKG und subsidiär das jeweils einschlägige LDSG. Greift das Fernmeldegeheimnis nicht ein oder geht es nicht um telekommunikationsbezogene Daten, gilt das jeweilige Landesdatenschutzgesetz.

Im Rahmen der einzelfallspezifischen Abwägung bzgl. einer Erforderlichkeit sind dabei die Besonderheiten des Verhältnisses von Hochschule zu Nutzer zu beachten. Auch im Hinblick auf die datenschutzrechtlichen Restriktionen sind aber kaum Situationen denkbar, in denen eine Einsichtnahme in Mails von Studierenden gerechtfertigt wäre.

2. Studierender verstorben

Ist der Studierende verstorben, so ergeben sich im Übrigen keine Besonderheiten. Es ist für die Beantwortung der Frage, in welchem Umfang sich Abweichungen zum Falle der fehlenden Ansprechbarkeit ergeben, auf die o.g. Ausführungen zu verweisen.

Münster, April 2016

Forschungsstelle Recht im DFN

Die Forschungsstelle Recht ist ein Projekt 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