DFN

Infobrief Recht

9 / 2016

September 2016

Einer für alle, alle für einen

Bundesarbeitsgericht verneint Anspruch des Betriebsrates auf separaten Internetzugang und Telefonanschluss

Neues Datenschutzrecht = neue Sicherheit für Daten?

Die erforderlichen Maßnahmen datenverarbeitender Stellen nach der DS-GVO

Leben, um zu arbeiten oder arbeiten, um zu leben?!

Landesarbeitsgericht Rheinland-Pfalz: Herunterladen unbekannter Software am Arbeitsplatz als außerordentlicher Kündigungsgrund

Einer für alle, alle für einen

Bundesarbeitsgericht verneint Anspruch des Betriebsrates auf separaten Internetzugang und Telefonanschluss

von Florian Klein

Damit Betriebsräte ihre Aufgabe der Wahrnehmung und Vertretung der Arbeitnehmerinteressen gegenüber dem Arbeitgeber erfüllen können, sind sie darauf angewiesen, bestimmte Arbeitsmittel, insbesondere Informations- und Kommunikationsmittel, zu nutzen. Dass ein Betriebsrat grundsätzlich einen Anspruch auf Gewährung eines Zugangs zum Internet hat, ist bereits höchstrichterlich geklärt. Mit Beschluss vom 20.04.2016 (Az. 7 ABR 50/14) hat das Bundesarbeitsgericht (BAG) diesen Anspruch nun aber dahingehend konkretisiert, dass der Betriebsrat im Regelfall nicht verlangen kann, dass ihm ein Telefon- und Internetanschluss zur Verfügung gestellt wird, der unabhängig von dem Internetzugang und der Telefonanlage des Arbeitgebers ist und damit keine Kontrollmöglichkeiten bietet.

I. Hintergrund

Der Betriebsrat ist ein institutionalisiertes Gremium der Arbeitnehmervertretung, welches die Interessen der Belegschaft gegenüber dem Arbeitgeber wahrnehmen und in diesem Sinne insbesondere zahlreiche Mitbestimmungsrechte ausüben soll. Auch wenn nach dem Leitbild des Gesetzes Arbeitgeber und Betriebsrat vertrauensvoll zusammenarbeiten, liegt es auf der Hand, dass die jeweiligen Interessen häufig gegensätzlich sind und eine harmonische Zusammenarbeit deshalb nicht immer möglich ist. Um dem Gedanken der Waffengleichheit Rechnung zu tragen, ist der Betriebsrat mit bestimmten Rechten ausgestattet. So hat der Betriebsrat gemäß § 40 Abs. 2 Betriebsverfassungsgesetz (BetrVG) unter anderem einen Anspruch gegen den Arbeitgeber auf die erforderliche Ausstattung mit Räumen, sachlichen Mitteln, Informations- und Kommunikationstechnik sowie Büropersonal für Sitzungen, Sprechstunden und die laufende Geschäftsführung. Der Betriebsrat kann seine Aufgaben nur ordnungsgemäß wahrnehmen, wenn er über das nötige Fachwissen verfügt, wozu insbesondere auch Kenntnisse über das Arbeitsrecht sowie entsprechende Entwicklungen in Rechtsprechung und Gesetzgebung gehören. Deshalb hat die Rechtsprechung mittlerweile unter anderem einen Anspruch des Betriebsrats auf Bereitstellung eines Internetzugangs und eines Telefonanschlusses anerkannt.

Hochschulen sind meistens Körperschaften des öffentlichen Rechts der Länder und unterliegen als solche nicht dem Betriebsverfassungsgesetz, sondern den jeweiligen Landespersonalvertretungsgesetzen (LPersVG). Deshalb besteht bei ihnen auch kein Betriebsrat, sondern ein Personalrat. Allerdings weisen die Personalvertretungsgesetze und das BetrVG zahlreiche Parallelen auf, sodass Gerichtsentscheidungen zum BetrVG häufig auch auf das Personalvertretungsrecht der Länder übertragen werden können. So findet sich auch in den LPersVG in der Regel eine Vorschrift, die § 40 Abs. 2 BetrVG weitgehend entspricht und somit einen Anspruch des Personalrats auf Ausstattung mit den erforderlichen Mitteln begründet (so z. B. Art. 44 Abs. 2 BayPVG, § 41 Abs. 2 LPVG BW, § 40 Abs. 2 PersVG Berlin, § 41 Abs. 2 BremPVG, § 42 Abs. 2 PVG Hessen, § 37 Abs. 4 NdsPersVG, § 40 LPVG NRW, § 43 Abs. 2 LPersVG Rheinland-Pfalz, § 42 Abs. 3 PersVG Sachsen-Anhalt, § 44 Abs. 2 ThürPersVG). Die Mehrzahl der LPersVG erwähnt dabei jedoch noch nicht ausdrücklich die Informations- und Kommunikationstechnik, sondern benennt nur allgemein den Anspruch auf Ausstattung mit Geschäftsbedarf. Dieser Begriff ist dann aber so auszulegen, dass er die Informations- und Kommunikationstechnik umfasst, sodass insoweit keine Besonderheiten gelten.

Steht somit fest, dass auch der Personalrat dem Grunde nach in der Regel einen Anspruch auf Bereitstellung eines Internet-

zugangs und eines Telefonanschlusses hat, stellt sich im Einzelfall jedoch die Frage, inwiefern dieser dem Einflussbereich des Dienstherrn entzogen sein und welche Eigenschaften er aufweisen muss.

II. Die Entscheidung des Gerichts

Das Bundesarbeitsgericht hat nun entschieden, dass ein Betriebsrat grundsätzlich keinen Anspruch auf einen gesonderten Zugang zum Internet hat, der von dem im Betrieb genutzten und über einen Proxy-Server des Arbeitgebers geleiteten Internetzugang getrennt ist, damit der Arbeitgeber keine Überwachungsmöglichkeit hat. Hierzu bedürfte es konkreter Anhaltspunkte für eine Überwachungstätigkeit des Arbeitgebers.

1. Sachverhalt

In dem der Entscheidung zugrundeliegenden Sachverhalt stritt der Betriebsrat eines konzernangehörigen Betriebs für einen separaten Telefon- und Internetanschluss inklusive eines vor Überwachung geschützten E-Mail-Verkehrs. Zwar war das Betriebsratsbüro mit PC und Laptop ausgestattet und verfügte über einen Internetzugang, allerdings wurde dieser, wie für alle Betriebsangehörigen, über den Proxy-Server des Mutterkonzerns vermittelt. Mittels dieses Proxy-Servers wurde der Zugang zu bestimmten im Konzern nicht für notwendig gehaltenen Internetseiten (wie z. B. „YouTube“ und „eRecht24“) über einen Filter gesperrt. Außerdem bot er aus technischer Sicht die Möglichkeit, eine komplette Überwachung, Protokollierung und personen- bzw. betriebsratsbezogene Auswertung der Internetnutzung vorzunehmen. Darüber hinaus konnten die den Mitarbeitern zur Verfügung gestellten E-Mail-Postfächer vollumfänglich von den Administratoren gelesen werden und Spam-Mails wurden mittels eines Filters automatisch in den Junkmail-Ordner verschoben. Das Passwort, das den Zugang zum Internet und Intranet ermöglichte, war für alle Betriebsratsmitglieder einheitlich, sodass insofern ein Rückschluss auf einzelne Mitglieder nicht gezogen werden konnte.

Ebenfalls stand dem Betriebsrat ein Telefon-Nebenstellenanschluss zur Verfügung, der jedoch zur zentral vom Konzern verwalteten Telefonanlage gehörte. Diese konnte wiederum so eingestellt werden, dass sämtliche Verkehrsdaten mit vollständigen Zielnummern gespeichert und zudem personenbezogen ausgewertet werden konnten.

Aufgrund dieser abstrakten Möglichkeit der arbeitgeberseitigen Überwachung der Kommunikation und Internetnutzung des Betriebsrats hielt dieser einen eigenen separaten Internet- und Telefonanschluss für erforderlich, der ihm vom Arbeitgeber jedoch verwehrt wurde, sodass der Streit durch die Instanzen bis zum BAG ging.

2. Urteil

Das Bundesarbeitsgericht erteilte der Forderung des Betriebsrates eine Absage, weil der Anspruch auf Ausstattung mit Informationstechnik durch den vom Arbeitgeber bereitgestellten Internetzugang in der beschriebenen Form bereits erfüllt sei. Zwar obliege es grundsätzlich dem Betriebsrat zu prüfen, welche Sachmittel zur Erledigung seiner Aufgaben erforderlich und deshalb vom Arbeitgeber bereitzustellen seien. Allerdings dürfe der Betriebsrat sich dabei nicht bloß an seinen subjektiven Bedürfnissen orientieren, sondern müsse die betrieblichen Verhältnisse und die sich ihm stellenden Aufgaben berücksichtigen. Dies erfordere insbesondere eine Abwägung des Interesses der Belegschaft an einer sachgerechten Ausübung des Betriebsratsamtes mit den Interessen des Arbeitgebers, zu denen auch eine Begrenzung der Kostenlast gehöre.

Der Betriebsrat könne einen Internetzugang sowie die Teilhabe am E-Mail-Verkehr verlangen, soweit dies zur ordnungsgemäßen Wahrnehmung seiner ihm zugewiesenen Aufgaben erforderlich sei. Insofern ist ein Internetzugang in der Regel ein für die Aufgabenwahrnehmung dienliches Sachmittel, da verantwortliche Betriebsratsarbeit voraussetze, dass sich jedes Mitglied des Betriebsrats über anstehende Aufgaben informieren und dazu recherchieren könne. Diesem Anspruch werde aber durch die vorhandene Ausstattung des Betriebsratsbüros Genüge getan, wohingegen ein vom Netzwerk des Unternehmens unabhängiger Internetzugang und E-Mail-Verkehr nicht für erforderlich gehalten werden durfte. Dem stehe nicht entgegen, dass der Zugang zu einzelnen Internetseiten gesperrt sei, weil dies keine unzulässige Beeinträchtigung der Betriebsratsarbeit darstelle. Denn mithilfe des vom Arbeitgeber eingesetzten Proxy-Servers würden Schadsoftware ausgefiltert und Webseiten mit unerlaubten Inhalten gesperrt. Im Hinblick auf Webseiten mit strafbarem oder sittenwidrigem Inhalt bestehe schon von vornherein kein legitimes Zugriffsinteresse, während im Hinblick auf andere gesperrte Webseiten gegebenenfalls eine Freischaltung vom Arbeitgeber gefordert werden könne, sofern der Betriebsrat den Zugriff darauf unter Berücksichtigung der Interessen des Arbeitgebers für erforder-

lich halten dürfe.

Auch die abstrakte technische Möglichkeit einer umfassenden Überwachung durch den Arbeitgeber könne kein anderes Ergebnis begründen. Solange keine konkreten Anhaltspunkte vorlägen, könne dem Arbeitgeber nicht unterstellt werden, dass er von den technischen Überwachungsmöglichkeiten in unzulässiger Weise Gebrauch mache und insbesondere Inhalte des E-Mail-Verkehrs des Betriebsrates zur Kenntnis nehme oder auswerte. Denn auch umgekehrt gelte, dass die rein theoretische Möglichkeit einer sachfremden Nutzung des Internetanschlusses durch Mitglieder des Betriebsrats nicht dessen Anspruch auf einen Internetzugang ausschließe. Außerdem stehe der Vermutung, dass die Betriebsparteien das Internet missbräuchlich nutzen, der in § 2 Abs. 1 BetrVG niedergelegte Grundsatz der vertrauensvollen Zusammenarbeit entgegen. Im Übrigen könnte eine Kontrolle der Betriebsratstätigkeit durch Auswertung der Internetaktivitäten als unzulässige Behinderung (im Sinne von § 78 S. 1 BetrVG) eingestuft werden, die eine Strafbarkeit (gem. § 119 Abs. 1 Nr. 2 BetrVG) und Unterlassungsansprüche (§ 23 Abs. 3 BetrVG) nach sich ziehen könnte.

Ein anderes Ergebnis sei erst denkbar, wenn objektive Tatsachen vorlägen, die die Vermutung begründen, dass der Arbeitgeber seine abstrakten Kontrollmöglichkeiten missbräuchlich ausnutzt. Zudem stand dem Betriebsrat ein nicht personalisierter Internetzugang zur Verfügung, sodass daraus kein gesteigertes Risiko einer personenbezogenen Kontrolle erwachse, welche die Arbeit der einzelnen Mitglieder des Betriebsrats behindern könnte.

Schließlich führt das Gericht noch an, dass auch die Sicherheitsinteressen des Arbeitgebers vom Betriebsrat nicht hinreichend berücksichtigt worden seien. Es sei berechtigt, wenn der Arbeitgeber die Kommunikation über sein geschütztes technisches Netzwerk abwickeln wolle, um die erforderlichen Sicherheitsstandards der IT-Systeme gewährleisten zu können. Dieses Interesse des Arbeitgebers sei jedenfalls dann höher zu gewichten als das Interesse des Betriebsrats an einem unabhängigen Internetzugang, wenn keine Anhaltspunkte für eine arbeitgeberseitige Kontrolle bestünden. Auch aus datenschutzrechtlicher Sicht sei es vom berechtigten Interesse beider Betriebsparteien gedeckt, wenn die E-Mail-Kommunikation, die vertrauliche Informationen und persönliche Daten enthalte, innerhalb des geschützten gemeinsamen Netzwerks erfolge und dadurch unnötige Sicherheitslücken vermieden würden.

Zu guter Letzt weisen die Richter auch den Anspruch auf einen separaten Telefonanschluss ab, da über den bereitgestellten Nebenstellenanschluss eine uneingeschränkte Telekommunikation möglich sei und keine konkreten Anhaltspunkte für eine Überwachungstätigkeit des Arbeitgebers vorlägen. Außerdem habe der Arbeitgeber seine Bereitschaft erklärt, eine Vereinbarung mit dem Betriebsrat abzuschließen, die die Verpflichtung enthalte, die Aufzeichnung der Verkehrsdaten des Anschlusses des Betriebsrats zu unterdrücken. Dadurch würde dem Verlangen des Betriebsrats hinreichend entsprochen.

III. Fazit und Konsequenzen für die Hochschulpraxis

In erfreulicher Klarheit bringt das BAG zum Ausdruck, dass Betriebsräte im Regelfall keinen Anspruch auf einen Internetzugang haben, der unabhängig von den im Unternehmen bestehenden IT-Systemen ist. Eine zusätzliche Kostenbelastung des Arbeitgebers wird dadurch vermieden. Selbstredend soll der Betriebsrat seine Aufgaben frei und unabhängig wahrnehmen können, ohne eine Kontrolle und Überwachung durch den Arbeitgeber befürchten zu müssen. Dem trägt die Entscheidung des BAG aber hinreichend Rechnung, indem sie die Unzulässigkeit einer Überwachung durch den Arbeitgeber feststellt und die rechtlichen Folgen eines potentiellen Verstoßes gegen dieses Verbot aufzeigt. Es sollte nicht der Regelfall sein, dass Arbeitgebern unterstellt wird, dass sie rechtswidrig handeln, indem sie in unzulässiger Weise die Kommunikation des Betriebsrats überwachen. Sobald jedoch konkrete Anhaltspunkte für eine Überwachungstätigkeit bestehen, hat der Betriebsrat ausreichende rechtliche Mittel zur Hand, um sich dagegen zu wehren. Insbesondere lässt es die Entscheidung des BAG in solchen Fällen auch zu, dass ein Anspruch auf einen separaten Internetzugang geltend gemacht werden kann. Dies hat der Arbeitgeber sich dann letztlich selbst zuzuschreiben, sodass darin keine unangemessene Belastung gesehen werden kann. Von diesen Ausnahmefällen abgesehen ist es jedoch auch für den Betriebsrat keine unzumutbare Benachteiligung, wenn er seine Geschäfte über den normalen Internetzugang des Unternehmens abwickeln muss. Erhebliche Nachteile drohen insoweit nicht, da der Arbeitgeber für etwaige Verstöße zur Rechenschaft gezogen werden kann und aus einer rechtswidrigen Überwachung erlangte Kenntnisse in vielen Fällen einem Beweisverwertungsverbot unterliegen werden. Zu Recht weist das Bundesarbeitsgericht in diesem Zusammenhang auch auf die Sicherheitsrisiken und die Belange des Datenschutzes hin. Die Gewährleistung einer hinreichenden IT-Sicherheit ist in

der heutigen Zeit mit großem Aufwand verbunden und angesichts der stetig steigenden Bedrohung durch Kriminelle, die im Internet agieren, von großer Bedeutung. Insofern ist es sachgerecht, den Arbeitgeber grundsätzlich nur mit der Sicherung seines zentralen Netzwerks zu belasten und Nebenstellen möglichst zu vermeiden.

Diese Erwägungen lassen sich auf die Ansprüche des Personalrats auf Ausstattung mit den nötigen Sachmitteln und Informationstechnik an Hochschulen und öffentlichen Forschungseinrichtungen weitestgehend übertragen. Auch dort gibt es in der Regel keine Notwendigkeit für die Bereitstellung eines vom Netz der Einrichtung separierten Internetzugangs. Erst wenn konkrete Anhaltspunkte für eine Überwachung der Kommunikation und Internetnutzung des Personalrats vorliegen, kann sich die Interessenlage ändern. Sicherheitsinteressen und die Gewährleistung des Datenschutzes haben hierbei mindestens den gleichen Stellenwert wie im Bereich des Betriebsverfassungsrechts.

Auch wenn nicht für alle vom BAG herangezogenen Normen vergleichbare Regelungen im Personalvertretungsrecht zu finden sind, ist zu vermuten, dass die Richter hier gewissermaßen aus dem Vollen schöpfen und zu demselben Ergebnis kommen würden, wenn „nur" konkrete Anhaltspunkte für eine Überwachungstätigkeit fehlen und der Grundsatz der vertrauensvollen Zusammenarbeit berücksichtigt wird. Deshalb ist es unschädlich, dass eine Störung oder Behinderung der Tätigkeiten des Personalrats nach den LPersVG nicht strafbar ist, so wie dies § 119 Abs. 1 Nr. 2 BetrVG im Hinblick auf Tätigkeiten des Betriebsrats vorsieht. Immerhin legen auch die LPersVG in der Regel fest, dass eine Störung oder Behinderung der Tätigkeiten des Personalrats unzulässig ist (so z. B. Art. 8 BayPVG, § 6 Abs. 1 LPVG BW, § 8 LPersVG Brandenburg, § 56 BremPVG, § 64 Abs. 1 LPVG Hessen, § 41 Abs. 1 NdsPersVG, § 7 Abs. 1 LPVG NRW, § 6 S. 1 LPersVG Rheinland-Pfalz, § 8 S. 1 PersVG Sachsen-Anhalt, § 8 ThürPersVG). Auch der Grundsatz der vertrauensvollen Zusammenarbeit zwischen Personalrat und Dienststelle existiert im Personalvertretungsrecht gleichermaßen (so z. B. Art. 2 Abs. 1 BayPVG, § 2 Abs. 1 LPersVG Brandenburg, § 2 Abs. 1 PersVG Berlin, § 2 Abs. 1 LPVG BW, § 60 Abs. 1 PVG Hessen, § 2 Abs. 1 NdsPersVG, § 2 Abs. 1 LPVG NRW, § 2 Abs. 1 LPersVG Rheinland-Pfalz, § 2 Abs. 1 PersVG Sachsen-Anhalt, § 2 Abs. 1 ThürPersVG). Ein per se rechtswidriges Verhalten kann den Hochschulen und Forschungseinrichtungen nicht unterstellt werden, sodass es grundsätzlich keine Vermutung für eine unzulässige Überwachung der Tätigkeiten des Personalrats durch den Dienstherrn gibt.

Vereinzelt spricht sogar der Wortlaut des jeweiligen LPersVG unmittelbar für die Richtigkeit beziehungsweise Übertragbarkeit der Entscheidung des BAG auf das Personalvertretungsrecht. So sehen beispielsweise sowohl § 41 Abs. 2 LPVG BW als auch § 44 Abs. 2 ThürPersVG vor, dass die Dienststelle für die laufende Geschäftsführung die Informations- und Kommunikationstechnik bereitstellen muss, die üblicherweise in der Dienststelle genutzt werden. Ein Anspruch auf einen separaten Internetzugang, der vom Netzwerk der Dienststelle komplett unabhängig ist, lässt sich daraus grundsätzlich nicht ableiten. Zu den üblicherweise genutzten Informations- und Kommunikationstechniken gehören vielmehr die herkömmlichen Zugänge über das Netzwerk der Einrichtung. Insofern kommt auf Hochschulen und Forschungseinrichtungen kein erhöhter Kosten- und Arbeitsaufwand zu. Zusammenfassend ist deshalb davon auszugehen, dass sich auch Personalräte an Hochschulen und öffentlichen Forschungseinrichtungen in der Regel mit einem Internetzugang über das Netz der Einrichtung begnügen müssen.

Neues Datenschutzrecht = neue Sicherheit für Daten?

Die erforderlichen Maßnahmen datenverarbeitender Stellen nach der DS-GVO

von Lennart Sydow

Nach Verabschiedung der Datenschutz-Grundverordnung (DS-GVO) kommen auf datenverarbeitende Stellen teilweise neue und/oder geänderte Verpflichtungen beim Umgang mit personenbezogenen Daten zu, die sie ab Mai 2018 einhalten müssen. Neben einigen Anforderungen, die sich aus den Rechten ergeben, welche die Betroffenen gegenüber der datenverarbeitenden Stelle geltend machen können, bestehen zahlreiche Verpflichtungen auch schon ohne Tätigwerden der Betroffenen.
Dazu zählen unter anderem die Einhaltung der Prinzipien des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen, die Erstellung von Verfahrensverzeichnissen, die Bestellung eines Datenschutzbeauftragten und die Umsetzung angemessener technischer und organisatorischer Maßnahmen zur Erfüllung der Datenschutzanforderungen.

I. Überblick

Der folgende Artikel soll zunächst die allgemeinen Verpflichtungen zur Umsetzung von Maßnahmen bei der Datenverarbeitung darstellen, die unabhängig davon bestehen, ob die Betroffenen ihre Rechte aus der DS-GVO wie z. B. das Recht auf Löschung (siehe dazu: Leinemann, Vergiss mein nicht… – Das Recht auf Löschung gemäß Artikel 17 Datenschutz-Grundverordnung, DFN-Infobrief Recht 08/2016, S. 2) geltend machen, und aufzeigen, welche Änderungen im Vergleich zur bisherigen Rechtslage zu erwarten sind. Dabei können auf Hochschulen und Forschungseinrichtungen neue Verpflichtungen zukommen, sodass möglicherweise Abläufe geändert und Vorkehrungen getroffen werden müssen. Die neuen Melde- und Benachrichtigungspflichten der DS-GVO sollen dann später in einem weiteren Beitrag vorgestellt werden.

Bei Verstößen gegen diese Verpflichtungen können die Aufsichtsbehörden nach Art. 83 DS-GVO Bußgelder gegen die verantwortliche Stelle (und ggf. beteiligte Auftragsdatenverarbeiter) verhängen. Da diese nach der DS-GVO bis zu 10 000 000 € oder bei Unternehmen 2 % des weltweiten Jahresumsatzes betragen können, werden solche Sanktionsmittel nun auch deutlich gravierender, als dies bisher der Fall war. Denkbar sind darüber hinaus Schadensersatzansprüche der Betroffenen gemäß Art. 82 DS-GVO, wenn diesen durch einen Verstoß des Verantwortlichen ein Schaden entstanden ist. Es können sowohl materielle als auch immaterielle Schäden geltend gemacht werden.

II. Datenschutz durch technische Umsetzung

Die Verwirklichung der Grundsätze der Datenverarbeitung aus Art. 5 DS-GVO (siehe dazu Leinemann, Alles neu macht der Mai!?, DFN-Infobrief Recht 06/2016, S. 8 ff.) soll unter anderem durch die beiden Prinzipien des Datenschutzes durch Technik („Privacy by design“) und der datenschutzfreundlichen Voreinstellungen („Privacy by default“) erreicht werden.

Das Prinzip des Datenschutzes durch Technik ist in Art. 25 Abs. 1 DS-GVO enthalten und verpflichtet datenverarbeitende Stellen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, um die Datenschutzgrundsätze auch in

der Praxis umzusetzen. Relevant dafür, welche Maßnahmen in diesem Rahmen erforderlich sind, sind unter anderem die Art, der Umfang und Zweck der Datenverarbeitung sowie das Risiko für die Betroffenen und die Kosten der Maßnahmen. Für datenverarbeitende Stellen in Deutschland ergeben sich daraus höchstens geringe Änderungen, da eine vergleichbare Verpflichtung bereits in § 9 BDSG (und ähnlich, wenn auch oft allgemeiner formuliert, in den Landesdatenschutzgesetzen, siehe bspw. § 10 DSG NRW) besteht. Neu ist allerdings die Sanktionsmöglichkeit durch Auferlegen eines Bußgeldes, die dafür bisher nicht ausdrücklich vorgesehen ist.
Unter dem Begriff der datenschutzfreundlichen Voreinstellungen wird das in Art. 25 Abs. 2 DS-GVO festgeschriebene Prinzip verstanden, die technischen und organisatorischen Abläufe von vornherein so einzurichten, dass nur die Daten gespeichert werden, die zu dem verfolgten Zweck unbedingt erforderlich sind. Dies betrifft sowohl die Menge der Daten als auch den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung.

Durch Einführung dieser Prinzipien wird den datenverarbeitenden Stellen eine neue sehr allgemein gehaltene Verpflichtung auferlegt, ihre Abläufe und technischen Einrichtungen so auszugestalten, dass das Risiko von Datenschutzverletzungen durch präventive Maßnahmen verringert wird. Da die Vorschriften bußgeldbewehrt sind, entsteht ein spürbarer Druck, dies einzuhalten. Da die Prinzipien sehr allgemein verfasst sind, besteht allerdings erheblicher Spielraum bei der Frage, wann eine Stelle ihre Verpflichtungen erfüllt hat und damit einhergehend auch eine gewisse Unsicherheit.
Die Erwägungsgründe der DS-GVO nennen als Beispiele für solche Maßnahmen die Minimierung der Verarbeitung personenbezogener Daten, schnellstmögliche Pseudonymisierung sowie Transparenz und die Möglichkeit des Betroffenen, die Datenverarbeitung zu überwachen.
Zum Zweck der eindeutigeren Beurteilung kann bezüglich der Erfüllung dieser Prinzipien gemäß Art. 25 Abs. 3 DS-GVO ein Zertifizierungsverfahren eingerichtet werden, um genauere und spezifischere Vorgaben für die Umsetzung dieser Prinzipien vorzugeben und datenverarbeitenden Stellen die Einhaltung zu erleichtern. Bis solche Zertifizierungsmöglichkeiten bestehen, müssen die Stellen selbst (unter Einbeziehung des Datenschutzbeauftragten) eine Einschätzung treffen, welche Maßnahmen diesbezüglich erforderlich sind.

III. Technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau

Auch die erforderlichen Sicherheitsmaßnahmen sollen die Datenschutzgrundsätze konkretisieren und ihre Umsetzung in der Verarbeitungspraxis sicherstellen. Sie ergeben sich ab 2018 aus Art. 32 DS-GVO und nicht mehr wie bisher aus der Anlage zu § 9 BDSG (für private Stellen) beziehungsweise für öffentliche Stellen aus den vergleichbaren Vorschriften in den Landesdatenschutzgesetzen (z. B. § 10 DSG NRW). Dort wird allerdings kein ausführlicher Katalog konkreter Maßnahmen aufgeführt. Stattdessen werden – wie bisher – lediglich die Ziele vorgegeben, an denen die erforderlichen technischen und organisatorischen Maßnahmen auszurichten sind. Zwar besteht daher ein neuer Anforderungskatalog, die Ziele als solche ergeben aber zusammengenommen ein sehr ähnliches Bild. Es ist weiterhin erforderlich, die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme bei der Datenverarbeitung sicherzustellen. Das Erfordernis einer regelmäßigen Überprüfung der getroffenen Maßnahmen inklusive einer Bewertung ihrer Wirksamkeit ist aus deutscher Sicht ebenfalls nicht neu. Darüber hinaus müssen ausdrücklich die Verfügbarkeit von Daten und der Zugang zu diesen auch im Fall eines Zwischenfalls rasch wiederhergestellt werden können.
Wie erwähnt gibt es kaum genaue Angaben darüber, wie diese Ziele erreicht werden können. Ausdrücklich als solche Maßnahmen genannt werden lediglich die Pseudonymisierung und die Verschlüsselung von Daten. In Art. 32 Abs. 1 DS-GVO finden sich aber darüber hinaus Kriterien für die Abwägung, welche Maßnahmen erforderlich sind, um ein angemessenes Schutzniveau zu gewährleisten. Danach ist das Risiko eines Schadenseintritts ebenso zu berücksichtigen wie der Stand der Technik, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung.

Zu bestimmen, was genau unter diese teils sehr allgemeinen Begriffe fällt, ist im Einzelfall nicht immer ohne Schwierigkeiten möglich. Aber auch bei der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit können die Aufsichtsbehörden den datenverarbeitenden Stellen diese Ermessensentscheidung gemäß Art. 32 Abs. 3 DS-GVO durch Zertifizierungsverfahren erleichtern.

Im Ergebnis bleibt das Erfordernis technischer und organisatorischer Maßnahmen durch die DS-GVO mindestens ebenso

vage, wie dies nach der bisherigen Rechtslage der Fall war. Es sind lediglich die Ziele aufgeführt, an denen die Verarbeitungsprozesse auszurichten sind. Insgesamt sind dabei keine erheblichen Änderungen zu erkennen. Für die Praxis bleibt daher zu hoffen, dass die Aufsichtsbehörden den datenverarbeitenden Stellen die Einhaltung dieser Grundsätze durch ein Zertifizierungsverfahren erleichtern.

IV. Datenschutzbeauftragte

Für Hochschulen und Forschungseinrichtungen, die als öffentliche Einrichtungen ausgestaltet sind, bleibt das Erfordernis, einen Datenschutzbeauftragten zu bestellen, gemäß Art. 37 Abs. 1 a) DS-GVO bestehen. Eine Lockerung dieser Pflicht kann sich höchstens für private datenverarbeitende Stellen ergeben.

Anders als bisher (vgl. § 32a Abs. 1 S. 1 DSG NRW) können öffentliche Stellen in Zukunft allerdings nicht nur einen internen Datenschutzbeauftragten bestellen, sondern gemäß Art. 37 Abs. 6 DS-GVO auch auf externe Dienstleister zurückgreifen. Die Anforderungen an die zum Datenschutzbeauftragten bestellte Person bleiben gleich. Vorausgesetzt werden weiterhin die berufliche Qualifikation und das Fachwissen sowie die Fähigkeit, die Aufgaben eines Datenschutzbeauftragten zu erfüllen. Die Stellung des Datenschutzbeauftragten ist auch unter der DS-GVO frei (im Rahmen dieser Funktion) und nicht weisungsgebunden.

Auch der Aufgabenbereich des Datenschutzbeauftragten ändert sich durch die DS-GVO kaum. Er ist nach Art. 39 Abs. 1 DS-GVO weiterhin für die Beratung, Sensibilisierung und Schulung der mit der Datenverarbeitung befassten Mitarbeiter zuständig, überwacht die Einhaltung der Datenschutzvorschriften und ist die Kontaktperson für die Aufsichtsbehörde. Diese Aufgaben müssen Datenschutzbeauftragte in öffentlichen und privaten Stellen nach derzeit geltender Rechtlage in Deutschland auch vor Einführung der DS-GVO schon wahrnehmen. Neu ist die ausdrücklich erwähnte Beratung im Rahmen der Datenschutz-Folgenabschätzung.

V. Datenschutz-Folgenabschätzung und vorherige Konsultation

Ein neues Instrument der DS-GVO ist die Datenschutz-Folgenabschätzung in Art. 35 DS-GVO. Eine solche muss angestellt werden, wenn durch eine Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten“ der Betroffenen besteht. Diese ebenfalls sehr allgemein gehaltene Formulierung wird aber spezifiziert durch den Hinweis, dass insbesondere der Einsatz neuer Technologien solche Situationen hervorrufen kann, und durch die Feststellung in Absatz 3, dass die Folgenabschätzung insbesondere erforderlich ist, wenn auf Grundlage der Verarbeitung Entscheidungen mit Rechtswirkung getroffen, besonders sensible Daten (in Art. 9 DS-GVO aufgeführt) verarbeitet oder Daten bei der Überwachung im öffentlichen Raum gesammelt werden.

Insbesondere der Hinweis auf die neuen Technologien hat für Hochschulen und Forschungseinrichtungen eine hohe Relevanz. Aber auch Entscheidungen mit Rechtswirkung können z. B. bei Zulassungen oder Ablehnungen zu Studiengängen oder Prüfungsentscheidungen getroffen werden. Es ist daher erforderlich, sich mit der Erforderlichkeit und Durchführung einer Datenschutz-Folgenabschätzung auseinander zu setzen. Bei diesem Verfahren ist nach Art. 35 Abs. 2 DS-GVO auch der Datenschutzbeauftragte verpflichtend zu beteiligen.

Um die Entscheidung, wann eine solche Folgenabschätzung erforderlich ist, zu erleichtern, erstellen die Aufsichtsbehörden eine Liste mit Verarbeitungsvorgängen, die eine solche Folgenabschätzung zwingend erfordern und können darüber hinaus auch eine „White List“ herausgeben, wann auf diese ausdrücklich verzichtet werden kann.

Die Folgenabschätzung muss gemäß Art. 35 Abs. 7 DS-GVO zumindest eine Beschreibung der Datenverarbeitung und Angaben über den Zweck, die Verhältnismäßigkeit und die Risiken, einschließlich der getroffenen Abhilfemaßnahmen, enthalten. Inhaltlich bestehen Parallelen zur bisherigen Pflicht zur Vorabkontrolle, die die Landesdatenschutzgesetze aktuell noch für öffentliche Einrichtungen vorsehen (z. B. in § 10 Abs. 3 DSG NRW). Somit ist das Instrument als solches inhaltlich nicht gänzlich neu, es sind aber die neuen Voraussetzungen zu beachten.

Wenn die Folgenabschätzung ergibt, dass durch die Verarbeitung ein hohes Risiko für die Betroffenen besteht, muss die verantwortliche Stelle gemäß Art. 36 Abs. 1 DS-GVO die zuständige Aufsichtsbehörde konsultieren, das Vorhaben darlegen und Maßnahmen mit dieser absprechen.

VI. Verzeichnis von Verarbeitungstätigkeiten

Ebenfalls keine gravierenden Änderungen bringt die Ver-

pflichtung zur Erstellung eines Verzeichnisses über die Verarbeitungstätigkeiten in Art. 30 DS-GVO mit sich, die zudem nur für Einrichtungen ab 250 Mitarbeitern gilt. Auch dies ist für datenverarbeitende Stellen unter dem Begriff des Verfahrensverzeichnisses schon bisher verpflichtend (für öffentliche Stellen in NRW gem. § 8 DSG NRW). Die Angaben umfassen insbesondere Kontaktdaten der Verantwortlichen, die Zwecke der Verarbeitung, die Kategorien der verarbeiteten Daten, der betroffenen Personen und der Empfänger der Daten, sowie die vorgesehenen Fristen für die Löschung und die Beschreibung der getroffenen Sicherheitsmaßnahmen.
Geändert ist aber der Zugriff auf eben dieses Verzeichnis, welches dann nur noch der Aufsichtsbehörde zur Verfügung gestellt werden muss und nicht mehr für jedermann einsehbar ist.

VII. Fazit

Insgesamt ist festzustellen, dass die DS-GVO aus Sicht von Hochschulen und Forschungseinrichtungen zwar durchaus geänderte Verpflichtungen bereit hält, allerdings auch keinen völlig neuen Umgang mit personenbezogenen Daten vorsieht. Zudem lassen die teils sehr allgemeinen Formulierungen oft einigen Interpretationsspielraum. Es bleibt daher abzuwarten, ob und wie die Aufsichtsbehörden ihre Möglichkeiten zur Einführung von Zertifizierungsverfahren wahrnehmen und dadurch die geforderten Maßnahmen eindeutiger aufzeigen. Bis dahin bleibt datenverarbeitenden Stellen nur, die bisherigen Abläufe unter Beteiligung des Datenschutzbeauftragten auf Widersprüche zu den neuen Vorschriften zu untersuchen. Zumindest die Erforderlichkeit der Datenschutz-Folgenabschätzung erfordert darüber hinaus die Einführung gänzlich neuer Verfahrensabläufe, die praktisch einen durchaus erheblichen Aufwand verursachen können.

Auf die neu geregelten Benachrichtigungs- und Meldepflichten der DS-GVO wird in einem separaten Artikel eingegangen.

Siehe zur Datenschutz-Grundverordnung auch schon:

Sydow, Vereinheitlichung des EU-Datenschutzrechts?, DFN-Infobrief Recht 05/2016, S. 2 ff.

Leinemann, Alles neu macht der Mai!?, DFN-Infobrief Recht 06/2016, S. 8 ff.

Leinemann, Vergiss mein nicht… – Das Recht auf Löschung gemäß Artikel 17 Datenschutz-Grundverordnung, DFN-Infobrief Recht 08/2016, S. 2 ff.

Leben, um zu arbeiten oder arbeiten, um zu leben?!

Landesarbeitsgericht Rheinland-Pfalz: Herunterladen unbekannter Software am Arbeitsplatz als außerordentlicher Kündigungsgrund

von Armin Strobel

Arbeit und Privatleben vermischen sich zunehmend. Der Arbeitnehmer ist immer öfter auch in privaten Situationen für den Arbeitgeber erreichbar. Gleichzeitig nutzen immer mehr Arbeitnehmer die Ressourcen ihres Arbeitgebers, um private Dinge zu erledigen. Nicht selten werden dabei auch der Dienst-PC und der dienstliche Internetzugang während der Arbeitszeit zweckentfremdet. Schnell ist eine Datei für den privaten Gebrauch über den Dienst-PC heruntergeladen und auf diesem installiert. Das Landesarbeitsgericht (LAG) Rheinland-Pfalz hat sich in seinem Urteil vom 12.11.2015 (Az. 5 Sa 10/15) mit einem solchen Fall befasst. Hierbei hat das Gericht die arbeitsrechtlichen Risiken der privaten Nutzung von Arbeitgeberressourcen verdeutlicht und die Voraussetzungen für eine fristlose Kündigung wegen eines solchen Vergehens herausgearbeitet. Im Blickpunkt steht dabei das Herunterladen von Schadsoftware als wichtiger Grund für eine fristlose Kündigung.

I. Hintergrund

Vielen Arbeitnehmern fällt eine Trennung von Arbeits- und Privatleben angesichts fortschreitender Digitalisierung dieser beiden Bereiche schwer. Angelegenheiten, die zuvor einem Bereich eindeutig zugeordnet werden konnten, werden durcheinander gebracht und vermehrt auch in Situationen bearbeitet bzw. vorgenommen, in denen sie eigentlich nicht verortet sind. Hierzu zählen zum Beispiel das Kontrollieren von Arbeits-E-Mails nach der Arbeitszeit oder der private Anruf im Büro für die Wochenendplanung. Die ständige Verfügbarkeit durch das Internet und dessen Einbindung in alle Lebensbereiche verstärkt diese Entwicklung zunehmend.

Wenn die Arbeitsleistung nach Feierabend durch den Arbeitnehmer auch ärgerlich sein mag, so drohen für den Fall, dass in der Arbeitszeit oder mit Ressourcen des Arbeitgebers in unzulässiger Weise privaten Angelegenheiten nachgegangen wird, schwerwiegende arbeitsrechtliche Konsequenzen. Hierzu gehören insbesondere die ordentliche Kündigung gem. § 620 Abs. 2 des Bürgerlichen Gesetzbuches (BGB) oder im schlimmsten Fall sogar die außerordentliche Kündigung (§ 626 BGB). Wie ein solcher Fall aussehen kann, zeigt das Urteil des LAG Rheinland-Pfalz. Zunächst ist ein kurzer Blick auf die – hier relevanten – arbeitsrechtlichen Besonderheiten zu werfen.

Ein zeitlich unbegrenztes Arbeitsverhältnis kann nach § 620 Abs. 2 BGB i.V.m. dem Arbeitsvertrag jederzeit unter Einhaltung einer Kündigungsfrist und Berücksichtigung des Kündigungsschutzgesetzes von beiden Seiten beendet werden. Ein besonderer Grund ist hierfür nicht erforderlich. Neben dieser ordentlichen Kündigung, gibt es noch die Möglichkeit der außerordentlichen Kündigung nach § 626 BGB. Hierbei ist keine Kündigungsfrist zur Beendigung des Arbeitsverhältnisses erforderlich. Dafür muss aber ein wichtiger Grund vorliegen. Die Beurteilung, ob ein solcher Grund im Einzelfall vorliegt ist durch eine zweistufige Prüfung zu ermitteln. Zunächst ist zu fragen, ob das Verhalten des Arbeitnehmers, das zur Kündigung führen soll, allgemein ein wichtiger Grund für eine fristlose Kündigung ist. Das heißt es muss geprüft werden, ob der Sachverhalt ohne seine besonderen Umstände typischer-

weise – oder anders ausgedrückt: generalisierend – als wichtiger Grund angesehen werden kann. Es ist also eine abstrakte Prüfung erforderlich. Das kündigungsrelevante Verhalten wird insofern losgelöst vom konkreten Fall betrachtet. Wird dabei festgestellt, dass das beanstandete Verhalten allgemein, also grundsätzlich bei allen Arbeitsverhältnissen, eine fristlose Kündigung begründen kann, erfolgt der zweite Prüfungsschritt. Es ist zu bewerten, ob der Kündigungsgrund auch unter Berücksichtigung der konkreten Umstände des Einzelfalls und der Abwägung der Interessen beider Parteien (Arbeitgeber und Arbeitnehmer) als wichtiger Grund eingestuft werden kann. Hierbei ist unter anderem zu beachten, wie es zu dem kündigungsrelevanten Verhalten durch den Arbeitnehmer gekommen ist und ob die Einhaltung der Kündigungsfrist dem Arbeitgeber zuzumuten ist oder das Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer derart gestört ist, dass eine Einhaltung der Frist nicht zumutbar erscheint. Ist auch im Rahmen der konkreten Betrachtung des Kündigungsgrundes von einem wichtigen Grund auszugehen, kann die Voraussetzung bejaht werden und die fristlose Kündigung ist zulässig.

Da die fristlose Kündigung für den Arbeitnehmer ein besonders empfindliches Übel darstellt, ist die Maßnahme nur als letztes Mittel zu wählen. Die Möglichkeit einer Abmahnung ist als milderes Mittel immer zu berücksichtigen und genießt Vorrang, wenn keine wichtigen Gründe dagegen sprechen. Um dieses Ultima-ratio-Prinzip zu unterstreichen, gibt es zudem die Kündigungserhebungsfrist von zwei Wochen, § 626 Abs. 2 S. 1 BGB. Hiernach muss die fristlose Kündigung innerhalb von zwei Wochen nach Bekanntwerden des Kündigungsgrundes erklärt werden.

II. Entscheidung des LAG Rheinland-Pfalz

Das LAG Rheinland-Pfalz befasste sich in seiner Entscheidung mit diesen arbeitsrechtlichen Fragen und steckte die Grenzen der Arbeitssphäre vom Privatbereich ab. Dem Urteil lag der Sachverhalt zu Grunde, dass ein kriminaltechnisches Prüfungslabor (im Folgenden: Arbeitgeber) seinem Arbeitnehmer außerordentlich gekündigt hat. Die Kündigung stützte der Arbeitgeber auf die erhebliche Verletzung arbeitsvertraglicher Pflichten durch den Arbeitnehmer. Dieser habe den Dienst-PC zu privaten Zwecken verwendet und ein schadhaftes Programm heruntergeladen, obwohl der Arbeitgeber als kriminaltechnisches Prüflabor mit sensiblen Daten agiert und die private Nutzung von Arbeitsressourcen untersagt war. Gegen diese Kündigung erhob der Arbeitnehmer eine Kündigungsschutzklage, um feststellen zu lassen, dass die Kündigung unwirksam sei.

Das Arbeitsgericht Koblenz, als erste Instanz (Urt. v. 20.11.2014 – 2 Ca 1804/14), hatte dem Arbeitnehmer zunächst Recht gegeben und die außerordentliche Kündigung für unwirksam erklärt, da es den geltend gemachten Grund nicht als wichtigen Grund i.S.d. § 626 Abs. 1 BGB eingestuft hatte. Diese Entscheidung revidierte das LAG Rheinland-Pfalz daraufhin mit dem eingangs genannten Urteil.

Hierbei stellte das Gericht schwerpunktmäßig fest, dass der durch das kriminaltechnische Prüfungslabor geltend gemachte Kündigungsgrund ein wichtiger i.S.d. § 626 Abs. 1 BGB sei. Der Arbeitgeber stütze seine Kündigungsentscheidung auf ein Fehlverhalten des Arbeitnehmers in der Form, dass dieser unter Nutzung seines Arbeit-Accounts eine Musikbearbeitungssoftware auf den Dienst-PC heruntergeladen hat. Dabei handelte es sich um eine Schadsoftware, die einen Virus enthielt, durch den der unbefugte Zugriff über das Internet ermöglicht wurde. Der Virus beeinträchtigte dabei nicht nur in arbeitsrelevanter Form die Software des Dienst-PCs, sondern ermöglichte auch einen unkontrollierten Datenabfluss. Hierin sah der Arbeitgeber eine wesentliche arbeitsvertragliche Pflichtverletzung, da zum einen die private Nutzung des Dienst-PCs und des Internets während der Arbeitszeit verboten waren und zum anderen der Arbeitnehmer durch bewusstes Ignorieren der Warnung des Virenscanners das Vertrauensverhältnis zwischen dem Arbeitgeber und dem Arbeitnehmer im besonderen Maße verletzt hat. Diese Auffassung wurde durch das LAG Rheinland-Pfalz bestätigt. Aufgrund des Verbots des Arbeitgebers und der Tatsache, dass die Arbeitnehmer des kriminaltechnischen Prüfungslabors mehrmals datenschutzrechtlich geschult wurden, bewertete das Gericht das Verhalten des Arbeitnehmers sowohl abstrakt, als auch unter Berücksichtigung des Einzelfalls, als wichtigen Grund für eine fristlose Kündigung.

Im Rahmen dieser Problematik stellte das Gericht klar, dass der Arbeitgeber berechtigt war im Berufungsverfahren Gründe für die Beurteilung der Schwere des Pflichtverstoßes nachzureichen. Die Tatsache, dass der Arbeitnehmer die Warnung des Virenscanners bewusst weggedrückt hatte und dadurch erst die Installation des schädigenden Programms ermöglichte, erfuhr der Arbeitgeber erst nach dem Ausspruch der fristlo-

sen Kündigung. Da der Sachverhalt jedoch bereits objektiv zum Zeitpunkt der Kündigungserklärung abgeschlossen war und lediglich später bekannt wurde, durfte die Begründung für die Gewichtung des Kündigungsgrundes nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) „nachgeschoben" werden.

Anschließend stellte das LAG fest, dass keine Abmahnung durch den Arbeitgeber erforderlich war. Eine solche ist zwar grundsätzlich als milderes Mittel immer in Betracht zu ziehen, jedoch kann sie in besonderen Fällen, wie z. B. einem besonders schwerwiegenden Pflichtverstoß, entbehrlich sein. Der betroffene Arbeitnehmer verwies darauf, dass sein Pflichtverstoß für seinen Arbeitgeber nicht so schwerwiegend und deshalb hinnehmbar gewesen sei. Er begründete das damit, dass ein Verbot der privaten Nutzung von Arbeitsressourcen bestand, dieses jedoch nicht ernsthaft verfolgt wurde. So hätten alle Mitarbeiter die Dienst-PCs in den Mittagspausen auch für private Bedürfnisse genutzt. Dies sei vom Arbeitgeber hingenommen bzw. toleriert worden. Zudem habe der Arbeitnehmer auch einmal für den Geschäftsführer des Arbeitgebers in privater Sache von dem Dienst-PC eine Bestellung vornehmen sollen. Dieser Argumentation folgte das LAG jedoch nicht. Es verwies darauf, dass der Arbeitgeber ausdrücklich die private Nutzung des Internets untersagt habe und die Mitarbeiter datenschutzrechtlich mehrfach geschult wurden. Außerdem sei zwischen dem „normalen" Surfen im Internet und dem Herunterladen von Software – insbesondere von unbekannten Quellen – und das anschließende Installieren der Software auf dem Dienst-PC zu unterscheiden. Das Herunterladen beinhalte erheblich höhere Risiken, zumal auch die Warnung des Virenscanners zunächst noch überwunden werden müsse. Dieses Zusammentreffen der verschiedenen Faktoren begründe in diesem Fall die Annahme der Entbehrlichkeit der Abmahnung durch den Arbeitgeber, auch wenn das Verbot der privaten Nutzung des Internets nicht in letzter Konsequenz verfolgt werde.

Die für eine fristlose Kündigung unerlässliche Interessenabwägung entschied das Gericht zugunsten des Arbeitgebers. Für den Arbeitnehmer spreche zwar seine Unterhaltspflicht gegenüber seinem Kind. Jedoch wird diese durch die Interessen des Arbeitgebers in Form der erhöhten datenschutzrechtlichen Anforderungen eines solchen Prüfungslabors und die Tatsache, dass der Betroffene durch seine erst einjährige Beschäftigung noch keinen nennenswerten sozialen Besitzstand erworben habe, überlagert.
Auch die Kündigungserhebungsfrist von zwei Wochen wurde nach Ansicht des Gerichts durch den Arbeitgeber eingehalten. Es beurteilte daher zugunsten des Arbeitgebers die außerordentliche Kündigung des Arbeitsverhältnisses als wirksam. Die Installation der Software zu privaten Zwecken trotz expliziten Verbots und die damit einhergehenden Risiken für den Arbeitgeber rechtfertigen nach Auffassung des LAG das Bedürfnis nach einer sofortigen Beendigung der vertraglichen Beziehungen.

III. Fazit und Konsequenzen für die Hochschulpraxis

Der geschilderte Fall zeigt sehr deutlich, welche Risiken die unbefugte private Nutzung von Arbeitsressourcen in – aber auch außerhalb – der Arbeitszeit mit sich bringt. Die fristlose Kündigung ist zwar eine drastische Maßnahme, aber deshalb nicht weniger wahrscheinlich. Die Hochschulen sind von dieser Problematik ebenso betroffen wie andere Arbeitgeber. Das Herunterladen von Software kann hier ebenso vorkommen wie im vorliegenden Fall. Dabei agieren auch Hochschulen mit sensiblen Daten, die eines Schutzes bedürfen.

Kommt es zu einem Verstoß der Arbeitsvorgaben durch einen Angestellten, den die Hochschule mit einer fristlosen Kündigung ahnden möchte, sollte sie eine gründliche Prüfung vornehmen, ob der konkrete Verstoß ein wichtiger Grund i.S.d. § 626 BGB darstellt. Hierbei ist nach dem zweistufigen Prüfungsaufbau vorzugehen. Das unbefugte Herunterladen von fremden Dateien kann einen solchen Grund darstellen. Die Entscheidung des LAG macht deutlich, dass das Herunterladen von Schadsoftware grundsätzlich als wichtiger Grund i.S.d. § 626 Abs. 1 BGB anzusehen ist. Die Risiken, die mit dem Herunterladen von Software verbunden sind, z. B. die Gefahr von Viren, sind den Nutzern des Internets bekannt. Es besteht dadurch die Gefahr, dass ungewollt und unerkannt Daten abfließen. Mögliche Folgeschäden von solchen Vorgängen begründen deshalb eine solche Bewertung im Allgemeinen. Einen solchen Verstoß könnte die Hochschule daher ahnden, wenn auch die Umstände des Einzelfalls für ein solches Ergebnis sprechen. Zumindest die erste Stufe der Prüfung kann insoweit aber bejaht werden und zwar unabhängig davon, ob die Internetnutzung als solche untersagt ist oder nur das Herunterladen von Software.

Die Prüfung, ob das beanstandete Verhalten eines Angestellten im Einzelfall tatsächlich eine fristlose Kündigung begründen kann, sollte gründlich und nicht vorschnell erfolgen. Insbesondere sollte auch die Frage berücksichtigt werden, ob eine Abmahnung als milderes Mittel im konkreten Fall ausreichend ist und daher vorzuziehen wäre. Trotz der gebotenen Sorgfalt darf aber auch nicht zu lange mit der Entscheidung über eine Kündigung gewartet werden. Ansonsten droht die fristlose Kündigung nach § 626 Abs. 2 BGB verspätet zu sein. Hierbei kommt dem Arbeitgeber jedoch die Möglichkeit des „Nachschiebens von Gründen“ zugute. Werden nach der Kündigungserklärung weitere Gründe für eine fristlose Kündigung bekannt, die bereits bei Aussprache der Kündigung vorlagen, können diese auch im späteren Verlauf noch nachgereicht werden. Insoweit besteht auch nach einer Kündigung die Möglichkeit nach weiteren Gründen zu forschen und diese zu dokumentieren.

Bei Angestellten mit unbefristeten Arbeitsverträgen ist zudem empfehlenswert sowohl die außerordentliche, als auch die ordentliche Kündigung zu erklären, um trotz möglicher Mängel bei der außerordentlichen Kündigung das Arbeitsverhältnis möglichst zeitnah zu beenden.

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