Rechtsanwalt Dr. Kai Stumper

Datenschutz in der Arbeitswelt 4.0

Version 1

Oktober 2018

Kanzlei Dr. Stumper – firstlex

Anschrift	Telefon/Mail	Internet
Kanzlei Dr. Stumper - firstlex® Neuer Wall 10 20354 Hamburg	+49 (700) 34778539* dr.stumper@firstlex.de	firstlex.de kanzlei.dr.stumper.de

Inhaltsverzeichnis

Urteile

1 BAG: Überwachung mittels Keylogger - Verwertungsverbot

BAG, 27.07.2017, 2 AZR 681/16

Leitsatz

Der Einsatz eines Software-Keyloggers ist nicht nach § 32 Abs. 1 BDSG erlaubt, wenn kein auf den Arbeitnehmer bezogener, durch konkrete Tatsachen begründeter Verdacht einer Straftat oder anderen schwerwiegenden Pflichtverletzung besteht.

Orientierungssatz

1. Die Aufzeichnung und Speicherung der Tastatureingaben am Dienst-PC eines Arbeitnehmers sowie das Fertigen von Screenshots durch einen Keylogger stellen Datenerhebungen i.S.v. § 3 Abs 1, Abs 2 S 1, Abs 3 und Abs 7 BDSG dar.(Rn.19) Ein Arbeitnehmer willigt nicht schon dadurch gemäß § 4a BDSG in diese Datenerhebung, dass er dem ihm mitgeteilten Einsatz eines Keyloggers nicht widerspricht. Das Unterlassen eines Protests kann nicht mit einer Einwilligung i.S.v. § 4a Abs 1 BDSG gleichgesetzt werden.

2. Mit einer ohne Einwilligung des Arbeitnehmers erfolgten Datenerhebung durch einen Keylogger greift der Arbeitgeber in dessen durch Art. 2 Abs 1 i.V.m. Art 1 Abs 1 GG geschütztes Recht auf informationelle Selbstbestimmung ein. Für einen Eingriff in den Schutzbereich dieses Grundrechts ist es ohne Bedeutung, ob die Datenerhebung in verdeckter Form oder für den Arbeitnehmer erkennbar erfolgt.

3. Der Eingriff in den Schutzbereich von Art 2 Abs 1 i.V.m. Art 1 Abs 1 GG entfällt nicht dadurch, dass lediglich Verhaltensweisen am Arbeitsplatz erfasst werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen desjenigen Rechnung, der sich in die (Betriebs-)Öffentlichkeit begibt.

4. Im Falle einer der (verdeckten) Videoüberwachung vergleichbar eingriffsintensiven Maßnahme, die auf § 32 Abs 1 S 1 BDSG gestützt werden soll, muss der auf konkrete Tatsachen begründete Verdacht einer schwerwiegenden, jedoch nicht strafbaren Pflichtverletzung bestehen. Eine entsprechende verdeckte Ermittlung "ins Blaue hinein", ob ein Arbeitnehmer sich pflichtwidrig verhält, ist auch nach § 32 Abs 1 S 1 BDSG unzulässig. Sie ist, ohne dass es noch darauf ankäme, ob mildere, gleich effektive Mittel vorhanden waren, jedenfalls unangemessen (nicht verhältnismäßig im engeren Sinne).

5. Weniger intensiv in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifende Datenerhebungen können nach § 32 Abs 1 BDSG ohne Vorliegen eines durch Tatsachen begründeten Anfangsverdachts - zumal einer Straftat oder anderen schweren Pflichtverletzung - zulässig sein. Das gilt vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende

offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen sollen.

6. Die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers kann zulässig sein, um die Einhaltung eines vom Arbeitgeber aufgestellten kompletten Verbots oder doch einer Beschränkung der Privatnutzung von IT-Einrichtungen zu kontrollieren.

Tatbestand

Die Parteien streiten über die Wirksamkeit einer außerordentlichen, hilfsweise ordentlichen Kündigung.

Der Kläger war bei der Beklagten, die in ihrem Betrieb regelmäßig mehr als zehn Arbeitnehmer beschäftigt, seit Juli 2011 als Webentwickler tätig. Zu Beginn des Arbeitsverhältnisses verpflichtete er sich schriftlich, Hard- und Software aus Gründen der informationstechnischen Sicherheit ausschließlich zur Erfüllung der vereinbarten Aufgaben zu nutzen.

Im Zusammenhang mit der Anbindung eines neuen Netzwerks richtete die Beklagte am 19. April 2015 (Sonntag) eine E-Mail folgenden Inhalts an ihre Mitarbeiter:

„Hallo liebes (…) Team,

es ist soweit, die Telekom hat es endlich geschafft, uns einen schnellen Internet Anschluss bereitzustellen.

Dieses möchte ich Euch natürlich nicht vorenthalten, aus diesem Grund erhaltet Ihr freien Zugang zum WLAN.

Da bei Missbrauch, zum Beispiel Download von illegalen Filmen, etc. der Betreiber zur Verantwortung gezogen wird, muss der Traffic mitgelogged werden. Da ein rechtlicher Missbrauch natürlich dann auch auf denjenigen zurückfallen soll, der verantwortlich dafür war.

Somit:

Hiermit informiere ich Euch offiziell, dass sämtlicher Internet Traffic und die Benutzung der Systeme (der Beklagten) mitgelogged und dauerhaft gespeichert wird. Solltet Ihr damit nicht einverstanden sein, bitte ich Euch mir dieses innerhalb dieser Woche mitzuteilen.

…

Bitte benutzt dieses Netzwerk für alles wie Spotify, YouTube, etc. um unser Hauptnetzwerk zu entlasten.

…"

In einer Unterweisung am 20. April 2015 wandte sich kein Arbeitnehmer gegen die Absicht der Beklagten, den „Internettraffic" und die Benutzung ihrer Systeme zur Verhinderung von Missbrauch des Internetzugangs „mitzuloggen".

Die Beklagte installierte sodann auf dem Dienst-PC des Klägers eine Software, die ab dem 21. April 2015 alle Tastatureingaben protokollierte und regelmäßig Screenshots fertigte (Keylogger). Nachdem die Beklagte die vom Keylogger erstellten Dateien ausgewertet hatte, fand am 4. Mai 2015 ein Gespräch mit dem Kläger statt, in dem dieser einräumte, seinen Dienst-Rechner während der Arbeitszeit privat genutzt zu haben. Er gab an, ein Computerspiel programmiert und E-Mail-Verkehr für das Logistikunternehmen seines Vaters abgewickelt zu haben. Auf die Programmierung des Spiels habe er am Arbeitsplatz in der Zeit von Januar bis April 2015 ca. drei Stunden verwendet. Für die Firma seines Vaters sei er - vorwiegend in seiner Freizeit - höchstens etwa zehn Minuten täglich tätig gewesen.

Die Beklagte kündigte das Arbeitsverhältnis des Klägers mit Schreiben vom 19. Mai 2015 außerordentlich fristlos, hilfsweise ordentlich zum nächstzulässigen Termin.

Hiergegen hat sich der Kläger fristgerecht mit der vorliegenden Klage gewandt. Er hat behauptet, die privaten Verrichtungen meist in den Pausen und in Zeiten erledigt zu haben, in denen er keines der ihm zugewiesenen Projekte habe bearbeiten können. Die Beklagte habe durch den Einsatz eines Keyloggers „hinterrücks" und ohne jeden Anlass massiv in sein Grundrecht auf informationelle Selbstbestimmung eingegriffen. In der E-Mail vom 19. April 2015 habe sie den Eindruck vermittelt, es sollten nur die Internetaktivitäten über das neue Netzwerk kontrolliert werden.

Der Kläger hat sinngemäß beantragt,

1. festzustellen, dass das Arbeitsverhältnis der Parteien nicht durch die außerordentliche Kündigung der Beklagten vom 19. Mai 2015 aufgelöst worden ist;

2. festzustellen, dass das Arbeitsverhältnis der Parteien nicht durch die ordentliche Kündigung der Beklagten vom 19. Mai 2015 aufgelöst worden ist;

3. hilfsweise für den Fall des Obsiegens mit den Feststellungsanträgen die Beklagte zu verurteilen, ihn bis zum rechtskräftigen Abschluss des Kündigungsschutzverfahrens als Webentwickler weiterzubeschäftigen.

Die Beklagte hat beantragt, die Klage abzuweisen. Aus den vom Keylogger erstellten Dateien ergebe sich, dass der Kläger am 21. April 2015 weitaus länger mit der Entwicklung des Computerspiels beschäftigt gewesen sei, als er eingeräumt habe. Die Einträge in den Logdateien widerlegten zudem seine Behauptung, höchstens zehn Minuten täglich mit Aufgaben für die Firma seines Vaters befasst gewesen zu sein. Ausweislich von Screenshots der auf seinem Dienst-PC befindlichen Ordner habe der Kläger für dessen Unternehmen 5.221 E-Mails empfangen und 5.835 Nachrichten versandt. Der Einsatz eines Keyloggers sei ohne Weiteres rechtmäßig gewesen, weil dem Kläger jede außerdienstliche Nutzung der IT-Systeme untersagt und damit seine Privatsphäre nicht betroffen gewesen sei. Im Übrigen habe gegen ihn der Verdacht des Arbeitszeitbetrugs bestanden. Am 9. Februar 2015 habe eine Arbeitnehmerin im Vorbeigehen gesehen, dass der Kläger eine „stark bebilderte" Webseite hastig „weggeklickt" habe. Weitere Mitarbeiter hätten mitgeteilt, der Kläger gehe während seiner Arbeitszeit in erheblichem Umfang privaten Aktivitäten nach. Zudem habe er sich zu einem sehr unproduktiven Mitarbeiter entwickelt.

Die Vorinstanzen haben der Klage stattgegeben. Mit ihrer Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter.

Entscheidungsgründe

Die Revision ist unbegründet. Das Landesarbeitsgericht hat die Berufung der Beklagten gegen das der Klage stattgebende Urteil des Arbeitsgerichts zu Recht zurückgewiesen. Die dem Senat allein zur Entscheidung anfallenden Feststellungsanträge sind begründet. Die Kündigungen der Beklagten vom 19. Mai 2015 sind unwirksam. Nach dem verfahrensrechtlich verwertbaren Sachvortrag der Beklagten fehlt es sowohl an einem wichtigen Grund für die außerordentliche Kündigung (§ 626 Abs. 1 BGB) als auch an einer sozialen Rechtfertigung für die unter Geltung des Kündigungsschutzgesetzes (§ 1 Abs. 1, § 23 Abs. 1) erklärte ordentliche Kündigung (§ 1 Abs. 2 KSchG).

I. Die Würdigung des Berufungsgerichts, die vom Kläger zugestandenen Sachverhalte rechtfertigten die beiden Kündigungen nicht, ist revisionsrechtlich nicht zu beanstanden.

1. Das Landesarbeitsgericht ist davon ausgegangen, der Kläger habe in der Zeit von Januar bis April 2015 an seinem Dienst-Rechner ca. drei Stunden auf die Programmierung des Computerspiels verwendet, dies aber überwiegend während der Pausen. Darüber hinaus hat das Berufungsgericht zugunsten der Beklagten unterstellt, der Kläger habe während der Arbeitszeit täglich zehn Minuten mit Tätigkeiten für die Firma seines Vaters verbracht. Damit habe er seine vertraglichen Pflichten in erheblicher Weise verletzt. Allerdings rechtfertigten die Pflichtverletzungen mangels vorheriger Abmahnung keine - außerordentliche oder ordentliche - Kündigung. Zwar habe der Kläger Hard- und Software der Beklagten entgegen der von ihm zu Beginn des Arbeitsverhältnisses unterzeichneten Erklärung für außerdienstliche Zwecke eingesetzt. Die „minutenweise" Privatnutzung über den Zeitraum eines Jahres habe sich zu einer Gesamtdauer von 36,66 Stunden summiert. Jedoch sei schon der E-Mail der Beklagten vom 19. April 2015 zu entnehmen, dass tatsächlich kein absolutes Verbot der privaten Nutzung betrieblicher IT-Einrichtungen gelebt worden sei. Die unzulässige Privatnutzung habe auch nur einen minimalen Bruchteil (2,08 vH) der täglichen Arbeitszeit des Klägers ausgemacht. Die Beklagte habe schließlich nicht substantiiert dargetan, dass seine Arbeitsleistung durch die außerdienstlichen Aktivitäten beeinträchtigt worden sei. Insgesamt liege keine derart schwere Pflichtverletzung vor, dass selbst deren erstmalige Hinnahme der Beklagten nach objektiven Maßstäben unzumutbar und damit offensichtlich - auch für den Kläger erkennbar - ausgeschlossen gewesen sei. Es gebe auch keine Anhaltspunkte dafür, dass sich der Kläger in Zukunft nach einer Abmahnung in gleicher oder ähnlicher Weise pflichtwidrig verhalten hätte.

2. Mit dieser Würdigung hat das Berufungsgericht, dem bei der Prüfung und Interessenabwägung im Rahmen von § 626 Abs. 1 BGB, § 1 Abs. 2 KSchG ein Beurteilungsspielraum zukommt, alle vernünftigerweise in Betracht zu ziehenden Umstände widerspruchsfrei und ohne Verstoß gegen Denkgesetze oder allgemeine Erfahrungssätze berücksichtigt. Entgegen der Annahme der Revision hat das Landesarbeitsgericht den „auf lange Sicht" - möglicherweise - verursachten Schaden

in seine Überlegungen einbezogen, indem es die „vertane" Arbeitszeit auf einen Zeitraum von einem Jahr hochgerechnet hat. Zu einem über die Vergütung der nicht bestimmungsgemäß verbrachten Arbeitszeit hinausgehenden Schaden hat die Beklagte nicht substantiiert vorgetragen. Soweit sie rügt, das Berufungsgericht habe übersehen, dass der Kläger nicht um Erlaubnis gefragt habe, obgleich er nur ausnahmsweise am Arbeitsplatz für die Firma seines Vaters habe tätig werden wollen und man insoweit eine „adäquate Lösung" hätte finden können, bestätigt die Beklagte letztlich nur die Einschätzung des Berufungsgerichts, es sei zumindest nicht ausgeschlossen gewesen, dass sie eine geringfügige Privatnutzung ihrer Betriebsmittel während der Arbeitszeit hinnehmen würde.

II. Das Landesarbeitsgericht ist zu Recht davon ausgegangen, es müsse bei seiner Entscheidung den Sachvortrag der Beklagten unberücksichtigt lassen, den sie nur aufgrund des von ihr eingesetzten Keyloggers in das Verfahren einführen konnte. Die Verwertung dieses Vorbringens bei der Urteilsfindung wäre mit dem Recht des Klägers auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) unvereinbar.

1. Ein Sachvortrags- oder Beweisverwertungsverbot wegen einer Verletzung des gemäß Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts einer Partei (vgl. auch Art. 8 Abs. 1 EMRK) kann sich im arbeitsgerichtlichen Verfahren aus der Notwendigkeit einer verfassungskonformen Auslegung des Prozessrechts - etwa von § 138 Abs. 3, § 286, § 331 Abs. 1 Satz 1 ZPO - ergeben. Wegen der nach Art. 1 Abs. 3 GG bestehenden Bindung an die insoweit maßgeblichen Grundrechte und der Verpflichtung zu einer rechtsstaatlichen Verfahrensgestaltung (BVerfG 13. Februar 2007 - 1 BvR 421/05 - Rn. 93, BVerfGE 117, 202) hat das Gericht zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Erkenntnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 21; 20. Oktober 2016 - 2 AZR 395/15 - Rn. 18; 22. September 2016 - 2 AZR 848/15 - Rn. 23, BAGE 156, 370; BGH 15. Mai 2013 - XII ZB 107/08 - Rn. 21). Das Grundrecht schützt neben der Privat- und Intimsphäre und seiner speziellen Ausprägung als Recht am eigenen Bild auch das Recht auf informationelle Selbstbestimmung, das die Befugnis garantiert, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden (BVerfG 11. März 2008 - 1 BvR 2074/05 ua. - Rn. 67, BVerfGE 120, 378; 23. Februar 2007 - 1 BvR 2368/06 - Rn. 37, BVerfGK 10, 330; 15. Dezember 1983 - 1 BvR 209/83 ua. - zu C II 1 a der Gründe, BVerfGE 65, 1).

2. Die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) über die Anforderungen an eine zulässige Datenverarbeitung konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung und am eigenen Bild (§ 1 Abs. 1 BDSG). Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe durch öffentliche oder nicht-öffentliche Stellen iSd. § 1 Abs. 2 BDSG in diese Rechtspositionen zulässig sind. Sie ordnen für sich genommen jedoch nicht an, dass unter ihrer Missachtung gewonnene Erkenntnisse oder Beweismittel bei der Feststellung des Tatbestands im arbeitsgerichtlichen Verfahren vom Gericht nicht berücksichtigt werden dürften (BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 17; 22. September 2016 - 2 AZR 848/15 - Rn. 22, BAGE 156, 370). Ist allerdings die

Datenverarbeitung gegenüber dem betroffenen Arbeitnehmer nach den Vorschriften des BDSG zulässig, liegt insoweit keine Verletzung seines Rechts auf informationelle Selbstbestimmung und am eigenen Bild vor (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 22).

3. In Anwendung dieser Grundsätze hat sich das Landesarbeitsgericht zu Recht gehindert gesehen, seiner Entscheidung den streitigen Sachvortrag der Beklagten über die Nutzung des Dienst-PC durch den Kläger am 21. und 23. April 2015 zugrunde zu legen. Hierdurch hätte das Landesarbeitsgericht eine durch die Beklagte begangene Grundrechtsverletzung perpetuiert und vertieft. Die Datenerhebung durch den Keylogger griff in das Recht des Klägers auf informationelle Selbstbestimmung ein. Der Kläger hat in die Maßnahme nicht eingewilligt. Der Eingriff war nicht aufgrund überwiegender Interessen der Beklagten nach § 32 Abs. 1 oder § 28 Abs. 1 BDSG gerechtfertigt. Ebenso lagen keine weiteren, über das schlichte Beweisinteresse der Beklagten hinausgehenden Aspekte vor, die gerade die in Frage stehende verdeckte Informationsbeschaffung durch einen Keylogger als gerechtfertigt erscheinen lassen könnten.

a) Die Aufzeichnung und Speicherung der Tastatureingaben am Dienst-PC des Klägers sowie das Fertigen von Screenshots durch den Keylogger stellten Datenerhebungen iSv. § 3 Abs. 1, Abs. 2 Satz 1, Abs. 3 und Abs. 7 BDSG dar. Die Beklagte hat sich dadurch Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten natürlichen Person, nämlich des Klägers als dem Nutzer des ihm zugeordneten Rechners, verschafft.

b) Der Kläger hat in die Datenerhebungen nicht dadurch gemäß § 4a BDSG eingewilligt, dass er der Ankündigung der Beklagten nicht widersprochen hat. Allein in der Tatsache, dass ein Arbeitnehmer einer ihm mitgeteilten Maßnahme nicht entgegen tritt, liegt keine Einverständniserklärung in die Informationserhebung. Das Unterlassen eines Protests kann nicht mit einer Einwilligung gleichgesetzt werden (für die Videoüberwachung im öffentlichen Raum: vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 40, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 25, BVerwGE 141, 329). Das gilt insbesondere, wenn - wie vorliegend - eine vom Arbeitgeber gesetzte „Widerspruchsfrist" noch nicht abgelaufen ist. Im Übrigen hatte die Beklagte dem Kläger nicht eröffnet, es sollten alle Tastatureingaben an seinem Dienst-PC „mitgeloggt" und regelmäßig Screenshots gefertigt werden. Auch konnte der Kläger nicht erkennen, zu welchem Zweck er überwacht wurde. Die E-Mail der Beklagten vom 19. April 2015 legte den Schluss nahe, dass allein eine etwaige Internetaktivität über das neue Netzwerk und diese auch „nur" hinsichtlich der abgerufenen Inhalte („Download von illegalen Filmen", „Betreiber zur Verantwortung gezogen", „rechtlicher Missbrauch") kontrolliert werden sollte. Das Landesarbeitsgericht hat nicht festgestellt, in der mündlichen Unterweisung am 20. April 2015 seien anderslautende oder weiter gehende Aussagen getroffen worden. Dementsprechend ließ die Beklagte dem Kläger in ihrem Schreiben vom 5. Mai 2015 lediglich mitteilen, sie habe „im Zuge der Umstellung des Internetanschlusses zur Vermeidung eines etwaigen Missbrauchs die Onlineaktivitäten, die über diesen Anschluss laufen, kontrolliert und diese Kontrolle im Vorfeld sowohl per E-Mail als auch im Rahmen einer Ansprache an die gesamte Belegschaft angekündigt."

c) Mit der ohne Einwilligung des Klägers erfolgten Datenerhebung durch den Keylogger hat die Beklagte in dessen durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschütztes Recht auf informationelle Selbstbestimmung eingegriffen.

aa) Für einen Eingriff in den Schutzbereich dieses Grundrechts ist es ohne Bedeutung, ob die Datenerhebung in verdeckter Form oder für den Arbeitnehmer erkennbar erfolgt.

(1) Bei dem verdeckten Einsatz eines Keyloggers wird der betroffene Arbeitnehmer in der Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden, beschränkt, indem er zum Ziel einer nicht erkennbaren - systematischen - Beobachtung durch den Arbeitgeber gemacht wird und dadurch auf sich beziehbare Daten über sein Verhalten preisgibt, ohne die Überwachung oder gar den mit ihr verfolgten Verwendungszweck zu kennen (für die automatisierte Erhebung öffentlich zugänglicher Informationen vgl. BVerfG 11. März 2008 - 1 BvR 2074/05 ua. - Rn. 67, BVerfGE 120, 378; für die Observation durch einen Detektiv außerhalb des Betriebsgeländes vgl. BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 24).

(2) Wird der Keylogger offen eingesetzt, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, weil die Aufzeichnung und Speicherung sämtlicher Tastatureingaben und bestimmter Bildschirminhalte der Vorbereitung möglicher belastender Maßnahmen (Ermahnung, Abmahnung, Kündigung) dienen und zugleich abschreckend wirken und insoweit das Verhalten des Betroffenen lenken soll (für die offene Videoüberwachung im öffentlichen Raum: vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 38, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 24, BVerwGE 141, 329).

bb) Der Eingriff in den Schutzbereich von Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG entfällt nicht dadurch, dass lediglich Verhaltensweisen am Arbeitsplatz erfasst werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen desjenigen Rechnung, der sich in die (Betriebs-)Öffentlichkeit begibt (für die Videoüberwachung vgl. BVerfG 23. Februar 2007 - 1 BvR 2368/06 - Rn. 39, BVerfGK 10, 330; BVerwG 25. Januar 2012 - 6 C 9/11 - Rn. 25, BVerwGE 141, 329; für die Observation durch einen Detektiv vgl. BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 24).

cc) Ein Eingriff in das Recht auf informationelle Selbstbestimmung setzt nicht voraus, dass der betroffene Arbeitnehmer das informationstechnische System, über das Daten erhoben werden, als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das System selbstbestimmt verfüge. Diese Einschränkung betrifft allein das ebenfalls von Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, dem ggf. eine lückenfüllende Funktion zukommt (BVerfG 27. Februar 2008 - 1 BvR 370/07 ua. - Rn. 201 und Rn. 206, BVerfGE 120, 274).

d) Der Einsatz des Keyloggers war der Beklagten nicht nach § 32 Abs. 1 BDSG erlaubt. Es fehlte bereits an dem insoweit erforderlichen, durch konkrete Tatsachen

begründeten Anfangsverdacht einer Straftat oder einer anderen schweren Pflichtverletzung. Eine Maßnahme, die hinsichtlich der Intensität des durch sie bewirkten Eingriffs in das allgemeine Persönlichkeitsrecht des Arbeitnehmers mit einer (verdeckten) Videoüberwachung vergleichbar ist, stellt sich als unverhältnismäßig dar, wenn sie aufgrund bloßer Mutmaßungen ergriffen wird.

aa) Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses ua. dann erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Zur Durchführung gehört die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt (Gola/Schomerus BDSG 12. Aufl. § 32 Rn. 16; Grimm JM 2016, 17, 19), zur Beendigung iSd. Kündigungsvorbereitung (dazu Grimm, aaO) die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 26). Sofern nach § 32 Abs. 1 Satz 1 oder Satz 2 BDSG zulässig erhobene Daten den Verdacht einer solchen Pflichtverletzung begründen, dürfen sie für die Zwecke und unter den Voraussetzungen des § 32 Abs. 1 Satz 1 BDSG auch verarbeitet und genutzt werden (BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 20. Oktober 2016 - 2 AZR 395/15 - Rn. 40; 22. September 2016 - 2 AZR 848/15 - Rn. 37 f., BAGE 156, 370). Der Begriff der Beendigung umfasst dabei die Abwicklung eines Beschäftigungsverhältnisses (BT-Drs. 16/13657 S. 21). Der Arbeitgeber darf deshalb alle Daten speichern und verwenden, die er benötigt, um die ihm obliegende Darlegungs- und Beweislast in einem potentiellen Kündigungsschutzprozess zu erfüllen (BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; Stamer/Kuhnke in Plath BDSG § 32 Rn. 149; HWK/Lembke 7. Aufl. § 32 BDSG Rn. 15).

bb) § 32 Abs. 1 Satz 2 BDSG erlaubt die Datenerhebung, -verarbeitung und -nutzung in Fällen, in denen - unabhängig von den in § 32 Abs. 1 Satz 1 BDSG näher bestimmten Zwecken - Anhaltspunkte für den Verdacht einer im Beschäftigungsverhältnis begangenen Straftat bestehen. Der Gesetzgeber geht davon aus, dass Maßnahmen, die vom Arbeitgeber ergriffen werden, um strafbares Verhalten eines Arbeitnehmers aufzudecken, in der Regel besonders intensiv in dessen allgemeines Persönlichkeitsrecht eingreifen (BT-Drs. 16/13657 S. 21). Das ist insbesondere bei einer zu diesem Zweck erfolgenden (verdeckten) Überwachung von Beschäftigten der Fall, weshalb die - von der Gesetzesbegründung in Bezug genommenen - restriktiven Grundsätze der hierzu ergangenen Rechtsprechung in § 32 Abs. 1 Satz 2 BDSG gesondert kodifiziert wurden. Die Vorschrift soll hinsichtlich der Eingriffsintensität damit vergleichbare Maßnahmen erfassen (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 27; 12. Februar 2015 - 6 AZR 845/13 - Rn. 75, BAGE 151, 1). Diese sollen allenfalls dann zulässig sein, wenn der durch konkrete Tatsachen begründete „einfache" Verdacht (Anfangsverdacht, BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 25) einer im Beschäftigungsverhältnis begangenen Straftat besteht.

cc) § 32 Abs. 1 Satz 2 BDSG entfaltet keine „Sperrwirkung" dergestalt, dass eine anlassbezogene Datenerhebung durch den Arbeitgeber ausschließlich zur Aufdeckung von Straftaten zulässig wäre und sie nicht nach § 32 Abs. 1 Satz 1 BDSG zulässig sein könnte (ausführlich BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 28 ff.). Allerdings muss der mit einer Datenerhebung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers auch im Rahmen von § 32 Abs. 1 Satz 1

BDSG einer Abwägung der beiderseitigen Interessen nach dem - dort gleichfalls verankerten - Grundsatz der Verhältnismäßigkeit standhalten (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 32; 17. November 2016 - 2 AZR 730/15 - Rn. 30; 7. September 1995 - 8 AZR 828/93 - zu II 2 c bb der Gründe, BAGE 81, 15; 22. Oktober 1986 - 5 AZR 660/85 - zu B I 2 a der Gründe, BAGE 53, 226). Dieser verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 17. November 2016 - 2 AZR 730/15 - aaO; 15. April 2014 - 1 ABR 2/13 (B) - Rn. 41, BAGE 148, 26; 29. Juni 2004 - 1 ABR 21/03 - zu B I 2 d der Gründe, BAGE 111, 173). Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (BVerfG 4. April 2006 - 1 BvR 518/02 - zu B I 2 b dd der Gründe, BVerfGE 115, 320; BAG 29. Juni 2017 - 2 AZR 597/16 - aaO; 15. April 2014 - 1 ABR 2/13 (B) - aaO). Die Datenerhebung, -verarbeitung oder -nutzung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Danach muss im Falle einer der (verdeckten) Videoüberwachung vergleichbar eingriffsintensiven Maßnahme, die auf § 32 Abs. 1 Satz 1 BDSG gestützt werden soll, der auf konkrete Tatsachen begründete Verdacht einer schwerwiegenden, jedoch nicht strafbaren Pflichtverletzung bestehen. Eine entsprechende verdeckte Ermittlung „ins Blaue hinein", ob ein Arbeitnehmer sich pflichtwidrig verhält, ist auch nach § 32 Abs. 1 Satz 1 BDSG unzulässig (BAG 29. Juni 2017 - 2 AZR 597/16 - aaO). Sie ist, ohne dass es noch darauf ankäme, ob mildere, gleich effektive Mittel vorhanden waren, jedenfalls unangemessen (nicht verhältnismäßig im engeren Sinne).

dd) Aus Vorstehendem folgt zugleich, dass weniger intensiv in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifende Datenerhebungen nach § 32 Abs. 1 BDSG ohne Vorliegen eines durch Tatsachen begründeten Anfangsverdachts - zumal einer Straftat oder anderen schweren Pflichtverletzung - zulässig sein können. Das gilt vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende offene Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen dienen sollen. Solche präventiven Maßnahmen können sich schon aufgrund des Vorliegens einer abstrakten Gefahr als verhältnismäßig erweisen, wenn sie keinen solchen psychischen Anpassungsdruck erzeugen, dass die Betroffenen bei objektiver Betrachtung in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt sind (dazu BAG 25. April 2017 - 1 ABR 46/15 - Rn. 20 und Rn. 28 ff.). Dementsprechend kann die vorübergehende Speicherung und stichprobenartige Kontrolle der Verlaufsdaten eines Internetbrowsers zulässig sein, um die Einhaltung eines vom Arbeitgeber aufgestellten kompletten Verbots oder doch einer Beschränkung der Privatnutzung von IT-Einrichtungen zu kontrollieren. Dabei werden lediglich die Adressen und Titel der aufgerufenen Seiten und der Zeitpunkt des Aufrufs protokolliert und damit nicht mehr Daten gespeichert, als benötigt werden, um einen möglichen inhaltlichen oder zeitlichen Missbrauch der Nutzungsrechte festzustellen (LAG Berlin-Brandenburg 14. Januar 2016 - 5 Sa 657/15 - zu B I 4 a aa

(8) (d) der Gründe). Würden die gespeicherten Verlaufsdaten nicht zumindest stichprobenartig überprüft, könnten Zuwiderhandlungen gegen das Verbot oder die Beschränkung der Privatnutzung von IT-Einrichtungen des Arbeitgebers nicht geahndet werden und könnte die Datenerhebung ihre verhaltenslenkende Wirkung nicht entfalten.

ee) Mit diesem Inhalt steht § 32 Abs. 1 BDSG im Einklang mit den Vorgaben der eine umfassende Harmonisierung (zur Begrifflichkeit EuGH 6. November 2003 - C-101/01 - [Lindqvist] Rn. 96 f., Slg. 2003, I-12971) vorsehenden Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG - ABl. L 281 vom 23. November 1995 S. 31). Einerseits wird mit dem aus dem Grundsatz der Verhältnismäßigkeit abgeleiteten Erfordernis des auf konkrete Tatsachen gestützten Anfangsverdachts einer Straftat oder anderen schweren Pflichtverletzung für besonders eingriffsintensive Maßnahmen nicht entgegen Art. 5 der Richtlinie ein zusätzlicher, die Datenerhebung erschwerender Grundsatz eingeführt oder durch eine zusätzliche Bedingung die Tragweite eines der in Art. 7 der Richtlinie vorgesehenen Grundsätze verändert (dazu EuGH 19. Oktober 2016 - C-582/14 - [Breyer] Rn. 57 ff.; 24. November 2011 - C-468/10 und C-469/10 - [ASNEF] Rn. 33, 34 und 36). Andererseits genügt der vom Senat herangezogene Verhältnismäßigkeitsgrundsatz dem durch die Richtlinie sowie Art. 7 der Charta der Grundrechte der Europäischen Union (dazu EuGH 11. Dezember 2014 - C-212/13 - [Ryneš] Rn. 28) und Art. 8 EMRK (dazu EuGH 9. November 2010 - C-92/09 und C-93/09 - [Volker und Markus Schecke] Rn. 52, Slg. 2010, I-11063; BAG 19. Februar 2015 - 8 AZR 1007/13 - Rn. 20 f.) garantierten Schutzniveau für die von einer Datenerhebung Betroffenen (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 38; EGMR 5. Oktober 2010 - 420/07 - EuGRZ 2011, 471).

ff) Bei dem (zeitlich nicht begrenzten) verdeckten Einsatz eines Keyloggers an einem Dienst-PC handelt es sich um eine Datenerhebung, die hinsichtlich der Intensität des mit ihr verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht des Betroffenen mit einer - verdeckten - Videoüberwachung am Arbeitsplatz vergleichbar ist. Zwar berührt der Einsatz eines Keyloggers grundsätzlich nicht das Recht am eigenen Bild, insbesondere ist er regelmäßig nicht geeignet, Verhaltensweisen optisch zu erfassen, die von dem Betroffenen als peinlich empfunden werden. Jedoch wird mit der Datenerhebung durch einen Keylogger massiv in das Recht des Betroffenen auf informationelle Selbstbestimmung eingegriffen. Es werden - für den Benutzer irreversibel - alle Eingaben über die Tastatur eines Computers einschließlich des Zeitpunkts der Eingabe sowie des zeitlichen Abstands zwischen zwei Eingaben erfasst und gespeichert. Die auf diese Weise gewonnenen Daten ermöglichen es, ein nahezu umfassendes und lückenloses Profil sowohl von der privaten als auch dienstlichen Nutzung durch den Betroffenen zu erstellen. Dabei werden nicht nur gespeicherte Endfassungen und ggf. Zwischenentwürfe bestimmter Dokumente sichtbar, sondern es lässt sich jeder Schritt der Arbeitsweise des Benutzers nachvollziehen. Darüber hinaus können besondere Arten personenbezogener Daten iSv. § 3 Abs. 9 BDSG oder - so im Streitfall - andere hochsensible Daten wie zB Benutzernamen, Passwörter für geschützte Bereiche, Kreditkartendaten, PIN-Nummern etc. protokolliert werden, ohne dass dies für die verfolgten Kontroll- und Überwachungszwecke erforderlich

wäre. Ebenso hat der betroffene Arbeitnehmer weder Veranlassung noch die Möglichkeit, bestimmte Inhalte als privat oder gar höchstpersönlich zu kennzeichnen und damit ggf. dem Zugriff des Arbeitgebers zu entziehen. Dieser ohnehin schon weit überschießende Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen wird noch verstärkt, wenn - wie hier - regelmäßig Screenshots gefertigt werden.

gg) Die Würdigung des Berufungsgerichts, die Beklagte habe keine Tatsachen dargelegt, die vor dem Einsatz des Keyloggers den Anfangsverdacht einer Straftat oder schweren Pflichtverletzung begründet hatten, ist revisionsrechtlich nicht zu beanstanden.

(1) Das Landesarbeitsgericht hat angenommen, die Beklagte habe lediglich einen Vorfall konkret beschrieben. Das von einer Arbeitnehmerin mitgeteilte einmalige hastige „Wegklicken" einer „stark bebilderten" Webseite sei aber nicht geeignet, den konkreten Verdacht einer exzessiven Privatnutzung des Dienst-PC zu begründen. Im Weiteren sei der Vortrag der Beklagten substanzlos geblieben. Das gelte zum einen für die einer Beweisaufnahme nicht zugängliche Behauptung, auch andere Mitarbeiter hätten angegeben, der Kläger gehe während seiner Arbeitszeit in erheblichem Umfang außerdienstlichen Aktivitäten nach. Zum anderen habe die Beklagte nicht substantiiert dargetan, dass die Leistungen des Klägers erheblich nachgelassen hätten.

(2) Diese Ausführungen lassen keinen materiellen Rechtsfehler erkennen. Die Revision zeigt auch keinen Fehler bei der Anwendung des Prozessrechts auf.

(a) Das Berufungsgericht hat es - stillschweigend - zu Recht als unmaßgeblich angesehen, dass die Beklagte die tatsächlichen Anhaltspunkte, die aus ihrer Sicht den Verdacht strafbaren Verhaltens des Klägers begründeten, nicht iSv. § 32 Abs. 1 Satz 2 BDSG dokumentiert hat. Ein solches Versäumnis führt weder zu einer Präklusion mit Vortrag zu den Verdachtsmomenten im Prozess noch begründet es für sich genommen die Unverwertbarkeit der aus der Maßnahme gewonnenen Erkenntnisse. Die Vorgabe, die Tatsachen zu dokumentieren, auf die sich ein Anfangsverdacht gründet, verfolgt den Zweck, dem hiervon erfassten Personenkreis die nachträgliche Rechtmäßigkeitskontrolle zu erleichtern. Aus ihr kann ein prozessuales Verwertungsverbot jedenfalls dann nicht abgeleitet werden, wenn der Arbeitgeber den Verdacht von Straftaten spätestens im Rechtsstreit durch konkrete Tatsachen untermauert und dadurch eine Rechtmäßigkeitskontrolle gesichert ist (BAG 20. Oktober 2016 - 2 AZR 395/15 - Rn. 33).

(b) Das Landesarbeitsgericht hat die Darlegungslast der Beklagten nicht überspannt. Auch bei vermeintlich kreativ tätigen Arbeitnehmern lässt sich anhand objektiver Tatsachen feststellen, inwieweit sie die ihnen übertragenen Aufgaben fristgerecht und entsprechend den inhaltlichen Vorgaben erledigt haben. Keinesfalls reicht es aus, sich im Rechtsstreit auf einen nicht näher begründeten Eindruck eines Vorgesetzten oder des Geschäftsführers zurückzuziehen.

(c) Die von der Beklagten erhobene Rüge, das Berufungsgericht habe sie gemäß § 139 ZPO darauf hinweisen müssen, dass ihr Vortrag zum Vorliegen eines durch

konkrete Tatsachen begründeten Anfangsverdachts unzureichend sei, ist unzulässig. Die Revision legt nicht dar, warum die Vorinstanz einem gewissenhaften und kundigen Prozessbeteiligten in der konkreten Lage des Prozesses, insbesondere nach den Einlassungen des Klägers den von ihr vermissten Hinweis hätte erteilen müssen. Überdies fehlte es nach dem eigenen Vorbringen der Beklagten an der Entscheidungserheblichkeit einer Verletzung der richterlichen Hinweispflicht. Sie räumt selbst ein, es sei ihr nicht möglich gewesen, ihr Vorbringen zu ergänzen.

e) § 28 Abs. 1 BDSG schied als Erlaubnisnorm aus. Die Vorschrift findet im Beschäftigungsverhältnis nur Anwendung, wenn nicht - wie hier - die Zwecke des § 32 Abs. 1 BDSG betroffen sind (BT-Drs. 16/13657 S. 20 f.). Demgegenüber kann eine Datenerhebung, die weder der Aufdeckung von Straftaten iSd. § 32 Abs. 1 Satz 2 BDSG noch sonstigen Zwecken des Beschäftigungsverhältnisses iSv. § 32 Abs. 1 Satz 1 BDSG dient, „zur Wahrung berechtigter Interessen" iSv. § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein (BAG 29. Juni 2017 - 2 AZR 597/16 - Rn. 25; Gola/Schomerus BDSG 12. Aufl. § 32 Rn. 2, 45 f.).

f) Es kann dahinstehen, ob Erkenntnisse, die der Arbeitgeber im Anwendungsbereich des § 32 Abs. 1 BDSG unter Verletzung des Rechts auf informationelle Selbstbestimmung gewonnen hat, ausnahmsweise im Rechtsstreit verwertet werden dürfen. Das könnte nur dann in Betracht kommen, wenn weitere, über das schlichte Beweisinteresse hinausgehende Aspekte hinzutreten und diese besonderen Umstände gerade die in Frage stehende Informationsbeschaffung als gerechtfertigt ausweisen (BAG 22. September 2016 - 2 AZR 848/15 - Rn. 24, BAGE 156, 370; 20. Juni 2013 - 2 AZR 546/12 - Rn. 29, BAGE 145, 278). Im Streitfall fehlt es schon an erstem. Ein Arbeitgeber, der - wie hier die Beklagte - eine Überwachungsmaßnahme „ins Blaue hinein" veranlasst, befindet sich weder in einer Notwehr- oder notwehrähnlichen Situation gemäß § 227 BGB bzw. § 32 StGB noch in einer Notstandslage iSv. § 34 StGB (dazu BAG 13. Dezember 2007 - 2 AZR 537/06 - Rn. 36; BGH 15. Mai 2013 - XII ZB 107/08 - Rn. 23 f.).

4. Das Landesarbeitsgericht hat zu Recht angenommen, die Kündigungen seien auch als Verdachtskündigungen unwirksam. Es musste den Sachvortrag der Beklagten, mit dem sie die durch den Keylogger gewonnenen Erkenntnisse in den Rechtsstreit eingeführt hat, auch bei der Würdigung außer Acht lassen, ob gegen den Kläger der dringende Verdacht eines Verhaltens bestand, das, wäre es erwiesen, eine außerordentliche, fristlose Kündigung gerechtfertigt hätte (dazu, dass dies auch für eine ordentliche Verdachtskündigung erforderlich ist, BAG 18. Juni 2015 - 2 AZR 256/14 - Rn. 22).

(…)

2 BAG: Pflicht zur Teilnahme an einem elektronischen Warn- und Berichtssystem

BAG, 17.11.2016, 2 AZR 730/15

Orientierungssatz

1. Zur außerordentlichen Kündigung eines Busfahrers wegen Verweigerung der Teilnahme an einem elektronischen Warn- und Berichtssystems (RIBAS-Informationssystem) nach § 20 Abs 6 des Spartentarifvertrags Nahverkehr Nordrhein-Westfalen (TV-N NW) vom 25. Mai 2001 i.V.m. § 626 Abs 1 BGB.

2. Regelt eine Betriebsvereinbarung eine nach § 32 Abs 1 S 1 BDSG zulässige Verarbeitung von personenbezogenen Daten von Beschäftigten, so ist diese durch eine Rechtsvorschrift i.S.d. § 4 Abs 1 BDSG erlaubt. Es bedarf in diesem Fall keiner Entscheidung, ob auch allein die Regelungen einer Betriebsvereinbarung eine die Datenerhebung, -verarbeitung oder -nutzung gestattende Rechtsvorschrift i.S.d. § 4 Abs 1 BDSG sein können.

3. Nach Beendigung des Arbeitsverhältnisses kann ein Anspruch auf Entfernung von Abmahnungen nach §§ 242, 1004 Abs 1 S 1 BGB nur dann bestehen, wenn es objektive Anhaltspunkte dafür gibt, dass die Abmahnung dem Arbeitnehmer noch schaden kann.

Tatbestand

Die Parteien streiten über die Wirksamkeit einer außerordentlichen Kündigung mit Auslauffrist sowie die Entfernung von Abmahnungen aus der Personalakte des Klägers.

Die Beklagte betreibt öffentlichen Nahverkehr. Der Kläger war bei ihr seit Oktober 1989 als Busfahrer beschäftigt. Auf das Arbeitsverhältnis fand aufgrund arbeitsvertraglicher Bezugnahme der Spartentarifvertrag für Nahverkehrsbetriebe (TV-N NW) vom 25. Mai 2001 Anwendung. Nach dessen § 20 Abs. 6 Unterabs. 1 kann das Arbeitsverhältnis nach einer Betriebszugehörigkeit von mehr als 15 Jahren durch den Arbeitgeber nur noch „aus einem wichtigen Grund (§ 626 Abs. 1 BGB)" gekündigt werden.

Die Beklagte schloss mit ihrem Betriebsrat im Jahre 2014 eine Betriebsvereinbarung über den Einsatz des sog. RIBAS-Systems (BV) auf ihren Fahrzeugen. Dieses wertet elektronisch Fahrereignisse aus und informiert die Busfahrer durch eine Warnleuchte über hochtouriges Fahren, Leerlaufzeitüberschreitungen, scharfes Bremsen, überhöhte Beschleunigung und Geschwindigkeitsüberschreitungen. Die Daten werden aufgezeichnet und gespeichert.

Nach der BV sind alle Fahrer zur Teilnahme am RIBAS-System verpflichtet. Fahrer, die nicht an dem vorgesehenen personalisierten Berichts- und Prämiensystem teilnehmen wollen, erhalten einen anonymisierten Systemschlüssel. Aufgrund von Einwendungen des Landesdatenschutzbeauftragten hatten die Betriebsparteien die BV entsprechend angepasst.

Der Kläger stimmte einer Teilnahme am personalisierten Berichts- und Prämiensystem nicht zu. Ihm wurde Ende August 2014 der anonymisierte RIBAS-Schlüssel zur Nutzung übergeben. Das entsprechende Empfangsbekenntnis sandte er nicht zurück. In einem von der Beklagten veranlassten Gespräch Mitte Oktober 2014 teilte er mit, er habe seinen Teamleiter so verstanden, dass er wählen könne, ob er - überhaupt - an dem System teilnehme.

Ende Oktober 2014 führten der Fachbereichsleiter Personal und der Leiter des Omnibusbetriebs ein weiteres Gespräch mit dem Kläger. Sie erläuterten ihm das RIBAS-System und wiesen auf die Beteiligung des Landesdatenschutzbeauftragten hin. Der Kläger wurde aufgefordert, den anonymisierten RIBAS-Schlüssel ab sofort zu verwenden. Dem kam er auch nach einer entsprechenden Schulung nicht nach. Die Beklagte mahnte den Kläger deshalb im Dezember 2014 ab und wies ihn darauf hin, dass er sich zur Vermeidung arbeitsrechtlicher Konsequenzen vor jeder Fahrt im System anzumelden habe.

Eine erneute Einweisung in das System lehnte der Kläger ab. Er nutzte seinen RIBAS-Schlüssel im Januar 2015 an sechs Arbeitstagen, an elf Arbeitstagen wiederum nicht. Ende Januar 2015 führte der Kläger ein Gespräch mit seinem Teamleiter. Diesem erklärte er, sich zu der Angelegenheit nicht mehr äußern und sie gerichtlich klären lassen zu wollen.

Anfang Februar 2015 erteilte die Beklagte dem Kläger eine weitere Abmahnung. Bei der Übergabe des Schreibens wies sie den Kläger darauf hin, sie erwarte - unabhängig von seiner Ankündigung, eine gerichtliche Klärung herbeizuführen - die Einhaltung des in der BV geregelten Verfahrens. Der Kläger setzte den RIBAS-Schlüssel weiterhin nicht ein. Die Beklagte erteilte ihm deshalb unter dem 26. Februar 2015 eine dritte Abmahnung und forderte ihn noch einmal eindringlich auf, sich vor jedem Dienstantritt im System anzumelden. Beide Schreiben gingen dem Kläger am 4. März 2015 zu. Am 5. und am 6. März 2015 meldete er sich erneut nicht im System an.

Die Beklagte hörte den Betriebsrat mit Schreiben vom 10. März 2015 zu ihrer Absicht an, das Arbeitsverhältnis der Parteien außerordentlich fristlos, hilfsweise außerordentlich mit einer sozialen Auslauffrist von sechs Monaten zum Schluss eines Kalendervierteljahres zu kündigen. Der Betriebsrat erklärte am Folgetag seine Zustimmung zu den beabsichtigten Kündigungen.

Mit Schreiben vom 12. März 2015, das dem Kläger am selben Tag zuging, kündigte die Beklagte das Arbeitsverhältnis der Parteien außerordentlich zum 13. März 2015, hilfsweise außerordentlich mit Auslauffrist zum 30. September 2015.

Dagegen hat sich der Kläger rechtzeitig mit der vorliegenden Kündigungsschutzklage gewandt. Er hat gemeint, ein wichtiger Grund zur außerordentlichen Kündigung liege nicht vor. Er sei nicht zur Teilnahme am RIBAS-System verpflichtet gewesen. Die BV sei unwirksam. Er habe nicht schuldhaft gehandelt, sondern sich in einem gut begründeten und vertretbaren Verbotsirrtum befunden. Der Lauf der Frist des § 626 Abs. 2 BGB habe überdies bereits mit seiner Erklärung begonnen, den Schlüssel bis zu einer gerichtlichen Klärung nicht zu bedienen. Die ausgesprochenen Abmahnungen seien zu Unrecht erfolgt und aus seiner Personalakte zu entfernen.

Der Kläger hat beantragt,

1. die Beklagte zu verurteilen, die Abmahnungen vom 18. Dezember 2014, 5. Februar 2015 und 26. Februar 2015 aus der Personalakte zu entfernen;
2. festzustellen, dass das Arbeitsverhältnis zwischen den Parteien nicht durch die Kündigung vom 12. März 2015 aufgelöst worden ist.

Die Beklagte hat beantragt, die Klage abzuweisen. Sie hat die Auffassung vertreten, der Kläger sei zur Nutzung des anonymisierten RIBAS-Schlüssels verpflichtet gewesen. Gegen diese Pflicht habe er beharrlich verstoßen. Seine Weigerung habe es ihr unzumutbar gemacht, ihn weiter zu beschäftigen.

Das Arbeitsgericht hat der Klage stattgegeben. Das Landesarbeitsgericht hat festgestellt, dass die außerordentliche, fristlose Kündigung das Arbeitsverhältnis der Parteien nicht aufgelöst hat. Im Übrigen hat es die Klage abgewiesen. Mit seiner Revision begehrt der Kläger die Wiederherstellung der erstinstanzlichen Entscheidung.

Entscheidungsgründe

Die Revision ist unbegründet. Das Landesarbeitsgericht hat sein Urteil ordnungsgemäß verkündet (I.) und die außerordentliche Kündigung mit Auslauffrist zu Recht als wirksam angesehen (II.). Ein Anspruch des Klägers auf Entfernung der ihm erteilten Abmahnungen aus der Personalakte besteht nicht (III.).

(…)

II. Die Würdigung des Landesarbeitsgerichts, für die außerordentliche Kündigung mit sozialer Auslauffrist habe ein wichtiger Grund iSd. § 20 Abs. 6 Unterabs. 1 TV-N NW, § 626 Abs. 1 BGB vorgelegen, hält einer revisionsrechtlichen Überprüfung stand.

1. Nach dem kraft einzelvertraglicher Bezugnahme anwendbaren § 20 Abs. 6 Unterabs. 1 TV-N NW konnte das Arbeitsverhältnis der Parteien durch die Beklagte nur noch aus wichtigem Grund iSd. § 626 Abs. 1 BGB gekündigt werden. Der Kläger war im Zeitpunkt der Kündigung weit mehr als 15 Jahre beschäftigt.

2. Die Tarifbestimmung verweist im Zusammenhang mit dem Begriff des wichtigen Grundes auf die Regelung des § 626 Abs. 1 BGB. Deren Verständnis ist deshalb auch für die Auslegung der Tarifnorm maßgebend (vgl. BAG 13. Mai 2015 - 2 AZR 531/14 - Rn. 26; 31. Juli 2014 - 2 AZR 407/13 - Rn. 23). Nach § 626 Abs. 1 BGB kann das Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung der Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung nicht zugemutet werden kann.

a) Dafür ist zunächst zu prüfen, ob der Sachverhalt ohne seine besonderen Umstände „an sich", dh. typischerweise als wichtiger Grund geeignet ist. Alsdann bedarf es der

Prüfung, ob dem Kündigenden die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Falls und unter Abwägung der Interessen beider Vertragsteile jedenfalls bis zum Ablauf der Kündigungsfrist zumutbar ist oder nicht (BAG 13. Mai 2015 - 2 AZR 531/14 - Rn. 28; 31. Juli 2014 - 2 AZR 407/13 - Rn. 25). Ein wichtiger Grund iSd. § 626 Abs. 1 BGB liegt auch im Verhältnis zu einem Arbeitnehmer, dessen Arbeitsverhältnis ordentlich nicht gekündigt werden kann, dann vor, wenn es dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls - objektiv - nicht zuzumuten ist, den Arbeitnehmer auch nur bis zum Ablauf der (fiktiven) ordentlichen Kündigungsfrist weiter zu beschäftigen. In diesem Fall wäre eine außerordentliche Kündigung auch dann gerechtfertigt, wenn die ordentliche Kündigung nicht ausgeschlossen wäre (BAG 13. Mai 2015 - 2 AZR 531/14 - Rn. 42).

b) Darüber hinaus kann ein pflichtwidriges Verhalten, das bei einem Arbeitnehmer ohne Sonderkündigungsschutz nur eine ordentliche Kündigung rechtfertigen würde, unter Umständen gerade wegen der infolge des Ausschlusses der ordentlichen Kündigung langen Bindungsdauer ebenfalls einen wichtigen Grund iSd. § 626 Abs. 1 BGB zur außerordentlichen Kündigung durch den Arbeitgeber darstellen. Zwar wirkt sich der Sonderkündigungsschutz insofern zum Nachteil für den Arbeitnehmer aus. Dies ist jedoch im Begriff des wichtigen Grundes gem. § 626 Abs. 1 BGB angelegt. Dieser richtet sich nach der Zumutbarkeit einer Fortsetzung des Dienstverhältnisses bis zum Ablauf der Kündigungsfrist oder der vereinbarten Beendigung des Dienstverhältnisses. Zur Vermeidung eines Wertungswiderspruchs muss in einem solchen Fall allerdings zugunsten des Arbeitnehmers zwingend eine der fiktiven ordentlichen Kündigungsfrist entsprechende Auslauffrist eingehalten werden. Der Arbeitnehmer, dessen Arbeitsverhältnis vom Arbeitgeber ordentlich nicht gekündigt werden kann, darf im Ergebnis nicht schlechter gestellt sein, als wenn er dem Sonderkündigungsschutz nicht unterfiele (BAG 13. Mai 2015 - 2 AZR 531/14 - Rn. 44; 15. November 2001 - 2 AZR 605/00 - zu II 5 a, b der Gründe, BAGE 99, 331).

3. Von diesen Grundsätzen ist auch das Landesarbeitsgericht ausgegangen und hat sie ohne Rechtsfehler auf den Streitfall angewandt.

a) Der Kläger hat es wiederholt vorsätzlich unterlassen, den für Fahrer, die nicht an dem personalisierten System teilnehmen, vorgesehenen anonymisierten RIBAS-Schlüssel zu verwenden. Er hat dadurch beharrlich seine arbeitsvertragliche Leistungspflicht verletzt. Dies ist „an sich" geeignet, einen wichtigen Grund für eine außerordentliche Kündigung iSd. § 626 Abs. 1 BGB zu bilden.

aa) Die Pflicht zur Verwendung des Schlüssels folgt aus § 77 Abs. 4 Satz 1 BetrVG iVm. § 4 BV. Nach § 4 Abs. 1 BV ist die Anmeldung eines jeden Fahrers an das RIBAS-System „zwingend erforderlich". Gem. § 4 Abs. 2 Satz 4 BV bleibt die „Pflicht zur generellen Teilnahme am System" bestehen, auch wenn der Fahrer seine Zustimmung zur Datenerhebung im personalisierten System nicht erteilt. Dafür erhält der Fahrer nach § 4 Abs. 2 Satz 2 BV einen anonymisierten Schlüssel.

bb) Die gem. § 77 Abs. 4 Satz 1 BetrVG auch für den Kläger begründete Pflicht zur Teilnahme am RIBAS-System steht mit höherrangigem Recht im Einklang. Sie

verletzt insbesondere nicht § 75 Abs. 2 Satz 1 BetrVG iVm. Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG.

(1) Zu dem durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrecht gehört das Recht auf informationelle Selbstbestimmung. Dieses garantiert die Befugnis, selbst über die Preisgabe und Verwendung persönlicher Daten zu befinden (BVerfG 11. März 2008 - 1 BvR 2074/05 ua. - BVerfGE 120, 378; BAG 21. November 2013 - 2 AZR 797/11 - Rn. 45, BAGE 146, 303). Der Achtung dieses Rechts dient zudem Art. 8 Abs. 1 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) (BAG 21. November 2013 - 2 AZR 797/11 - aaO; BGH 15. Mai 2013 - XII ZB 107/08 - Rn. 14). Die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) über die Anforderungen an eine zulässige Datenverarbeitung konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung. Sie regeln, in welchem Umfang im Anwendungsbereich des Gesetzes Eingriffe durch öffentliche oder nichtöffentliche Stellen iSd. § 1 Abs. 2 BDSG in diese Rechtspositionen zulässig sind (vgl. BAG 21. November 2013 - 2 AZR 797/11 - aaO).

(2) Danach ist das Recht des Klägers auf informationelle Selbstbestimmung durch die in § 4 BV begründete Verpflichtung, zumindest mithilfe des anonymisierten Schlüssels am RIBAS-System teilzunehmen, nicht verletzt. Zwar hat der Kläger in die damit verbundene Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht iSd. § 4 Abs. 1 BDSG eingewilligt. Diese ist aber gem. § 32 Abs. 1 Satz 1 BDSG und damit durch eine Rechtsvorschrift iSd. § 4 Abs. 1 BDSG gerechtfertigt. Es bedarf demnach keiner Entscheidung, ob auch allein die Regelungen der BV eine die Datenerhebung, -verarbeitung oder -nutzung gestattende Rechtsvorschrift iSd. § 4 Abs. 1 BDSG sein können.

(a) Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses ua. dann erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung erforderlich ist. Um personenbezogene Daten iSd. § 3 Abs. 1 BDSG handelt es sich auch bei einer zunächst anonymisierten Erhebung, Verarbeitung oder Nutzung, wenn die Anonymisierung ohne unangemessenen Aufwand aufgehoben werden kann. Es genügt, wie ein Umkehrschluss aus § 3 Abs. 6 BDSG ergibt, dass die betroffene Person ohne besondere Schwierigkeiten bestimmbar ist (Gola/Schomerus BDSG 12. Aufl. § 3 Rn. 10; Simitis/Dammann BDSG 8. Aufl. § 3 Rn. 23; Plath/Schreiber BDSG § 3 Rn. 15; Erbs/Kohlhaas Strafrechtliche Nebengesetze Stand 2015 § 3 BDSG Rn. 3; zum Begriff der personenbezogenen Daten iSd. RL 95/46/EG EuGH 19. Oktober 2016 - C-582/14 - Rn. 49). So liegt der Fall hier. Nach den Feststellungen des Landesarbeitsgerichts kann der Anonymisierungsschutz im RIBAS-System im Grundsatz ohne großen Aufwand durch Hinzuziehung der Dienstpläne aufgehoben werden. Eine entsprechende Personalisierung ist auch - in Abstimmung mit dem Betriebsrat - nach § 10 Satz 3 BV zur Ermittlung von Schulungsbedarf vorgesehen, sofern im anonymisierten Fahrdatenbestand erhebliche Überschreitungen der Grenzwerte im Vergleich zu durchschnittlichen Ergebnissen erkennbar werden.

(b) § 32 Abs. 1 Satz 1 BDSG kodifiziert die von der Rechtsprechung aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1

iVm. Art. 1 Abs. 1 GG) abgeleiteten allgemeinen Grundsätze zum Datenschutz im Beschäftigungsverhältnis (BT-Drs. 16/13657 S. 21). Dabei nimmt die Gesetzesbegründung zur Konkretisierung des Maßstabs der Erforderlichkeit einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses auf die Entscheidungen des Bundesarbeitsgerichts vom 22. Oktober 1986 (- 5 AZR 660/85 -) und 7. September 1995 (- 8 AZR 828/93 -) Bezug. Diesen zufolge dürfe sich der Arbeitgeber bei seinen Beschäftigten nicht nur über Umstände informieren oder Daten verwenden, um seine vertraglichen Pflichten ihnen gegenüber erfüllen zu können, wie zB Pflichten im Zusammenhang mit der Personalverwaltung, Lohn- und Gehaltsabrechnung, sondern auch, um seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte wahrzunehmen, zB durch Ausübung des Weisungsrechts oder durch Kontrollen der Leistung oder des Verhaltens des Beschäftigten (BT-Drs. 16/13657 aaO).

(c) Erforderlichkeit iSd. § 32 Abs. 1 Satz 1 BDSG setzt damit ein berechtigtes Interesse des Arbeitgebers an der Datenerhebung, -verarbeitung oder -nutzung voraus, das aus dem bestehenden Arbeitsverhältnis herrühren muss. Es muss ein Zusammenhang mit der Erfüllung der vom Arbeitnehmer geschuldeten vertraglichen Leistung, seiner sonstigen Pflichtenbindung oder mit der Pflichtenbindung des Arbeitgebers bestehen (BAG 7. September 1995 - 8 AZR 828/93 - zu II 2 c aa der Gründe, BAGE 81, 15). Die Datenerhebung, -verarbeitung oder -nutzung darf ferner keine übermäßige Belastung für den Arbeitnehmer darstellen. Sie muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Greift eine Maßnahme in das allgemeine Persönlichkeitsrecht des Arbeitnehmers ein, muss der Eingriff einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten (BAG 7. September 1995 - 8 AZR 828/93 - zu II 2 c bb der Gründe, aaO; 22. Oktober 1986 - 5 AZR 660/85 - zu B I 2 a der Gründe, BAGE 53, 226). Dieser verlangt, dass der Eingriff geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (BAG 15. April 2014 - 1 ABR 2/13 (B) - Rn. 41, BAGE 148, 26; 29. Juni 2004 - 1 ABR 21/03 - zu B I 2 d der Gründe, BAGE 111, 173). Es dürfen keine anderen, zur Zielerreichung gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkenden Mittel zur Verfügung stehen. Die Verhältnismäßigkeit im engeren Sinne ist gewahrt, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (BVerfG 4. April 2006 - 1 BvR 518/02 - zu B I 2 b dd der Gründe, BVerfGE 115, 320; BAG 15. April 2014 - 1 ABR 2/13 (B) - aaO).

(d) Danach hat das Landesarbeitsgericht zu Recht angenommen, die Verpflichtung des Klägers, zumindest mit dem anonymisierten Schlüssel am RIBAS-System teilzunehmen, greife nicht unverhältnismäßig in sein Recht auf informationelle Selbstbestimmung ein. Dies gilt auch dann, wenn die Betriebsparteien hinsichtlich Eignung und Erforderlichkeit des Eingriffs entgegen der Auffassung des Landesarbeitsgerichts (ebenso BAG 29. Juni 2004 - 1 ABR 21/03 - zu B I 2 d aa und bb der Gründe, BAGE 111, 173) nicht über einen vergleichbaren Beurteilungsspielraum wie der Gesetzgeber verfügen.

(aa) Das berechtigte Interesse der Beklagten an der Verwendung des RIBAS-Systems besteht darin, dass die bei ihr beschäftigten Busfahrer zu einer vorausschauenden und sparsamen Fahrweise angehalten werden sollen (§ 2 BV). Das betrifft unmittelbar die von ihnen geschuldete Arbeitsleistung und damit die Durchführung des Beschäftigungsverhältnisses iSd. § 32 Abs. 1 Satz 1 BDSG. Die verfolgten Ziele einer Reduzierung des Kraftstoffverbrauchs sowie einer Steigerung der Kundenzufriedenheit sind, wie das Landesarbeitsgericht zutreffend erkannt hat, nicht unbillig oder unrechtmäßig, sondern ökonomisch vernünftig und liegen zudem im ökologischen Interesse der Allgemeinheit. Das System hält die Busfahrer nicht, wie die Revision meint, in Bezug auf ihr Bremsverhalten zu einem straßenverkehrswidrigen Verhalten an. Dass es darauf hinweist und es aufzeichnet, wenn ein Fahrer scharf gebremst hat, heißt nicht, er solle auch dann nicht entsprechend reagieren, wenn die Verkehrssituation es erfordert.

(bb) Die Teilnahme der Busfahrer am RIBAS-System ist zur Erreichung dieser Ziele geeignet. Das Landesarbeitsgericht verweist zu Recht darauf, dass das System sowohl die Selbstkontrolle fördert als auch Erkenntnisse über einen etwaigen Schulungsbedarf aufgrund des Vergleichs von Fahrleistungen mit den durchschnittlichen Grenzwerten ermöglicht.

(cc) Zur Erreichung der verfolgten Ziele ist die Teilnahme aller Busfahrer, auch die des Klägers, erforderlich. Das RIBAS-System soll Durchschnittswerte ermitteln und bei erheblichen Abweichungen einen hierdurch begründeten konkreten Schulungsbedarf identifizieren. Dafür müssen alle Busfahrer - zumindest anonymisiert - daran teilnehmen. Dem trägt die nach § 4 Abs. 1 BV vorgesehene, für alle Busfahrer verpflichtende Teilnahme am System Rechnung. Ein anderes gleichermaßen geeignetes und der Beklagten zumutbares, das informationelle Selbstbestimmungsrecht des Klägers weniger berührendes Mittel ist nicht ersichtlich. So wäre eine ausschließlich freiwillige Teilnahme oder die Beschränkung auf eine elektronische Signalgebung unmittelbar im Anschluss an ein Fahrmanöver ohne eine weitere Speicherung der Daten zur Ermittlung von Schulungsbedarf nicht ausreichend. Durch ein Mitfahren von Fahrtrainern mag zwar Schulungsbedarf identifiziert werden können. Es ersetzte aber nicht den Erkenntnisgewinn durch die Ermittlung der Durchschnittswerte aller Fahrer und regte auch nicht in gleicher Weise zur Selbstkontrolle des Fahrverhaltens an wie das RIBAS-System. Ausschließlich vorbeugende Schulungen hätten diesen Effekt ebenso wenig. Der Einwand des Klägers, eine Ausrüstung der Busse mit technischen „Begrenzungsmechanismen" betreffend „Verzögerung, Drehzahl und Geschwindigkeit" wäre eine mildere, ebenso effektive Möglichkeit gewesen, lässt nicht erkennen, dass dadurch in gleich geeigneter Weise wie durch das RIBAS-System eine vorausschauende und sparsame Fahrweise gefördert werden könnte. Der Kläger macht nicht mit einer Verfahrensrüge geltend, hierzu bereits in den Vorinstanzen vorgetragen zu haben. Entsprechendes gilt für seine Behauptung, es wäre auch eine Kombination aus den von ihm benannten alternativen Maßnahmen möglich gewesen.

(dd) Die Verhältnismäßigkeit im engeren Sinne ist gewahrt. Die Beeinträchtigung des informationellen Selbstbestimmungsrechts des Klägers steht nicht außer Verhältnis zu den von der Beklagten legitimerweise verfolgten Interessen. Es liegt keine Dauerüberwachung in dem Sinne vor, dass die Busfahrer - wie bei einer

Videoüberwachung - in ihrem gesamten Verhalten während der Arbeitszeit kontrolliert würden. Gespeichert werden allein die Daten zu den fraglichen Fahrmanövern und dies im Grundsatz auch nur zur Ermittlung der Durchschnittswerte. Dem einzelnen Fahrer zugeordnet werden die Daten lediglich dann, wenn er dem zugestimmt hat oder es in seiner Fahrleistung erhebliche Abweichungen vom Durchschnitt gibt. Dadurch ermöglicht das System in erster Linie eine Selbstkontrolle der Busfahrer. Eine personalisierte Leistungskontrolle ist dagegen, wenn der Fahrer ihr nicht durch Teilnahme am Prämiensystem zugestimmt hat, nur aus gegebenem Anlass und ausschließlich zur Ermittlung von Schulungsbedarf zulässig. Ob im Einzelfall die Voraussetzungen für eine Personalisierung gegeben wären, ist dabei nach § 10 Satz 3 BV in Abstimmung mit dem Betriebsrat festzustellen und unterläge ggf. gesonderter Überprüfung. Die Vorgabe, die Personalisierung dürfe nur bei einer erheblichen Überschreitung der Grenzwerte erfolgen, trägt dem Maßstab des § 32 Abs. 1 Satz 1 BDSG im Grundsatz hinreichend Rechnung. Zudem ordnet § 11 BV an, dass die Bestimmungen des BDSG einzuhalten sind. Daraus folgt nicht etwa eine besondere Missbrauchsgefahr, wie die Revision zu Bedenken gibt, sondern die Garantie eines Schutzstandards entsprechend dem Gesetz. In Bezug genommen sind damit insbesondere auch die Verantwortung der Beklagten für eine Auftragsdatenverarbeitung nach § 11 BDSG sowie die Ansprüche auf Löschung oder Sperrung von Daten gem. § 35 BDSG.

cc) Die den Inhalt der von ihm zu erbringenden Arbeitsleistung als Busfahrer ausgestaltende Pflicht zur Teilnahme am RIBAS-System hat der Kläger beharrlich und vorsätzlich verletzt. Er ist seiner Verpflichtung, sich im System anzumelden, wiederholt nicht nachgekommen, obwohl er von der Beklagten mehrfach darauf hingewiesen wurde, dass dies für eine ordnungsgemäße Vertragserfüllung unerlässlich sei. Der Kläger hat es bewusst in Kauf genommen, dadurch nachhaltig seine arbeitsvertraglichen Leistungspflichten zu verletzen. Er unterlag insofern keinem unverschuldeten Rechtsirrtum.

(1) Der Geltungsanspruch des Rechts bewirkt, dass der Schuldner das Risiko eines Rechtsirrtums grundsätzlich selbst trägt und es nicht dem Gläubiger überbürden kann (BAG 22. Oktober 2015 - 2 AZR 569/14 - Rn. 43, BAGE 153, 111; 19. August 2015 - 5 AZR 975/13 - Rn. 31, BAGE 152, 213). Ein unverschuldeter Rechtsirrtum liegt nur vor, wenn der Schuldner seinen Irrtum auch unter Anwendung der zu beachtenden Sorgfalt nicht erkennen konnte. Dabei sind strenge Maßstäbe anzulegen. Es reicht nicht aus, dass er sich für seine eigene Rechtsauffassung auf eine eigene Prüfung und fachkundige Beratung stützen kann. Ein Unterliegen in einem möglichen Rechtsstreit muss zwar nicht undenkbar sein (BAG 12. November 1992 - 8 AZR 503/91 - zu I 1 der Gründe, BAGE 71, 350). Gleichwohl liegt ein entschuldbarer Rechtsirrtum nur dann vor, wenn der Schuldner damit nach sorgfältiger Prüfung der Sach- und Rechtslage nicht zu rechnen brauchte; ein normales Prozessrisiko entlastet ihn nicht (BAG 22. Oktober 2015 - 2 AZR 569/14 - aaO; 29. August 2013 - 2 AZR 273/12 - Rn. 34; BGH 6. Dezember 2006 - IV ZR 34/05 - zu II 1 a aa der Gründe; 27. September 1989 - IVa ZR 156/88 -).

(2) Hier hat der Kläger das Risiko, mit seiner Einschätzung falsch liegen zu können, nicht verkannt. Er hat lediglich gemeint, die Teilnahme am RIBAS-System zumindest so lange verweigern zu können, bis die Rechtslage durch die Gerichte geklärt sei.

Damit hat er es bewusst darauf ankommen lassen, sich pflichtwidrig zu verhalten. Die Beklagte hatte ihn mehrfach auf ihre Sichtweise hingewiesen sowie darauf, dass der Landesdatenschutzbeauftragte in die Ausgestaltung der BV einbezogen gewesen war. Für den Kläger stritt auch nicht etwa eine höchstrichterliche Entscheidung in einem vergleichbaren Fall (zu einer solchen Konstellation BAG 19. August 2015 - 5 AZR 975/13 - Rn. 31 f., BAGE 152, 213). Unerheblich ist, ob er mit seinem Vorbringen, einen Rechtsanwalt um Rechtsauskunft gebeten zu haben, in der Revision noch gehört werden könnte. Selbst dies zu Gunsten des Klägers unterstellt, läge kein unverschuldeter Rechtsirrtum vor. Der Kläger behauptet insbesondere nicht, der Rechtsanwalt habe ihn dahingehend beraten, es bestehe kein Risiko für eine andere rechtliche Bewertung durch die Gerichte.

b) Die Interessenabwägung des Landesarbeitsgerichts ist revisionsrechtlich nicht zu beanstanden.

(…)

4. Die Beklagte hat die Kündigungserklärungsfrist gem. § 626 Abs. 2 BGB gewahrt. Grund für die Kündigung war, dass der Kläger sich wiederholt nicht im RIBAS-System angemeldet hatte. Zuletzt war dies am 5. und 6. März 2015 der Fall gewesen. Die Kündigung ging dem Kläger am 12. März 2015 und damit innerhalb von zwei Wochen zu.

III. Der Kläger hat keinen Anspruch aus §§ 242, 1004 Abs. 1 Satz 1 BGB auf Entfernung der Abmahnungen vom 18. Dezember 2014, 5. Februar 2015 und 26. Februar 2015 aus seiner Personalakte. Ein Anspruch auf Löschung von in den Abmahnungen enthaltenen personenbezogenen Daten nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG, weil deren Kenntnis zur Erfüllung der Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sei, hat der Kläger nicht geltend gemacht.

1. Nach Beendigung des Arbeitsverhältnisses kann ein Anspruch auf Entfernung von Abmahnungen nach §§ 242, 1004 Abs. 1 Satz 1 BGB nur dann bestehen, wenn es objektive Anhaltspunkte dafür gibt, dass die Abmahnung dem Arbeitnehmer noch schaden kann (BAG 19. April 2012 - 2 AZR 233/11 - Rn. 51). Dafür hat der Kläger nach den Feststellungen des Landesarbeitsgerichts keine Tatsachen vorgetragen. Eine Verfahrensrüge erhebt er insoweit nicht.

2. Aus der Entscheidung des Bundesarbeitsgerichts vom 16. November 2010 (- 9 AZR 573/09 - BAGE 136, 156) ergibt sich kein anderer Maßstab. Dies hat das Landesarbeitsgericht zutreffend erkannt. Auch danach ist das Recht auf Einsicht in die Personalakte von der Frage zu trennen, unter welchen Voraussetzungen ein Anspruch darauf besteht, bestimmte Inhalte daraus entfernen zu lassen (BAG 16. November 2010 - 9 AZR 573/09 - Rn. 42, aaO).

IV. Als unterlegene Partei hat der Kläger gem. § 97 Abs. 1 ZPO die Kosten des Revisionsverfahrens zu tragen.

3 LAG Köln, Arbeitszeitbetrug am Heimarbeitsplatz - elektronische Überwachung

Landesarbeitsgericht Köln, 29.09.2014, 2 Sa 181/14

Leitsatz

Ergibt die Auswertung der elektronisch gespeicherten Arbeitsvorgänge, dass innerhalb von 10 Arbeitstagen mehrere Stunden Arbeitszeit zu viel in die manuell geführte Arbeitszeiterfassung eingetragen wurden, kann dies eine außerordentliche Kündigung ohne Abmahnung rechtfertigen.

Das Speichern des Bearbeiters und des letzten Änderungsdatums einer Datei verstößt nicht gegen das BDSchG, wenn die Speicherung erforderlich ist, um bei einer online-Datenbank überprüfen zu können, wer wann welche Eingaben gemacht hat. Es ist das berechtigte Interesse des Arbeitgebers, Fehleingaben, die zu erheblichen Schäden bei den Nutzern der Datenbank führen können, dem jeweiligen Sachbearbeiter zuordnen zu können, sowie den aktuellen Bearbeitungsstand feststellen zu können.

Gründe

Tatbestand

Die Parteien streiten um die Wirksamkeit einer außerordentlichen Kündigung vom 18.01.2013, einer ordentlichen Kündigung vom 30.01.2013 zum 30.06.2013 sowie um Vergütungsansprüche aus Annahmeverzug.

Die am 1958, geborene, verheiratete Klägerin ist seit dem 01.07.1998 bei der Beklagten, die ausschließlich der Auszubildenden mehr als 10 Arbeitnehmer beschäftigt, als Bürokraft tätig. Die Beklagte pflegt eine Krankenhausdatenbank, in der die öffentlich rechtlich genehmigten Entgeltvereinbarungen der Krankenhäuser eingegeben werden. Diese Eingabearbeiten gehörten zu den wesentlichen Tätigkeiten der Klägerin. Einzugeben war jeweils der Schlüssel (eine Zeichenfolge) für das betreffende Krankenhaus, der Schlüssel (ebenfalls eine Zeichenfolge) für die betroffene Leistung des Krankenhauses und der hierzu vereinbarte Entgeltsatz.

Zuletzt arbeitete die Klägerin aufgrund besonderer Vereinbarung über Telearbeit an 3 Wochentagen von zuhause aus.

Als die Klägerin Freizeitausgleich zum Abbau von Überstunden beantragte, nahm die Beklagte eine Überprüfung der Arbeitszeiten der Klägerin vor, weil die Überstunden nicht während der Arbeitstage im Büro angefallen waren. Die häuslichen Arbeitszeiten trug die Klägerin manuell in die von der Beklagten geführte Arbeitszeitdatei ein.

Am 04.12.2012 erfolgte ein erstes Gespräch mit der Klägerin. Die Klägerin schilderte, dass sie zuhause nicht immer zu den Zeiten, in denen nach der Gleitzeitordnung Arbeitszeit zulässig war, arbeitete. Die gegenüber der Beklagten angegebene Menge der Arbeitsstunden entspräche aber einer von der Klägerin zuhause geführten Excel-Tabelle. Diese übermittelte die Klägerin mit Mail vom 05.12.2012. Am 13.12.2012 fand ein zweites Gespräch mit der Klägerin statt. Hierbei erläuterte sie, dass sie die

zuhause gearbeiteten Stunden nicht 1 : 1, also in gleicher Menge in die betriebliche Arbeitszeitauswertung eingebe, wie sie am konkreten Arbeitstag angefallen seien, sondern dass sie nach ihrem persönlichen Bedarf zuhause Überstunden speichere und gegebenenfalls einen positiven Saldo nach ihren persönlichen Bedürfnissen in die betriebliche Arbeitszeitdatei eingebe, um dann zeitnah Überstundenausgleich zu erhalten.

Die Beklagte wertete danach die elektronisch gespeicherten Eingabezeiten für die häuslichen Dateneingaben in die Krankenhausentgeltvereinbarungsdatei aus. Sie kam dabei zu dem Ergebnis, dass die Klägerin in der Zeit vom 05.11. bis 16.11.2012 50,56 Stunden in die betriebliche Arbeitszeitliste eingegeben hatte, dass die Klägerin nach eigener Tabelle 43,26 Stunden gearbeitet hatte, dass die Zeitstempel der elektronischen Auswertung der vom häuslichen Arbeitsplatz getätigten Dateneingaben jedoch lediglich eine Arbeitszeit von 24,50 Stunden ergaben.

Die Beklagte behauptet hierzu, sie habe in der Addition alle Eingaben berücksichtigt, die in keinem größeren Abstand als 15 Minuten vorgenommen wurden. Zusätzlich habe sie für die 6 Heimarbeitstage noch je eine Viertelstunde Vor- und Nachbearbeitungszeit addiert, komme aber gleichwohl nur zu einer Arbeitszeit von 27,5 Stunden an 6 Heimarbeitstagen. Die Beklagte übersandte der Klägerin den Ausdruck der zeitlichen Lage der Dateneingaben und forderte die Klägerin gleichzeitig mit Schreiben vom 20.12.2012 auf, schriftlich Stellung zu nehmen bis zum 08.01.2013.

Mit Schreiben vom 07.01.2013 antworteten die Prozessbevollmächtigten der Klägerin und führten aus, dass die Klägerin entsprechend ihrer Stellenbeschreibung mit weiteren Tätigkeiten beschäftigt gewesen sei.

Mit Schreiben vom 14. Januar 2013 hörte die Beklagte den Betriebsrat zur außerordentlichen und ordentlichen Kündigung an. Der Betriebsrat widersprach der Kündigung u. a. mit der Begründung, dass die Zeitstempel der Datenbankeingabe als Zeitnachweis für die erbrachte Arbeitsleistung nicht heranzuziehen seien und die Arbeit außerhalb des betrieblichen Gleitzeitrahmens keinen Kündigungsgrund darstellen könne.

Die Klägerin hält die Kündigung für unwirksam, da dem Betriebsrat der Kündigungszeitpunkt der ordentlichen Kündigung nicht ordnungsgemäß mitgeteilt worden sei. Dem Betriebsrat seien auch die im Rahmen des Heimarbeitsplatzes zu erledigenden Aufgaben nicht zutreffend dargestellt worden. Die Errechnung der Arbeitszeiten dürfe nicht anhand der Datei durchgeführt werden. Die Verwertung sei unzulässig, da die Datenspeicherung § 32 BDSG widerspreche. Zudem sei das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG nicht gewahrt.

Weiter behauptet die Klägerin, zwischen zwei Speichervorgängen könnten durchaus längere Zeiträume als 15 Minuten liegen, da sie zwischen den Datenbankeingaben auch zuhause Recherchearbeiten vornehmen müsse. In diesem Fall müsse die Klägerin Entgeltvereinbarungen im Archiv oder im Internet suchen, um die entsprechenden Nummern in die Datenbank eingeben zu können. Sie habe auch in

der fraglichen Zeit zuhause die neuen Regelungen des PsychEntgeltG gelesen. Hierzu legt die Klägerin einen Ausdruck eines Verordnungsentwurfs vom 14.11.2012 vor.

Die Beklagte vertritt die Ansicht, mit der Angabe der auf das Arbeitsverhältnis anwendbaren Kündigungsfristen den Betriebsrat ausreichend informiert zu haben. Eine eventuell nicht beachtete Mitbestimmung des Betriebsrats aus § 87 BetrVG hindere die Verwertung des Zeitstempelausdrucks im Prozess nicht. Die Speicherung dieser Daten sei erforderlich gewesen, um nachvollziehen zu können, welcher Arbeitnehmer zu welchem Zeitpunkt welche Änderung an der Datenbank, die von mehreren Arbeitnehmern gepflegt wird, vorgenommen habe.

Die Beklagte erläutert den Inhalt der Liste der Zeitstempel (Bl. 56 - 96 d. A.) wie folgt: Die Registernummer sei der Schlüssel des jeweiligen Krankenhauses. Die Entgeltnummer sei der Schlüssel für die konkrete vom Krankenhaus erbrachte Leistung. Die nächsten beiden Spalten stellen die Geltungszeiträume der jeweiligen Vergütungssätze dar. Jeder konkreten Entgeltnummer sei dann ein konkreter Entgeltbetrag aus dem einzugebenden Datensatz zu zuordnen. Auf der rechten Seite des Ausdrucks befinde sich unter der Überschrift C-Date das Datum, zu dem die konkrete Datei erstmals angelegt wurde. Die Spalte C-User enthalte den Mitarbeiter, der die Datei angelegt habe. Unter M-Date werde die letzte Speicherung der Datei protokolliert. Durch weitere andere oder neue Eingaben in derselben Datei werde das M-Date jeweils erneut überschrieben. In der Spalte M-User befinde sich der Name des eingebenden Mitarbeiters, der die letzte Speicherung zu diesem Datensatz vorgenommen habe.

Der Mitarbeiter M , der einerseits Vorgesetzter der Klägerin und gleichzeitig auch Betriebsratsmitglied ist, habe eine Datenbankrecherche für die Heimarbeitstage der Klägerin in der Zeit vom 05.11. bis 16.11.2012 vorgenommen. Er habe dabei alle Datenspeicherungen in diese Datensammlung, die an den Heimarbeitstagen der Klägerin unter dem M-User der Klägerin gespeichert wurden, ausgedruckt. Damit enthalte die Liste der Zeitstempel alle Speicheraktivitäten der Klägerin unabhängig davon, ob sie die Datei soeben erst neu angelegt habe und dabei als C-User in der Liste aufgeführt ist oder ob die Datei bereits zuvor angelegt war.

Herr M habe sodann alle Zeiten zwischen M-Dates (von der Klägerin ausgelösten Speichervorgängen), die mehr als 15 Minuten betragen, von der Gesamtzeit der ersten bis zur letzten Eingabe eines Tages abgerechnet und jeweils zur Arbeitsvorbereitung und zum Arbeitsabschluss eine weitere Viertelstunde addiert. Daraus ergebe sich die Gesamtarbeitszeit von 27,5 Stunden anstelle der von der Klägerin angegebenen 43,26 Stunden.

Es sei auch nicht Aufgabe der Klägerin gewesen, zuhause andere Tätigkeiten als Dateneingaben zu erbringen. Vorbereitende Arbeiten wie die Suche nach den Entgeltvereinbarungen, die nicht den Genehmigungsbescheiden beigefügt waren, die Suche nach neuen Schlüsseln seien nicht vom Heimarbeitsplatz der Klägerin aus, sondern vom Büroarbeitsplatz aus vorzunehmen gewesen. Soweit die Entgeltvereinbarungen nicht in Papierform vorlägen, seien diese in einer anderen Datenbank gespeichert. In Fällen, in denen dies nicht der Fall sei, habe die Klägerin keine häuslichen Recherchearbeiten zu erledigen, da die Krankenhäuser dann durch

die Beklagte aufgefordert würden, die Entgeltvereinbarungen vorzulegen oder zu übermitteln. In der überprüften Zeit habe die Klägerin auch nur zweimal nach neuen Leistungsschlüsseln recherchieren müssen. Diese Recherchen seien vom dienstlichen Arbeitsplatz aus erfolgt.

Die Verordnung über pauschalierende Entgelte, Psychiatrie und Psychosomatik 2013 sei tatsächlich erst am 19.11.2012 in Kraft getreten. Herr M habe die Klägerin erst nach diesem Datum aufgefordert, sich mit dem Inhalt vertraut zu machen, da zuvor der Entwurf der Verordnung nicht verbindlich gewesen sei.

Das Arbeitsgericht hat die Klage in vollem Umfange zugesprochen und dabei zugrundegelegt, dass nicht ausreichend klargeworden sei, wie sich die Differenz der durch Herrn M errechneten Arbeitszeit und der von der Klägerin angegebenen Arbeitszeit ergebe.

Mit der Berufung beantragt die Beklagte,

das Urteil des Arbeitsgerichts Köln vom 28.11.2013 abzuändern und die Klage vollständig abzuweisen.

Die Klägerin beantragt,

die Berufung zurückzuweisen.

Das Gericht hat über die Erstellung der Zeitstempelliste, deren Inhalte und Bedeutung sowie den regelmäßigen Arbeitsablauf der Klägerin Beweis erhoben durch Vernehmung des Zeugen M . Hinsichtlich des Ergebnisses der Beweisaufnahme sowie des weiteren Sach- und Streitstandes wird gemäß § 313 ZPO auf den Akteninhalt Bezug genommen.

Entscheidungsgründe

Die zulässige und fristgerechte Berufung der Klägerin ist in vollem Umfange begründet. Das Arbeitsverhältnis der Parteien ist gemäß § 626 BGB außerordentlichen mit Zugang der Kündigung vom 18.01.2013 beendet worden.

Die Kündigung ist zunächst nicht wegen mangelnder Betriebsratsanhörung unwirksam. Hinsichtlich der außerordentlichen Kündigung spielt dabei die Frage, ob die ordentliche Kündigungsfrist mit einem Datum bezeichnet werden muss oder dem Betriebsrat lediglich die Rechtsgrundlagen für die Fristberechnung zur Kenntnis gebracht werden müssen keine Rolle, denn dem Betriebsrat war hinsichtlich der außerordentlichen Kündigung klar, dass diese mit Zugang der Kündigungserklärung wirksam werden soll.

Die Betriebsratsanhörung war auch nicht wegen einer mangelhaften Sachverhaltsdarstellung unwirksam. Die Arbeitgeberin hat dem Betriebsrat den von ihr recherchierten und der Kündigung zugrundegelegten Sachverhalt vollständig vorgetragen. Sie hat subjektiv determiniert das mitgeteilt, was sie zum Ausspruch der Kündigung bewog. Zudem ist zu berücksichtigen, dass der Betriebsrat die Klägerin vor Abgabe seiner eigenen Stellungnahme angehört hat. Hierbei vor Ausspruch der Kündigung gewonnene eigene Erkenntnisse konnte der Betriebsrat in

seine Beurteilung des Kündigungssachverhalts einfließen lassen. Eine arbeitgeberseitige Fehlinformation, die die gesamte Betriebsratsanhörung unwirksam erscheinen lassen könnte, ist damit nicht festzustellen.

Die Täuschung des Arbeitgebers darüber, dass ein Arbeitnehmer gearbeitet habe, während tatsächlich keine Arbeitsleistung erbracht wurde, stellt regelmäßig einen Grund dar, der geeignet ist, das Arbeitsverhältnis durch Arbeitgeberkündigung ohne Einhaltung der Kündigungsfrist zu beenden.

Nach durchgeführter Beweisaufnahme geht die erkennende Kammer davon aus, dass dieser Sachverhalt vorliegend gegeben ist und dass die Klägerin in einem Zeitraum von 6 Arbeitstagen gegenüber ihrem Arbeitgeber 15,76 Stunden zu viel an Arbeitszeit angegeben hat.

Dabei würde es nach Ansicht der Kammer nicht ausreichen, dass die Klägerin lediglich Arbeitszeiten, die außerhalb des betrieblichen Gleitzeitrahmens lagen zeitlich verlegt hat und hierdurch vorgegeben hat, ihre Arbeitszeit innerhalb des Gleitzeitrahmens erbracht zu haben. Auch würde es nach Ansicht der Kammer alleine nicht ausreichen, dass die Klägerin zuhause eine abweichende Excel-Tabelle geführt hat und die nach dieser Tabelle von der Klägerin festgehaltenen Stunden zu anderen Zeiten im Betrieb als Arbeitsleistung in die dortige Zeiterfassung eingegeben hat. Die Klägerin hat zwar versucht, sich hierdurch Vorteile zu sichern, da durch die gesteuerte Bekanntgabe der (behaupteten) Überstunden ein Verfall dieser Überstunden nicht eintreten konnte. Gleichwohl erscheint dieser Sachverhalt nicht derart schwerwiegend, dass dies die sofortige Beendigung oder die ordentliche Beendigung ohne Abmahnung rechtfertigen würde. Denn für diesen Sachverhalt lässt sich nicht feststellen, dass die Arbeitnehmerin mit krimineller Energie den Arbeitgeber über die Menge der tatsächlichen Arbeitszeit täuschen wollte. Allenfalls liegt ein Täuschen über die Lage der tatsächlichen Arbeitszeit vor.

Nach Durchführung der Beweisaufnahme und Auswertung der Zeitstempelliste hat die erkennende Kammer die hinreichende Gewissheit, dass die Klägerin die Beklagte über die Menge der von ihr am Heimarbeitsplatz durchgeführten Arbeiten täuschen wollte.

Dabei ist das Gericht zunächst nicht gehindert, die ausgedruckte Liste der Zeitstempel im Verfahren zu verwerten. Ein solches Verwertungsverbot ergibt sich zum einen nicht daraus, dass hinsichtlich der automatisierten Datenverarbeitung ein Mitbestimmungsrecht des Betriebsrats nach § 87 BetrVG bestand. Auch dann, wenn die Art der Datenverarbeitung bereits vor der erstmaligen Konstitution eines Betriebsrats im Betrieb durchgeführt wurde, steht dem Betriebsrat das Mitbestimmungsrecht zur automatischen Datenverarbeitung nach § 87 Abs. 1 Nr. 6 BetrVG zu. Allerdings folgt hieraus nicht die Unverwertbarkeit der erhobenen Daten im Prozess (BAG vom 13.12.2007 - 2 AZR 537/06 -).

Ebenso wenig folgt ein Verwertungsverbot aus § 32 BDSG. Die Beklagte hat grundsätzlich ein Interesse daran, die von ihr als ihr Geschäftszweck gespeicherten Daten, die in einer Datenbank gepflegt werden, zu der mehrere Personen schreibenden Zugang haben, dem einzelnen Mitarbeiter zuordnen zu können und

auch anhand des Speicherdatums feststellen zu können, ob die eingegebenen Daten tatsächlich dem aktuellen durch die Speicherung dokumentierten Zeitpunkt entsprechen. Die Beklagte stellt die Dateien mit den Entgeltvereinbarungen ihren Mitgliedern zu Abrechnungszwecken zur Verfügung. Die Pflege der Datenbank ist damit eine wesentliche geschäftliche Aufgabe der Beklagten. Sind die Dateneingaben fehlerhaft oder nicht aktuell, so können bei den Nutzern der Datenbank erhebliche wirtschaftliche Schäden entstehen. Es ist deshalb für die Durchführung der Arbeitsverhältnisse der mit der Dateneingabe befassten Mitarbeiter erforderlich, Fehler in der Dateneingabe, die sich sowohl auf die Inhalte als auch auf den Gültigkeitszeitraum der eingegebenen Daten beziehen, kontrollieren und vermeiden zu können. Nur dann, wenn identifiziert werden kann, wer Fehleingaben gemacht hat, kann die Beklagte arbeitsrechtlich tätig werden und die erforderliche Qualität der Dateneingaben wirklich sicherstellen. Die erkennende Kammer hält deshalb auch unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung die vorgenommene Abspeicherung des sog. M-Date und des M-User für zulässig.

Vorliegend ist gleichwohl abzuwägen, ob das allgemeine Persönlichkeitsrecht der Klägerin den Vorrang gegenüber der Auswertung der automatisiert erhobenen Datenlisten verdient. Dabei ist zu berücksichtigen, dass die Beklagte aufgrund der von der Klägerin eingereichten Zeitaufschreibungen und der in der gleichen Zeit erledigten Arbeitsmenge den konkreten Verdacht hatte, dass die angegebenen Arbeitszeiten nicht zutreffend sind. Der Verdacht wurde auch nicht dadurch widerlegt, dass die Klägerin eingeräumt hat, andere Arbeitszeiten gegenüber der Arbeitgeberin angegeben zu haben, als in ihrer privaten Excel-Tabelle an tatsächlicher von ihr behauptete Arbeitszeit nieder gelegt war. Nachdem der Verdacht entstanden war, ergab sich für die Beklagte keine andere Überprüfungsmöglichkeit als die elektronische Auswertung der Datenbankeingaben. In einem solchen konkreten Verdachtsfall steht das Persönlichkeitsrecht hinter der Möglichkeit der Datenermittlung zurück. Das vorrangige Ziel des Datenschutzes ist nicht der Täterschutz.

Nach Durchführung der Beweisaufnahme ergibt sich damit für die Kammer folgendes Bild: Die vorgelegte Liste der Datenbankeingaben enthält alle von der Klägerin an ihrem Heimarbeitsplatz vorgenommenen Datenbankeingaben. Die von dem Zeugen geschilderte Arbeitsorganisation sah vor, dass die Klägerin an ihrem Heimarbeitsplatz im Wesentlichen Dateneingaben vornehmen sollte. An ihrem Büroarbeitsplatz hatte sie dafür Sorge zu tragen, dass die zuhause zu bearbeitenden Genehmigungsbescheide vollständig waren, also die häuslichen Tätigkeiten vorzubereiten. Zu der ordnungsgemäßen Arbeitsvorbereitung gehörte deshalb die Kontrolle des Genehmigungsbescheides darauf, ob die einzugebenden Daten in Papierform oder als Datei zugänglich waren, die genehmigten Entgeltvereinbarungen vorlagen, um in die Datenbank übertragen zu werden. Danach sind beispielsweise am 07.11.2007 in der Zeit von 6.38 Uhr bis 10.09 Uhr keinerlei Dateneingaben von der Klägerin vorgenommen worden. Es handelt sich um 191 Minuten, in denen keine Arbeitsleistung in der Datenbank feststellbar ist. Für den entsprechenden Tag hat die Klägerin lediglich 63 Minuten Pause angegeben.

Die Klägerin konnte auch weder diese Arbeitsunterbrechungen noch andere längere Arbeitsunterbrechungen erklären. Nachdem die Klägerin angegeben hat, die

Verordnung über die Neuregelung der Entgelte Psychiatrie und Psychosomatik am 14.11.2012 gelesen zu haben, wäre für den 12.11.2012 erklärungsbedürftig gewesen, welche Tätigkeiten die Klägerin konkret von 8.49 Uhr bis 12.31 Uhr, von 13.07 Uhr bis 14.22 Uhr und von 16.16 Uhr bis 16.36 Uhr verrichtet hat. Laut eigener Liste hat sie an diesem Tag nur 45 Minuten Pause gemacht. Sie hat angegeben, um 7.39 Uhr die Arbeit aufgenommen zu haben, die erste Eingabe war aber erst um 8.32 Uhr. Der Klägerin war bereits durch die Kündigungsanhörung zeitnah Gelegenheit gegeben worden, zu den Unterbrechungen in der Dateneingabe Stellung zu nehmen.

Die von dem Zeugen M geschilderten Arbeitsaufgaben und Strukturen der Datenbankeingabe haben bei der Kammer zu der Überzeugung geführt, dass eine ordnungsgemäße Arbeitsleistung der Klägerin nicht darin bestehen konnte, zuhause darauf zu warten, dass eventuell fehlende Dateien mit Entgeltvereinbarungen der Klägerin per E-Mail zugesandt werden. Vielmehr hätte sie in dieser Zeit andere Dateneingaben vornehmen müssen und können bzw. im Vorfeld bei der Planung ihrer häuslichen Tätigkeiten darauf achten müssen, dass jedem Genehmigungsbescheid die erforderlichen Entgeltvereinbarungen bereits beigefügt waren oder diese zugänglich waren.

Aufgrund der von dem Zeugen M geschilderten Überprüfung der Dateistempel ergibt sich auch, dass die Anforderung an die Klägerin, einzelne Unterbrechungszeiten zu erklären nicht unzumutbar war, denn sie betraf nur die Zeiten, bei denen die einzelnen Speichervorgänge länger als 15 Minuten auseinanderlagen. Für die vom Arbeitsgericht angenommene Hypothese, die Klägerin habe zunächst eine Unzahl Dateien aufgemacht und dann hintereinander geschlossen, spricht nichts. Nicht nur hat die Klägerin selber nicht behauptet, so gearbeitet zu haben. Vielmehr ergibt sich aus den unzähligen neuangelegten Dateien (C-Date), dass regelmäßig eine Eingabezeit von nur wenigen Sekunden von der Neuanlage einer Datei bis zu deren letzter Abspeicherung benötigt wird.

Das Gericht hat keine Anhaltspunkte gesehen, dem Zeugen M nicht zu glauben. Die Darstellung der Arbeitsabläufe war plausibel und ist insbesondere von der Klägerin in der Stellungnahmefrist, die ihr auch zu dem Ergebnis der Beweisaufnahme gesetzt wurde, nicht angegriffen worden.

Auch bei der vorzunehmenden individuellen Abwägung der Kündigungsgründe gelangt das Gericht zu der Überzeugung, dass es der Beklagten unzumutbar war, die ordentliche Kündigungsfrist abzuwarten und das Arbeitsverhältnis länger als bis zum Zugang der außerordentlichen Kündigung aufrecht zu erhalten. Zwar ist die Versuchung, Arbeitszeiten vorzutäuschen, wenn diese nicht effektiv kontrolliert werden können, bei einem Heimarbeitsplatz besonders groß. Trotzdem durfte die Klägerin nicht annehmen, ihr Arbeitgeber werde eine falsche Angabe von Arbeitszeiten, also die Abrechnung von Freizeit als Arbeitszeit hinnehmen oder allenfalls mit einer Abmahnung reagieren. Dabei ist zu berücksichtigen, dass es sich vorliegend nicht nur um wenige Minuten handelt, die beim Stechkartenbetrug auch schon für die Rechtfertigung einer fristlosen Kündigung ausgereicht haben. Vielmehr hat die Klägerin sich in erheblichem Maße Zeitguthaben durch Falschangaben "erarbeitet", um sodann nach Belieben Freistellungstage geltend machen zu können.

Die Beendigung der Möglichkeit, Dateneingaben am Heimarbeitsplatz vorzunehmen, stellt auch nicht ein milderes Mittel gegenüber der außerordentlichen Kündigung dar. Nachdem die Klägerin durch ihre Vorgehensweise das Vertrauen in eine ordnungsgemäße Arbeitsleistung erschüttert hat, hätte die Beklagte die Klägerin auch am betrieblichen Arbeitsplatz ununterbrochen kontrollieren müssen, um sichergehen zu können, dass in der vereinbarten Arbeitszeit tatsächlich Arbeitsleistung erbracht wird. Die Verletzung des Vertrauens in die korrekte Arbeitserfüllung durch die Klägerin ist so schwerwiegend, dass auch unter Berücksichtigung des hohen Lebensalters, einer nicht übermäßig günstigen Prognose hinsichtlich einer neuen Arbeitsstelle und der langjährigen Betriebszugehörigkeit das arbeitgeberseitige Interesse an der sofortigen Beendigung des Vertragsverhältnisses überwiegt.

Die Kündigung ist auch nicht gemäß § 626 Abs. 2 BGB unwirksam. Die Beklagte hat hinreichend schnell recherchiert und die erforderliche Sachverhaltsaufklärung zügig betrieben. Die der Klägerin nach dem Ausdruck der Zeitstempelliste eingeräumte Stellungnahmefrist war wegen der Weihnachtsfeiertage und des Jahreswechsels nicht zu lang bemessen.

Nach alldem war das erstinstanzliche Urteil abzuändern und die Klage abzuweisen.

Die Kostenentscheidung folgt aus § 91 ZPO.

Die Revision wurde mangels allgemeiner Bedeutung des Rechtsstreits nicht zugelassen.

4 BAG: Verpflichtung zur Nutzung einer elektronischen Signaturkarte

BAG, 25.09.2013 10 AZR 270/126.

Verpflichtung zur Nutzung einer elektronischen Signaturkarte

Leitsatz

Ein Arbeitgeber kann von seinem Arbeitnehmer die Beantragung einer qualifizierten elektronischen Signatur und die Nutzung einer elektronischen Signaturkarte verlangen, wenn dies für die Erbringung der vertraglich geschuldeten Arbeitsleistung erforderlich und dem Arbeitnehmer zumutbar ist.(Rn.36)

Orientierungssatz

1. Nach § 4 Abs 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt. Rechtsvorschriften in diesem Sinne sind auch Tarifverträge und Betriebs- oder Dienstvereinbarungen. Enthalten die Bestimmungen einer Dienstvereinbarung eine

solche Erlaubnis, ist eine Einwilligung des Arbeitnehmers nicht erforderlich gemäß § 4a BDSG.

2. Durch eine Weisung, die einen Arbeitnehmer verpflichtet seine aus dem Personalausweis ersichtlichen Daten einem durch den Arbeitgeber ausgewählten Zertifizierungsdiensteanbieter zur Verfügung zu stellen, wird in das Recht auf informationelle Selbstbestimmung eingegriffen.

3. Dieser Eingriff ist zumutbar, wenn der Einsatz einer elektronischen Signaturkarte für den vertraglich vereinbarten Aufgabenbereich unverzichtbar ist, es sich bei den Angaben im Personalausweis nicht um besonders sensible Daten iSv. § 3 Abs 9 BDSG handelt und der Schutz der personenbezogenen Daten durch Vorschriften des Signaturgesetzes und der Signaturverordnung sichergestellt werden.

Tatbestand

Die Parteien streiten über die Verpflichtung der Klägerin, eine elektronische Signaturkarte zu beantragen und bei ihrer Tätigkeit einzusetzen.

Die 1956 geborene Klägerin ist seit 1980 bei der Beklagten als Angestellte beschäftigt. Sie wird im Wasser- und Schifffahrtsamt (WSA) Cuxhaven eingesetzt. Auf das Arbeitsverhältnis finden kraft arbeitsvertraglicher Vereinbarung die Tarifverträge des öffentlichen Dienstes in der für den Bund geltenden Fassung Anwendung. Die Klägerin wird nach Entgeltgruppe 5 TVöD vergütet.

Nach der Dienstpostenbeschreibung vom 12. Juni 1996 umfasst das Aufgabengebiet der Klägerin ua. Schreibarbeiten, die Koordinierung von Terminen sowie die Durchführung des inneren Dienstes der Dienststelle einschließlich der Zusammenstellung von Ausschreibungsunterlagen. Bestandteil ihrer Tätigkeit ist die Veröffentlichung von Vergabeunterlagen im Rahmen von Ausschreibungen der Beklagten.

Am 10. Dezember 2003 beschloss die Bundesregierung, die Vergabeverfahren aller Bundesbehörden sukzessive auf ein elektronisches Vergabesystem umzustellen. Am 8./13. März 2006 schloss das Bundesministerium für Verkehr, Bau und Stadtentwicklung (im Folgenden: BMVBS) mit dem bei ihm gebildeten Hauptpersonalrat eine „Dienstvereinbarung zur Nutzung qualifizierter digitaler Signaturen" (DV Digitale Signaturen).

Mit Erlass vom 11. Dezember 2009 verfügte das BMVBS, dass ab dem 1. Januar 2010 alle Vergabebekanntmachungen gemäß der Verdingungsordnung für Leistungen (VOL) und der Verdingungsordnung für freiberufliche Leistungen (VOF) über die elektronische Vergabeplattform des Bundes zu erstellen und entsprechend zu veröffentlichen seien. Voraussetzung für die Veröffentlichung von Vergabeunterlagen auf der elektronischen Vergabeplattform des Bundes ist ein qualifiziertes Zertifikat mit qualifizierter elektronischer Signatur (im Folgenden: elektronische Signaturkarte) nach dem Signaturgesetz (SigG), das nur natürlichen Personen erteilt wird (§ 2 Nr. 7 SigG). Die Ausstellung einer elektronischen Signaturkarte setzt voraus, dass der Antragsteller von dem Zertifizierungsdiensteanbieter anhand des Personalausweises

oder gleichwertiger Dokumente identifiziert worden ist (§ 5 Abs. 1 SigG, § 3 Abs. 1 SigV).

Mit Schreiben vom 15. März 2010 forderte die Amtsleitung des WSA die Klägerin auf, bei der T GmbH, einem Tochterunternehmen der D AG, eine elektronische Signaturkarte zu beantragen. Mit Schreiben vom 18. März 2010 teilte die Klägerin mit, sie sei nicht bereit, einen entsprechenden Antrag zu stellen, weil sie Bedenken habe, ihre persönlichen Daten einer privaten Firma zur Verfügung zu stellen. Das WSA wandte sich daraufhin über das BMVBS an die Bundesnetzagentur. Diese teilte mit E-Mail vom 4. Mai 2010 mit, dass aus ihrer Sicht kein Anlass bestehe, an der Datensicherheit und der Integrität der Systeme des von der Beklagten verwendeten Zertifizierungsdiensteanbieters zu zweifeln. Anschließend forderte die Amtsleitung des WSA die Klägerin mit Schreiben vom 22. Juni 2010 erneut auf, eine elektronische Signaturkarte zu beantragen. Nachdem sich die Klägerin zunächst wiederum weigerte, beantragte sie am 7. September 2010 „unter Vorbehalt und unter Protest" eine elektronische Signaturkarte, die sie kurz darauf erhielt.

Die Klägerin hat die Auffassung vertreten, sie sei nicht verpflichtet, eine elektronische Signaturkarte zu beantragen und zu nutzen. Eine Nutzung der elektronischen Signaturkarte durch sie sei nicht erforderlich. Die Diplom-Ingenieure, welche die Ausschreibungsunterlagen erstellten, könnten diese selbst auf der elektronischen Vergabeplattform des Bundes veröffentlichen. Außerdem gebe es andere Beschäftigte im WSA, die bereits über eine Signaturkarte verfügten und daher in der Lage seien, die Veröffentlichungen vorzunehmen. Entgegen den Vorgaben der DV Digitale Signaturen sei die Klägerin im Umgang mit der elektronischen Signaturkarte nicht geschult worden. Darüber hinaus verletze die Weisung der Beklagten das Recht der Klägerin auf informationelle Selbstbestimmung, weil sie ihre persönlichen Daten gegen ihren Willen einer privaten Firma mitteilen müsse. Sie habe Angst, dass mit ihren Daten Missbrauch getrieben werde.

Die Klägerin hat, soweit in der Revision noch von Interesse, beantragt

festzustellen, dass sie nicht verpflichtet ist, ein qualifiziertes Zertifikat nach dem Signaturgesetz zu beantragen und im Rahmen des elektronischen Vergabeverfahrens einzusetzen.

Die Beklagte hat beantragt, die Klage abzuweisen. Sie ist der Ansicht, sie habe ihr Direktionsrecht rechtmäßig ausgeübt. Insbesondere bestünden keine Anhaltspunkte für die Behauptung der Klägerin, mit ihren persönlichen Daten könne Missbrauch getrieben werden.

Das Arbeitsgericht hat die Klage abgewiesen. Das Landesarbeitsgericht hat die Berufung der Klägerin zurückgewiesen. Mit der vom Bundesarbeitsgericht insoweit zugelassenen Revision verfolgt die Klägerin ihren Feststellungsantrag weiter.

Entscheidungsgründe

Die zulässige Revision ist unbegründet. Die Klägerin war verpflichtet, bei der T GmbH ein qualifiziertes Zertifikat mit qualifizierter elektronischer Signatur (elektronische Signaturkarte) zu beantragen, und sie ist verpflichtet, unter dessen Nutzung

Ausschreibungsunterlagen auf der elektronischen Vergabeplattform des Bundes zu veröffentlichen. Das Landesarbeitsgericht hat die Rechtmäßigkeit der entsprechenden Weisung zutreffend beurteilt.

I. Die Klage ist mit dem in der Revision noch anhängigen Feststellungsantrag zulässig.

(…)

II. Die Klage ist unbegründet. Die Weisung der Beklagten ist wirksam.

1. Nach § 106 Satz 1 GewO kann der Arbeitgeber Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrags oder gesetzliche Vorschriften festgelegt sind.

2. Die Veröffentlichung von Ausschreibungsunterlagen unter Einsatz einer elektronischen Signaturkarte gehört zum vertraglich vereinbarten Aufgabenbereich der Klägerin.

a) Die Klägerin wird gemäß § 1 des Arbeitsvertrags vom 13. Februar 1980 als Angestellte beschäftigt; aufgrund des 2. Nachtrags zum Arbeitsvertrag vom 29. Mai 1981 wurde sie in die Vergütungsgruppe VII BAT höhergruppiert und später in die EG 5 TVöD übergeleitet. Das Direktionsrecht des Arbeitgebers im öffentlichen Dienst erstreckt sich bei einer Vertragsgestaltung, die den vertraglichen Aufgabenbereich allein durch eine allgemeine Tätigkeitsbezeichnung und die Nennung der Vergütungsgruppe beschreibt, auf solche Tätigkeiten des allgemein umschriebenen Aufgabenbereichs, welche die Merkmale der Vergütungsgruppe erfüllen, in die der Arbeitnehmer eingestuft ist. Dem Arbeitnehmer können andere, dem allgemein umschriebenen Aufgabenbereich zuzuordnende Tätigkeiten nur zugewiesen werden, soweit sie den Merkmalen dieser Vergütungsgruppe entsprechen (st. Rspr., zuletzt zB BAG 17. August 2011 - 10 AZR 322/10 - Rn. 15).

b) Die Veröffentlichung von Vergabeunterlagen gehört zum Aufgabenbereich der Klägerin und entspricht den Merkmalen der Vergütungsgruppe VII BAT (nunmehr EG 5 TVöD). Nach der Dienstpostenbeschreibung vom 12. Juni 1996, die zwischen den Parteien ebenso wenig im Streit steht wie die Eingruppierung selbst, gehört zu den Aufgaben der Klägerin die Durchführung des inneren Dienstes der Dienststelle einschließlich der Zusammenstellung von Ausschreibungsunterlagen. Zu den administrativen Aufgaben im Zusammenhang mit Ausschreibungsunterlagen gehört nach der Verkehrsanschauung (vgl. ErfK/Preis 13. Aufl. § 106 GewO Rn. 5) auch deren Veröffentlichung. Dementsprechend hat die Klägerin bereits in der Vergangenheit regelmäßig Vergabeunterlagen - unter anderem im Intranet - veröffentlicht. Der geforderte Einsatz einer elektronischen Signaturkarte verändert den Aufgabenbereich der Klägerin nicht; lediglich die Art und Weise der Veröffentlichung und die dazu genutzten Arbeitsmittel werden technischen Entwicklungen angepasst.

3. Die Weisung der Beklagten ist unter Wahrung der Mitbestimmungsrechte nach dem BPersVG erfolgt (vgl. zur Theorie der Wirksamkeitsvoraussetzung im Anwendungsbereich des BPersVG zuletzt: BAG 22. Mai 2012 - 1 AZR 94/11 - Rn. 29). Der Hauptpersonalrat des BMVBS (§ 82 Abs. 1, § 53 Abs. 1 BPersVG) hat seine Rechte nach dem BPersVG im Zusammenhang mit der Einführung qualifizierter digitaler Signaturen (vgl. § 75 Abs. 3 Nr. 17 BPersVG) durch den Abschluss der DV Digitale Signaturen ausgeübt.

Die Weisung der Beklagten verstößt auch nicht gegen Vorschriften dieser Dienstvereinbarung. Insbesondere wurden entgegen der Rechtsauffassung der Klägerin die Vorgaben für die Schulung der Beschäftigten eingehalten. Dabei kann dahinstehen, ob deren Verletzung überhaupt zu einer Unwirksamkeit der Weisung führen oder nur einen nachträglichen Schulungsanspruch auslösen würde. Mit dem Schreiben der Amtsleitung des WSA vom 15. März 2010 wurde der Klägerin eine Kopie der Dienstvereinbarung übersandt. In dem Schreiben wird zudem auf eine „geplante Schulung in der IT-Anwendung" Bezug genommen. Eine weitere Schulung fand im März 2011 statt. Dass die Klägerin an dieser krankheitsbedingt nicht teilnehmen konnte, stellt die Erfüllung der Pflichten aus der Dienstvereinbarung durch die Beklagte nicht infrage. Es gibt keine Anhaltspunkte dafür, dass die Beklagte die Schulung der Klägerin vorenthalten wollte oder sie nicht nachschulen würde, soweit die Klägerin hieran mitwirkt und teilnimmt.

4. Die Weisung zur Beantragung und Nutzung der elektronischen Signaturkarte verstößt nicht gegen Bestimmungen des BDSG.

a) Die Beklagte selbst erhebt, verarbeitet oder nutzt im Zusammenhang mit der Beantragung des qualifizierten Zertifikats mit qualifizierter elektronischer Signatur und der Erstellung der Signaturkarte keine Daten iSd. Bestimmungen des BDSG.

aa) Zwar ist das WSA als Bundesbehörde (vgl. Art. 87 Abs. 1 Satz 1, Art. 89 Abs. 2 GG) eine öffentliche Stelle iSd. § 1 Abs. 2 Nr. 1, § 2 Abs. 1 Satz 1 BDSG. Bei den Daten, welche die Klägerin im Rahmen der Beantragung der elektronischen Signaturkarte mitzuteilen hat, handelt es sich auch um personenbezogene Daten iSd. § 3 Abs. 1 BDSG. In Bezug auf diese Daten ist das WSA jedoch nicht verantwortliche Stelle iSd. BDSG.

(1) Normadressat der im BDSG niedergelegten Rechte und Pflichten ist die jeweils verantwortliche Stelle (ErfK/Franzen § 1 BDSG Rn. 12; Simitis/Dammann BDSG 7. Aufl. § 3 Rn. 224 f.; Gola/Schomerus BDSG 11. Aufl. § 3 Rn. 48). Das ist gemäß § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(2) Personenbezogene Daten, die für die Erstellung und Nutzung einer elektronischen Signaturkarte erforderlich sind, werden von dem betreffenden Zertifizierungsdiensteanbieter unter Berücksichtigung der Vorgaben des SigG erhoben, verarbeitet und genutzt (§ 5 ff. SigG). Hinsichtlich des Umgangs mit diesen Daten unterliegt der Zertifizierungsdiensteanbieter daher - neben den speziellen Datenschutzbestimmungen des SigG - den Regelungen des BDSG (vgl.

Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 29). Er ist insoweit die verantwortliche Stelle iSd. § 3 Abs. 7 BDSG.

(3) Das WSA ist demgegenüber weder in die Beschaffung noch in die Verarbeitung der Daten eingeschaltet. Vielmehr wurde die Klägerin aufgefordert, die elektronische Signaturkarte direkt beim Zertifizierungsdiensteanbieter zu beantragen (vgl. Schreiben vom 15. März 2010; DV Digitale Signaturen „Antragstellung durch den Beschäftigten"). Diese Vorgehensweise entspricht dem Modell des BDSG, wonach personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Abs. 2 Satz 1 BDSG), und den Vorgaben des Signaturgesetzes (§ 14 Abs. 1 SigG). Das WSA nutzt auch nicht die zur Ausstellung der elektronischen Signaturkarte durch die T GmbH erhobenen Daten. Ein Nutzen von Daten iSv. § 3 Abs. 5 BDSG liegt vor, wenn die Daten mit einer bestimmten Zweckbestimmung ausgewertet, zusammengestellt, abgerufen oder ansonsten zielgerichtet zur Kenntnis genommen werden sollen (Gola/Schomerus BDSG § 3 Rn. 42; Gola/Wronka Handbuch zum Arbeitnehmerdatenschutz 5. Aufl. Rn. 911). Bei einem Einsatz der elektronischen Signaturkarte durch die Klägerin werden deren personenbezogene Daten durch das WSA nicht zielgerichtet zur Kenntnis genommen. Das WSA hat keinen Zugriff auf diese Daten.

bb) Zwischen dem WSA und dem Zertifizierungsdiensteanbieter besteht kein Auftragsverhältnis iSd. § 3 Abs. 7, § 11 BDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag ist dadurch gekennzeichnet, dass sich eine verantwortliche Stelle eines Dienstleistungsunternehmens bedient, das lediglich weisungsgebunden mit den Daten umgeht (Gola/Schomerus BDSG § 11 Rn. 3; Simitis/Petri BDSG § 11 Rn. 20). Die verantwortliche Stelle bestimmt weiterhin allein über die Erhebung, Verarbeitung und Nutzung der Daten und behält die uneingeschränkte Verfügungsgewalt (Gola/Wronka Handbuch zum Arbeitnehmerdatenschutz Rn. 983; Wedde in Däubler/Klebe/Wedde/Weichert BDSG 3. Aufl. § 11 Rn. 5). Der Bereich der Auftragsdatenvergabe wird verlassen, sobald dem Dienstleistungsunternehmen eine eigenständige rechtliche Zuständigkeit für die Aufgabe, deren Erfüllung die Datenverarbeitung oder -nutzung dient, zugewiesen wird (Gola/Schomerus BDSG § 11 Rn. 9). Nach den Vorgaben des SigG ist der Zertifizierungsdiensteanbieter allein für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des Antragstellers verantwortlich. Er entscheidet selbst über den Umgang mit den von ihm erhobenen Daten und hat dabei die zwingenden gesetzlichen Vorgaben insbesondere des SigG zu beachten. Das WSA hat keinen Zugriff auf und damit keine Verfügungsgewalt über die Daten. Ihm stehen auch keinerlei Kontroll- oder Weisungsrechte im Hinblick auf den Umgang mit den Daten zu.

b) Ein Verstoß gegen Bestimmungen des BDSG im Zusammenhang mit der Datenerhebung durch die T GmbH als Zertifizierungsdiensteanbieter ist nicht erkennbar.

aa) Das Unternehmen ist verantwortliche Stelle iSd. BDSG, es erhebt, verarbeitet und nutzt im Zusammenhang mit der Ausstellung der elektronischen Signaturkarte als nicht-öffentliche Stelle Daten der Klägerin (§ 1 Abs. 2 Nr. 3, § 2 Abs. 4 Satz 1, § 3 Abs. 7 BDSG).

bb) Die Erhebung der Daten erfolgt unmittelbar bei der Klägerin auf Grundlage der DV Digitale Signaturen (§ 4 Abs. 1, Abs. 2 Satz 1 BDSG); ihre Einwilligung (§ 4a BDSG) ist deshalb nicht erforderlich.

(1) Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt. Rechtsvorschriften in diesem Sinne sind auch Tarifverträge (BAG 25. Juni 2002 - 9 AZR 405/00 - zu A II 4 d der Gründe, BAGE 101, 357) und Betriebs- oder Dienstvereinbarungen (BAG 27. Mai 1986 - 1 ABR 48/84 - zu B II 3 b aa der Gründe, BAGE 52, 88; 20. Dezember 1995 - 7 ABR 8/95 - zu B III 2 der Gründe, BAGE 82, 36 [jeweils zu Betriebsvereinbarungen]; ErfK/Franzen § 4 BDSG Rn. 2).

(2) Eine solche Erlaubnis enthalten die Bestimmungen der DV Digitale Signaturen. Danach wird jeder IT-Arbeitsplatz im Bereich der elektronischen Vergabe mit einem Kartenlesegerät und Chipkarten nach den Regelungen des SigG ausgestattet. Durch den jeweiligen Beschäftigten persönlich erfolgt eine entsprechende Antragstellung beim Zertifizierungsdiensteanbieter, die seine zuverlässige Identifizierung anhand der Personalausweisdaten erfordert. Unter diese Dienstvereinbarung fällt auch die Klägerin; sie gilt unmittelbar und zwingend (§§ 73, 75 Abs. 3 Nr. 17 BPersVG; Weber in Richardi/Dörner/Weber Personalvertretungsrecht 4. Aufl. § 73 BPersVG Rn. 21). Dem steht nicht entgegen, dass die Dienstvereinbarung eine Hergabe der Daten an Dritte verlangt. Durch § 2 Nr. 7 SigG ist vorgegeben, dass eine elektronische Signaturkarte nur von einer natürlichen Person beantragt werden kann und ihre Ausstellung durch Zertifizierungsdiensteanbieter erfolgt (§ 4 f. SigG).

Bedenken gegen die Wirksamkeit der DV Digitale Signaturen hat die Klägerin nicht geltend gemacht, sie sind auch nicht ersichtlich. Insbesondere begrenzt die Dienstvereinbarung den Kreis der Zertifizierungsdiensteanbieter auf solche, die gemäß § 15 SigG akkreditiert sind und damit einer weiter gehenden aufsichtsbehördlichen Kontrolle unterliegen. Auch beinhaltet die DV Digitale Signaturen weitere Bestimmungen zum Schutz der Beschäftigten, wie beispielsweise eine Haftungsausschlussregelung. Die Dienstvereinbarung beschränkt insgesamt den Eingriff in das Recht der Beschäftigten auf informationelle Selbstbestimmung auf das zur Erfüllung der Arbeitsaufgaben zwingend notwendige Maß; ein übermäßiger Eingriff wird durch sie nicht erlaubt (vgl. im Einzelnen zu 5 b dd).

c) Die Klägerin hat nicht behauptet, das WSA erhebe, verarbeite oder nutze Daten der Klägerin im Zusammenhang mit dem Einsatz der elektronischen Signaturkarte, Feststellungen hat das Landesarbeitsgericht hierzu nicht getroffen. Allerdings liegt nahe, dass die bei der elektronischen Vergabe notwendigen Außenverbindungen zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitung in streng zweckgebundenen Protokolldateien registriert werden (§ 14 Abs. 4 BDSG; vgl. zum Inhalt der Zweckbindung zB Simitis/Dammann BDSG § 14 Rn. 114). Dabei ergeben sich durch den Einsatz der elektronischen Signaturkarte keine Besonderheiten. Vielmehr erhöht diese die Sicherheit, dass der Kommunikationsinhalt unverändert übermittelt wird und Dritte von dessen Kenntnisnahme ausgeschlossen werden (Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 16). Zur Leistungs- und

Verhaltenskontrolle dürfen eventuell anfallende Daten nach den Bestimmungen der DV Digitale Signaturen nicht genutzt werden.

5. Die Weisung der Beklagten entspricht billigem Ermessen.

a) Eine Leistungsbestimmung entspricht billigem Ermessen, wenn die wesentlichen Umstände des Falls abgewogen und die beiderseitigen Interessen angemessen berücksichtigt worden sind (st. Rspr., zuletzt zB BAG 29. August 2012 - 10 AZR 385/11 - Rn. 45; 12. Oktober 2011 - 10 AZR 746/10 - Rn. 26, BAGE 139, 283). Das bei der Ausübung des Leistungsbestimmungsrechts zu wahrende billige Ermessen wird inhaltlich durch die Grundrechte des Arbeitnehmers mitbestimmt. Kollidieren diese mit dem Recht des Arbeitgebers, dem Arbeitnehmer eine von der vertraglichen Vereinbarung gedeckte Tätigkeit zuzuweisen, sind die gegensätzlichen Rechtspositionen grundrechtskonform auszugleichen (vgl. BAG 24. Februar 2011 - 2 AZR 636/09 - Rn. 23 mwN, BAGE 137, 164; 13. August 2010 - 1 AZR 173/09 - Rn. 10, BAGE 135, 203). Dabei sind die betroffenen Interessen des Arbeitnehmers und des Arbeitgebers im Sinne einer praktischen Konkordanz so abzuwägen, dass die geschützten Rechtspositionen für alle Beteiligten möglichst weitgehend wirksam werden (BAG 23. August 2012 - 8 AZR 804/11 - Rn. 36; 24. Februar 2011 - 2 AZR 636/09 - aaO). Ob die Entscheidung der Billigkeit entspricht, unterliegt der vollen gerichtlichen Kontrolle (BAG 26. September 2012 - 10 AZR 311/11 - Rn. 28; 12. Oktober 2011 - 10 AZR 746/10 - Rn. 46 mwN, aaO).

b) Diese Sachentscheidung ist wegen der zu berücksichtigenden Umstände des Einzelfalls vorrangig den Tatsachengerichten vorbehalten (BAG 12. Oktober 2011 - 10 AZR 746/10 - Rn. 46, aaO; 10. Mai 2005 - 9 AZR 294/04 - zu B II 3 b und B IV 1 der Gründe; vgl. zur Kontroverse über den Umfang der revisionsrechtlichen Überprüfung: GMP/Müller-Glöge 8. Aufl. § 73 Rn. 10). Unabhängig hiervon hält die Entscheidung des Landesarbeitsgerichts auch einer uneingeschränkten Überprüfung stand.

aa) Die Beklagte hat ein berechtigtes Interesse daran, die Vergabe öffentlicher Aufträge mithilfe eines elektronischen Vergabesystems durchzuführen. Wie sich dem Beschluss der Bundesregierung vom 10. Dezember 2003 entnehmen lässt, dient die Einführung des elektronischen Vergabesystems der Steigerung von Effizienz und Kompetenz bei der Beschaffung von Gütern und Dienstleistungen durch die öffentliche Hand. Durch die elektronische Vergabe öffentlicher Aufträge sollen erhebliche Einsparungen sowohl bei den Kosten der Vergabe als auch bei den Preisen für die beschafften Leistungen erzielt werden. Die Einführung des elektronischen Vergabesystems dient damit legitimen Zwecken.

bb) Die Amtsleitung des WSA hat keine Möglichkeit, die Veröffentlichung von Vergabeunterlagen anders zu gestalten. Das WSA ist eine dem BMVBS nachgeordnete Behörde. Der Erlass des BMVBS vom 11. Dezember 2009, nach dem ab dem 1. Januar 2010 alle Vergabebekanntmachungen über die elektronische Vergabeplattform des Bundes zu veröffentlichen sind, ist daher für das WSA bindend (vgl. Ehlers in Erichsen/Ehlers Allgemeines Verwaltungsrecht 13. Aufl. § 2 Rn. 62 ff.). Eine Veröffentlichung der Vergabeunterlagen auf anderem Wege scheidet aus. Das betrifft alle Bediensteten der nachgeordneten Behörden gleichermaßen.

cc) Der Einwand der Klägerin, eine Veröffentlichung der Vergabeunterlagen durch sie selbst sei nicht erforderlich, weil die Unterlagen auch durch Diplom-Ingenieure oder Beschäftigte, die bereits über ein Signaturkarte verfügen, veröffentlicht werden könnten, steht der Weisung der Beklagten nicht entgegen.

(1) Dem Gericht obliegt nicht die Prüfung, ob die Weisung der Beklagten die beste, effizienteste oder wirtschaftlich vernünftigste Lösung darstellt. Im Rahmen der Ausübung des Direktionsrechts steht dem Arbeitgeber ein nach billigem Ermessen auszufüllender Entscheidungsspielraum zu. Innerhalb dieses Spielraums können ihm mehrere Entscheidungsmöglichkeiten zur Verfügung stehen. Dem Gericht obliegt (lediglich) die Prüfung, ob der Arbeitgeber als Gläubiger die Grenzen seines Bestimmungsrechts beachtet hat (vgl. BAG 26. September 2012 - 10 AZR 311/11 - Rn. 28; 13. Juni 2012 - 10 AZR 296/11 - Rn. 28; BGH 18. Oktober 2007 - III ZR 277/06 - Rn. 20, BGHZ 174, 48).

(2) Das ist hier der Fall. Die Diplom-Ingenieure sind für die Erstellung und den Inhalt der Vergabeunterlagen verantwortlich. Angesichts ihrer besonderen Ausbildung und Qualifikation ist es nachvollziehbar und nicht zu beanstanden, wenn sich die Beklagte dazu entschließt, sie nicht mit rein administrativen Tätigkeiten wie der Veröffentlichung der Vergabeunterlagen zu betrauen, sondern diese Aufgabe von anderen Beschäftigten erledigen zu lassen. Dass andere Beschäftigte des WSA bereits über eine elektronische Signaturkarte verfügen, lässt das Bedürfnis für die Beantragung und Nutzung einer elektronische Signaturkarte durch die Klägerin ebenfalls nicht entfallen. Abwesenheitszeiten einzelner Mitarbeiter (zB aufgrund von Krankheit oder Urlaub) können es erforderlich machen, dass mehrere Mitarbeiter über eine elektronische Signaturkarte verfügen. Nur so kann sichergestellt werden, dass die Vergabeunterlagen unabhängig von den jeweils in der Dienststelle anwesenden Beschäftigten zeitnah veröffentlicht werden können. Es lag nahe, auch die Klägerin für diese Tätigkeit heranzuziehen, weil die Veröffentlichung von Vergabeunterlagen bereits vor dem 1. Januar 2010 zu ihrem Aufgabengebiet gehörte.

dd) Der mit der Weisung verbundene Eingriff in das Recht der Klägerin auf informationelle Selbstbestimmung ist dieser zumutbar.

(1) Das in Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG verankerte Recht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen und darüber zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (BVerfG 15. Dezember 1983 - 1 BvR 209/83, 1 BVR 269/83 ua - zu C II 1 a der Gründe, BVerfGE 65, 1; 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - Rn. 180, BVerfGE 120, 274). Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden (BVerfG 4. April 2006 - 1 BvR 518/02 - Rn. 69, BVerfGE 115, 320). Dabei kommt es nicht darauf an, ob es sich um Daten der Privat- oder gar der Intimsphäre handelt. Ein „belangloses" Datum gibt es aus Sicht der Verfassung nicht (vgl. BVerfG 15. Dezember 1983 - 1 BvR 209/83, 1 BvR 269/83 ua. - zu C II 2 der

Gründe, aaO). Das Recht auf informationelle Selbstbestimmung findet eine Entsprechung im Unionsrecht. Gemäß Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) In das Recht der Klägerin auf informationelle Selbstbestimmung wird durch die streitgegenständliche Weisung eingegriffen, weil die Klägerin nicht mehr frei entscheiden kann, wann sie wem welche Daten zur Verfügung stellt. Durch die Weisung wird sie verpflichtet, einem von der Beklagten ausgewählten Zertifizierungsdiensteanbieter die aus dem Personalausweis ersichtlichen Daten zur Verfügung zu stellen.

(3) Dieser Eingriff ist der Klägerin zumutbar (ebenso für die an einen Beamten gerichtete Anordnung, eine elektronische Signaturkarte zu beantragen und zu nutzen: Bayer. VGH 2. November 2011 - 6 CE 11.1342 -).

(a) Die Veröffentlichung der Vergabeunterlagen durch die Klägerin ist ohne Eingriff in ihr Recht auf informationelle Selbstbestimmung nicht möglich. Nach den für den Senat bindenden Feststellungen des Landesarbeitsgerichts (§ 559 Abs. 2 ZPO) ist für die Veröffentlichung von Vergabeunterlagen auf der elektronischen Vergabeplattform des Bundes der Einsatz einer elektronischen Signaturkarte unverzichtbar. Dieser Einsatz setzt wiederum zwingend voraus, dass die Klägerin selbst die Karte unter Mitteilung ihrer personenbezogenen Daten beim Zertifizierungsdiensteanbieter beantragt hat. Gemäß § 2 Nr. 7 SigG kann eine elektronische Signaturkarte nur von einer natürlichen Person beantragt werden (vgl. Spindler/Schuster/Gramlich Recht der elektronischen Medien 2. Aufl. § 2 SigG Rn. 16). Die Beantragung einer elektronischen Signaturkarte für die gesamte Dienststelle oder auch nur für mehrere Beschäftigte ist nicht möglich. Auch die Nutzung einer für einen anderen Beschäftigten ausgestellten elektronischen Signaturkarte durch die Klägerin kommt nicht in Betracht, weil die mit der Signaturkarte verbundenen Rechte nur von den jeweiligen Antragstellern ausgeübt werden dürfen; dies legt die DV Digitale Signaturen („Rechte und Pflichten") ausdrücklich fest. Im Übrigen würde eine solche Handhabung dem Zweck der elektronischen Signaturkarte als sicherem Identifizierungsmittel des jeweiligen Absenders zuwiderlaufen.

(b) Die Weisung stellt keinen besonders schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die aus dem Personalausweis ersichtlichen Daten betreffen den äußeren Bereich der Privatsphäre. Insbesondere Name, Alter und Adresse gehören zu den „Stammdaten" des Arbeitnehmers, deren Erhebung für die Durchführung eines Arbeitsverhältnisses regelmäßig erforderlich ist (BAG 23. August 2012 - 8 AZR 804/11 - Rn. 38 mwN). Diese Daten werden auch im allgemeinen Geschäftsverkehr häufig eingesetzt. Bei den Angaben im Personalausweis handelt es sich nicht um besonders sensible Daten iSv. § 3 Abs. 9 BDSG, für die nach § 4a Abs. 3, § 28 Abs. 6 bis Abs. 9 BDSG erhöhte Anforderungen an die Erhebung und Speicherung zu stellen sind (vgl. zum Umgang mit solchen Daten im Rahmen der Personalaktenführung: BAG 12. September 2006 - 9 AZR 271/06 - BAGE 119, 238). Dass die Angaben - insbesondere das Passfoto und die ausgewiesene Staatsangehörigkeit - mittelbar Rückschlüsse auf die ethnische Herkunft zulassen, reicht für eine Anwendung der genannten Vorschriften nicht aus,

weil eine entsprechende Auswertungsabsicht nicht besteht; die Datenerhebung dient allein der Identifizierung (vgl. Gola/Schomerus BDSG § 3 Rn. 56a; zur Abgrenzung von Staatsangehörigkeit und ethnischer Herkunft: BAG 21. Juni 2012 - 8 AZR 364/11 - Rn. 31).

Darüber hinaus werden die Daten nicht der allgemeinen Öffentlichkeit oder einer unbestimmten Anzahl von Personen bekannt gegeben, sondern nur einem einzigen Zertifizierungsdiensteanbieter übermittelt. Dieser darf die Daten zudem nur insoweit erheben und nutzen, als dies für Zwecke einer elektronischen Signaturkarte erforderlich ist (§ 14 Abs. 1 Satz 1 SigG). Zu anderen Zwecken dürfen die Daten nur verwendet werden, wenn das SigG es erlaubt oder der Betroffene eingewilligt hat (§ 14 Abs. 1 Satz 3 SigG).

(c) Der Schutz der personenbezogenen Daten der Klägerin wird durch Vorschriften des Signaturgesetzes und der Signaturverordnung sichergestellt. Einen Zertifizierungsdienst darf danach nur anbieten, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde nachweist (§ 4 Abs. 2 Satz 1 SigG) und der zuständigen Behörde ein Sicherheitskonzept vorgelegt hat, in dem die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach dem SigG und der SigV im Einzelnen aufgezeigt werden (§ 4 Abs. 2 Satz 4 SigG, § 2 SigV). Der Zertifizierungsdiensteanbieter hat für die Ausübung der Zertifizierungstätigkeit zuverlässiges Personal und zuverlässige Produkte für elektronische Signaturen einzusetzen (§ 5 Abs. 5 SigG, § 5 Abs. 3 SigV). Die Daten eines Antragstellers dürfen nur unmittelbar bei diesem selbst und grundsätzlich nur für Zwecke einer elektronischen Signaturkarte erhoben werden (§ 14 Abs. 1 Satz 1 SigG). Der Zertifizierungsdiensteanbieter hat das Sicherheitskonzept einschließlich etwaiger Änderungen, die Unterlagen zur Fachkunde der im Betrieb tätigen Personen und die vertraglichen Vereinbarungen mit den Antragstellern zu dokumentieren (§ 10 Abs. 1 SigG, § 8 SigV). Dem Antragsteller ist auf Verlangen jederzeit Einblick in die ihn betreffenden Daten zu gewähren (§ 10 Abs. 2 SigG).

Über diese zwingenden gesetzlichen Vorgaben hinaus bestimmt die DV Digitale Signaturen, dass als Zertifizierungsdiensteanbieter nur solche in Betracht kommen, die sich gemäß § 15 ff. SigG bei der zuständigen Behörde freiwillig akkreditiert haben. Die freiwillige Akkreditierung beinhaltet eine regelmäßige Überprüfung des Sicherheitskonzepts des Zertifizierungsdiensteanbieters durch öffentlich anerkannte fachkundige Dritte (§ 15 Abs. 2, § 18 SigG) und gewährleistet damit ein Sicherheitskonzept von besonders hoher Qualität (vgl. Spindler/Schuster/Gramlich Recht der elektronischen Medien § 15 SigG Rn. 6; Roßnagel/Roßnagel Handbuch Datenschutzrecht Abschnitt 7.7 Rn. 26). noDer von der Beklagten ausgewählte Zertifizierungsdiensteanbieter entspricht diesen Vorgaben.

(d) Angesichts der Sicherheitsvorkehrungen bestehen keine Anhaltspunkte für die Befürchtung der Klägerin, mit ihren Daten könnte Missbrauch getrieben werden. Konkrete Tatsachen, die auf die Möglichkeit eines Missbrauchs hindeuten, hat die Klägerin nicht vorgetragen. Die Beklagte hat die Bedenken der Klägerin dennoch aufgegriffen und sich bei der gemäß § 3 SigG zuständigen Bundesnetzagentur nach der Reputation der T GmbH erkundigt. Auch nach Auskunft der Bundesnetzagentur

besteht kein Anlass, an der Datensicherheit und der Integrität der Systeme zu zweifeln.

ee) Die Weisung der Beklagten stellt zwar einen Eingriff in die durch Art. 2 Abs. 1 GG geschützte Vertragsfreiheit (vgl. BVerfG 16. Juli 2012 - 1 BvR 2983/10 - Rn. 21 mwN) der Klägerin dar, weil sie verpflichtet wird, gegen ihren Willen ein Vertragsverhältnis mit dem Zertifizierungsdiensteanbieter einzugehen. Dieser Eingriff ist der Klägerin aber ebenfalls zumutbar. Zur Begründung kann auf die obigen Ausführungen verwiesen werden. Ergänzend ist zu berücksichtigen, dass der vom Arbeitgeber geforderte Vertragsschluss einen unmittelbaren Bezug zur geschuldeten Arbeitsleistung aufweist und der Klägerin durch ihn keine Zahlungspflichten auferlegt werden. Sämtliche Kosten für die Leistungen des Zertifizierungsdiensteanbieters trägt nach der DV Digitale Signaturen die Beklagte.

ff) Soweit die Weisung die Verpflichtung der Klägerin beinhaltet, die elektronische Signaturkarte bei der Veröffentlichung der Vergabeunterlagen zu nutzen, begegnet sie ebenfalls keinen Bedenken. Besondere, speziell mit der dienstlichen Nutzung der elektronischen Signaturkarte für sie verbundene Gefahren benennt die Klägerin nicht. Die Klägerin hat nach den Bestimmungen der DV Digitale Signaturen einen Schulungsanspruch gegenüber der Beklagten; die Dienstvereinbarung legt bestimmte Verhaltensweisen zur sicheren Nutzung durch die Beschäftigten fest. Den Interessen der Klägerin wird zudem durch eine Haftungsfreistellung Rechnung getragen: Nach der DV Digitale Signaturen stellt das BMVBS die Beschäftigten von etwaigen Haftungsansprüchen des Zertifizierungsdiensteanbieters oder anderer Dritter frei, die im Zusammenhang mit einer fehlerhaften Nutzung der Signaturkarte zu dienstlichen Zwecken erhoben werden können. Die DV Digitale Signaturen („Anwendung") stellt schließlich klar, dass aufgrund des Einsatzes der elektronischen Signaturkarte beim Arbeitgeber gewonnene Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden dürfen. Eine Nutzung der elektronischen Signaturkarte über den dienstlichen Einsatz hinaus, insbesondere zu privaten Zwecken, wird von der Klägerin nicht verlangt.

5 ArbG Augsburg, Mitarbeiterüberwachung - heimliche Installation und Anwendung eines Computerkontrollprogramms

ArbG Augsburg, 04.10.2012, 1 BV 36/12

Leitsatz

1. Die durch die heimliche Installation und Anwendung eines Computerkontrollprogramms gewonnenen Daten können zum Zwecke des Nachweises, dass nachträglich durchgeführte Änderungen im elektronischen Arbeitszeitkonto eines Arbeitnehmers von dessen Computer aus durchgeführt worden sind nach den von der Rechtsprechung des Bundesarbeitsgerichts zur heimlichen Videoüberwachung aufgestellten Grundsätzen (vgl. zuletzt BAG Urteil vom 21.06.2012 - 2 AZR 153/11) bzw. unter den Voraussetzungen des § 32 Abs 1 S 2 BDSG prozessual verwertbar sein.

2. Es stellt ein Übermaß an Kontrolle und einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht des kontrollierten Arbeitnehmers dar, wenn das Computerkontrollprogramm nicht nur Zugriffe auf das in Frage stehende Arbeitszeitkonto aufzeichnet, sondern bei Verlassen oder Unterbrechen des Arbeitszeitprogramms durch den Anwender bis zum Ende des vorgesehenen Zeitintervalls weiterläuft und dadurch die bis dahin auf dem Bildschirm des Arbeitnehmers stattfindenden Aktivitäten erfasst, obwohl diese mit dem Arbeitszeitkonto des Arbeitnehmers nichts mehr zu tun haben, und jedenfalls ein automatisches Abschalten des Kontrollprogramms in solchen Fällen technisch möglich ist.

3. Der unverhältnismäßige Eingriff in das Persönlichkeitsrecht des Arbeitnehmers führt dazu, dass das Interesse des Arbeitgebers an einer prozessualen Verwertung des mit dem heimlich installierten Kontrollprogramms gewonnenen Beweismaterials gegenüber dem Schutz des informationellen Selbstbestimmungsrechts des Arbeitnehmers zurückzutreten hat.

Gründe

I.

Die Beteiligten streiten über einen Antrag der Arbeitgeberin (Beteiligte zu 1) auf gerichtliche Ersetzung der verweigerten Zustimmung des in ihrem Betrieb gebildeten Betriebsrats (Beteiligter zu 2) zu einer beabsichtigten außerordentlichen Kündigung des Betriebsratsvorsitzenden F. (Beteiligter zu 3).

Die Beteiligte zu 1) beschäftigt in ihrem Produktionsbetrieb 475 Mitarbeiter. Es ist ein elfköpfiger Betriebsrat errichtet, dessen Vorsitzender der Beteiligte zu 3) ist.

Der am…geborene Beteiligte zu 3) ist bei der Beteiligten zu 1) seit dem 01.02.2000 gegen eine monatliche Bruttovergütung von zuletzt 4.655,62 € beschäftigt. Er ist mit einem Grad von 50 (GdB) schwerbehindert und gem. § 38 Abs. 1 BetrVG von seiner beruflichen Tätigkeit in vollem Umfang freigestellt. Nach dem bei der Beteiligten zu 1) bestehenden elektronischem Zeiterfassungssystem hält der Beteiligte zu 3) bei Beginn und Ende der Arbeitszeit einen blauen personalisierten Chip an das Zeiterfassungsterminal. Dadurch wird eine elektronische Buchung im Interflex-Arbeitszeitprogramm vorgenommen, die den Beginn der Arbeitszeit minutengenau festhält. Ebenso verhält es sich beim "Ausstempeln". Alle Mitarbeiter der Personalabteilung haben über einen persönlichen User-Namen und einem dazugehörigen Passwort eine Zugriffsberechtigung auf alle Arbeitszeitdaten der Mitarbeiter verbunden mit der Berechtigung, diese manuell zu ändern. Ebenso haben die beiden Mitarbeiter der EDV-Abteilung mittels eines zentralen Administratoren-Benutzernamens "EDV" Zugriff auf das Interflex-Arbeitszeitprogramm. Dieser Nutzername ist aufgrund der Notwendigkeit, EDV-technische Installationsarbeiten u. s. w. vorzunehmen, mit umfassenden Rechten versehen. Schließlich hat auch der externe Dienstleister der Beteiligten zu 1), die Fa. N. die Möglichkeit, im Arbeitszeitprogramm Änderungen vorzunehmen. Neben den Schicht- und Abteilungsleitern haben die fünf Mitglieder des Betriebsausschusses des Beteiligten zu 2) sowie zwei Ersatzmitglieder ein Leserecht für das Arbeitszeitsystem, jedoch

keine Berechtigung zur Änderung der Daten. Zur Ausübung dieses Leserechts wurden dem Beteiligten zu 2) von der Beteiligten zu 1) zwei Passwörter zur Verfügung gestellt, von denen eines der stellvertretende Betriebsratsvorsitzende und das andere die übrigen leseberechtigten Betriebsratsmitglieder benutzen. Der Beteiligte zu 2) verfügt über drei Rechner sowie einem Laptop. Ein Rechner sowie der Laptop befinden sich im Büro des Beteiligten zu 3), die beiden anderen Rechner im Büro der stellvertretenden Betriebsratsvorsitzenden. Der Beteiligte zu 3) kann mit dem Laptop von zu Hause aus über seinen Router auf das Arbeitszeitkonto bei der Beteiligten zu 1) zugreifen (Bl. 701 d. A.).

Aufgrund einer am 10.01.2012 festgestellten nachträglich am 09.01.2012 mit dem Benutzernamen "EDV" Nr. 79 vorgenommenen Änderung des Arbeitszeitkontos des Beteiligten zu 3) im Interflex-Arbeitszeitprogramm betreffend den 09.12.2011 überprüfte die Beteiligte zu 1) die Arbeitszeitdaten des Beteiligten zu 3) im Arbeitszeitprogramm bis in das Jahr 2010 zurück. Dabei wurde festgestellt, dass das Arbeitszeitkonto des Beteiligten zu 3) im Zeitraum vom 05.05.2010 bis 14.12.2011 mit dem Benutzernamen 79 = "EDV" jeweils nachträglich manuell abgeändert worden ist. Diese Abänderungen führten in diesem Zeitraum insgesamt zu einer Ausweitung der geleisteten Arbeitszeiten des Beteiligten zu 3) von rund 165 Stunden. Hinsichtlich der jeweils nachträglich geänderten Arbeitszeiten wird im Einzelnen auf Bl. 36 bis 38 d. A. Bezug genommen. Eine Überprüfung der Originalstempelzeiten des Beteiligten zu 3) ergab, dass dieser mit Ausnahme des 03.09.2011 zu allen Änderungszeitpunkten im Betrieb anwesend war. Von welchem Rechner aus die Änderungen durchgeführt worden waren wurde im Interflex-Arbeitszeitprogramm nicht protokolliert. Um diesen Rechner zu lokalisieren, ließ die Beteiligte zu 1) ohne Beteiligung des Beteiligten zu 2) ein Programm installieren, das alle Anmeldedaten an das Arbeitszeitprogramm aller Computer protokollierte. Da diese Vorgehensweise sich für die Beteiligte zu 1) als nicht praktikabel herausstellte, ließ sie am 16.04.2012 ebenfalls ohne Beteiligung des Beteiligten zu 2) ein Programm auf dem Rechner des Beteiligten zu 3 installieren, um damit feststellen zu können, ob bzw. dass von diesem Rechner aus der Zugriff stattfinde. Am 03.05.2012 erstellte dieses Programm sogenannte Screenshots, aus denen sich ergibt, dass an diesem Tag gegen 8.43 Uhr in das Interflexsystem unter Eingabe des Benutzernamens "EDV" und des dazugehörigen Passworts eingeloggt wurde. Dabei wurde der 24.04.2012 aufgerufen, der bisher keine Kommens- und Gehenszeit ausgewiesen hatte. Um 8.44 Uhr und 39 Sekunden wurde sodann eine Neubuchung vorgenommen, die für den 24.04.2012 einen Arbeitszeitbeginn um 6.30 Uhr und ein Arbeitszeitende um 15.45 Uhr ausweist. Während dieser Aufzeichnung durch das Kontrollprogramm wurde ebenfalls mit aufgezeichnet, dass von dem Arbeitsplatzrechner des Beteiligten zu 3) über das Internet in dessen privaten E-Mail-Account eingeloggt und dort private E-Mails bearbeitet wurden. Im Einzelnen wird auf Bl. 225 bis 432 d. A. sowie auf die Anlage 34 Bezug genommen.

Der Beteiligte zu 3) wurde am 10.05.2012 hierzu zunächst mündlich und mit Schreiben vom selben Tag schriftlich angehört (Bl. 434/435 d. A.). Der Beteiligte zu 3) erwiderte am 11.05.2012, dass er seinen Ausführungen vom 10.05.2012 nichts mehr hinzuzufügen habe. Seinen Anwalt werde er erst am Montag sprechen können. Daraufhin verlängerte die Beteiligte zu 1) dem Beteiligten zu 3) die Frist zur

Stellungnahme bis zum 14.05.2012, 15.00 Uhr, um ihm noch Gelegenheit zur Besprechung mit seinem Anwalt zu geben (Bl. 447 d. A.). Nach Eingang einer schriftlichen Stellungnahme des Anwalts des Beteiligten zu 3) am 14.05.2012 beantragte die Beteiligte zu 1) noch am selben Tag beim Integrationsamt die Zustimmung zu einer außerordentlichen fristlosen Verdachtskündigung des Beteiligten zu 3). Mit Schreiben vom 29.05.2012 teilte das Integrationsamt der Beteiligten zu 1) mit, dass die Zustimmung zur außerordentlichen Kündigung des Beteiligten zu 3) nach § 91 Abs. 3 Satz 2 SGB IX als erteilt gelte (Bl. 511 bis 513). Daraufhin wurde dem Betriebsrat am 30.05.2012 das Anhörungsschreiben zu einer beabsichtigten außerordentlichen Verdachtskündigung des Beteiligten zu 3) nebst 16 Anlagen ausgehändigt. Hinsichtlich des Inhalts dieses Anhörungsschreibens wird im Einzelnen auf Bl. 515 bis 525 d. A. Bezug genommen. Am 04.06.2012 teilte der Beteiligte zu 2) der Beteiligten zu 1) mit, dass er die Zustimmung nicht erteile.

Die Beteiligte zu 1) trägt vor, der Beteiligte zu 2) habe die Zustimmung zu der beabsichtigten außerordentlichen Kündigung des Beteiligten zu 3) zu Unrecht nicht erteilt. Die Zustimmung sei daher antragsgemäß vom angerufenen Arbeitsgericht zu ersetzen. Vorliegend hätten sich schwerwiegende Verdachtsmomente ergeben, die auf objektiven Tatsachen beruhten und zu einer fristlosen Kündigung berechtigten. Die unberechtigten Manipulationen des Arbeitszeitkontos des Beteiligten zu 3) seien immer unter dem User-Namen "EDV" Nr. 79 vorgenommen worden. Mit diesem User-Namen sei ausschließlich Zugriff auf das Arbeitszeitkonto des Beteiligten zu 3) genommen worden. Die Manipulationen seien immer zugunsten des Beteiligten zu 3) erfolgt und hätten damit zu einer Verlängerung der bisher gebuchten Arbeitszeiten geführt. Die Änderungszeitpunkte stimmten mit den Anwesenheitszeiten in allen Fällen außer dem 03.09.2011 überein, die größeren Pausen zwischen den Manipulationen mit den Fehlzeiten des Beteiligten zu 3).

Die am 03.05.2012 auf dem Arbeitszeitkonto des Beteiligten zu 3) vorgenommene unerlaubte Manipulation der Arbeitszeiten zu seinen Gunsten sei vom Rechner des Beteiligten zu 3) aus erfolgt. Das auf dem Betriebsratsrechner des Beteiligten zu 3) installierte Programm sei so konzipiert, dass es sich erst dann aktiviere, wenn das Interflex-Arbeitszeitprogramm gestartet werde und dann in einem Zeitraum von 5 Minuten ab Aktivierung in sekündlichen Abständen sogenannte Screenshots mache, um den Anmeldevorgang und gegebenenfalls im Anschluss daran durchgeführte Arbeitszeitänderungen darstellen zu können. Nach 5 Minuten deaktiviere sich das Programm wieder. Dieses Programm sei auf keinem anderen Rechner installiert worden. Am 03.05.2012 seien auf dem Arbeitszeitkonto des Beteiligten zu 3) für den 24.04.2012 Arbeitszeiten nachträglich eingetragen worden, obwohl der Beteiligte zu 3) zu keinem Zeitpunkt an diesem Tag im Betrieb der Beteiligten zu 1) gewesen sei. Da der Beteiligte zu 3) sein eigenes Arbeitszeitkonto jederzeit sehr genau beobachte und vermeintliche Fehlbuchungen stets sofort reklamiert habe, sei anzunehmen, dass er die Veränderungen zu seinen Gunsten bemerkt jedoch zu keiner Zeit der Beteiligten zu 1) angezeigt habe. Deshalb bestehe der schwerwiegende Verdacht, dass der Beteiligte zu 3) zu seinen Gunsten sein Arbeitszeitkonto manipuliert habe. Die im Zeitkonto des Beteiligten zu 3) vorgenommenen Manipulationen hätten dazu geführt, dass zum Quartalsende, dem Stichtag, an dem die Arbeitszeitsalden geprüft würden, ein meist ausgeglichenes Zeitkonto vorgelegen habe, das Zeitkonto kein

oder nur ein geringes Minus aufgewiesen habe. Die durchgeführten Arbeitszeiterhöhungen hätten damit sichergestellt, dass das Monatsgehalt in vollem Umfang ausgezahlt werde und zu wenig geleistete Stunden gerade nicht am Monatsende in Abzug gebracht worden seien oder aber durch ein künftiges Mehr an Anwesenheit im Betrieb vom Beteiligten zu 3) auszugleichen gewesen seien (hinsichtlich der jeweiligen Arbeitszeitdifferenzen wird im Einzelnen auf Bl. 591 bis 593 d. A. Bezug genommen).

Für den Einsatz des Interflex-Arbeitszeitprogramms bestehe auch eine betriebsverfassungsrechtliche Grundlage, da die Betriebsparteien ausweislich der "Betriebsvereinbarung Arbeitszeitkorrekturen" darin übereinstimmten, dass dieses Programm im Betrieb der Beteiligten zu 1) angewendet werde und damit personenbezogene Daten erhoben, verarbeitet und gespeichert würden.

Die heimlichen Aufzeichnungen mittels des auf dem Rechner des Beteiligten zu 3) installierten Programms unterlägen keinem Beweisverwertungsverbot. Zwar stelle die heimliche Datenaufzeichnung über den Rechner des Beteiligten zu 3) einen Eingriff in das Persönlichkeitsrecht des Beteiligten zu 3) dar. Dieses werde nach der höchstrichterlichen Rechtsprechung aber nicht schrankenlos gewährleistet. Bestünden überwiegende schutzwürdige Interessen des Arbeitgebers, könne ein solcher Eingriff gerechtfertigt sein. Vorliegend habe der konkrete Verdacht einer strafbaren Handlung oder aber einer anderen schweren Verfehlung zu Lasten der Beteiligten zu 1) bestanden. Weniger einschneidende Mittel zur Aufklärung des Verdachts seien ausgeschöpft gewesen und hätten sich darüber hinaus nicht ergeben. Die heimliche Überwachung des Computer des Beteiligten zu 3) ausschließlich im Falle des Einloggens auf das Interflex-Arbeitszeitprogramm und dies auch nur für eine Höchstzeit von jeweils 5 Minuten sei praktisch das einzig verbleibende Mittel gewesen, um auszuschließen, dass andere Mitarbeiter eine solche Manipulation begangen hätten bzw. um festzustellen, dass der Beteiligte zu 3) derjenige gewesen sei der die Manipulationen vorgenommen habe. Die mit dem Programm aufgenommenen Bilder seien zugriffsgeschützt mit Datum, Zeit, User-Name und Computername als Dateiname abgelegt worden. Die Beteiligte zu 1) habe auf diese Daten nicht zugreifen können. Der Zugriff habe nur durch den mit der Programmerstellung von N. beauftragten Mitarbeiter, dem Zeugen C., erfolgen können. Bei Meldung der Datenmanipulation am 03.05.2012 durch die Beteiligte zu 1) seien ausschließlich die Daten dieses Vorgangs der Beteiligten zu 1) zur Verfügung gestellt worden. Mit dieser Vorgehensweise sei sichergestellt worden, dass ein möglichst geringer Eingriff in das Persönlichkeitsrecht des Beteiligten zu 3) begangen werde. Es sei nur der Zugriff auf das Arbeitszeitprogramm des Beteiligten zu 3) überwacht worden, alle anderen Daten, die auf diesem Computer abgelegt worden seien, hätten mit Hilfe des Kontrollprogramms nicht gelesen werden können. Dass der Beteiligte zu 2) vor Durchführung der Überwachungsmaßnahme nicht gem. § 87 Abs. 1 Nr. 6 BetrVG beteiligt worden sei, führe noch nicht zu einem Verwertungsverbot. Hinzu kommen müsse eine erhebliche Verletzung des allgemeinen Persönlichkeitsrechts des Arbeitnehmers. Dabei könnten Eingriffe in das Persönlichkeitsrecht durch die Wahrnehmung überwiegender schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein.

Die Beteiligte zu 1) habe sich aufgrund der vorliegenden rechtswidrigen Angriffe in einer Notwehrsituation bzw. notwehrähnlichen Lage befunden. Der rechtswidrige Angriff des Täters sei heimlich erfolgt. Dem heimlich vorgehenden Täter könne nur mit Heimlichkeit begegnet werden. Die Überwachung des verdächtigen Rechners sei das einzig verbleibende Mittel gewesen, um den Täter weitestgehend zu identifizieren. Weniger einschneidende Mittel hätten nicht zur Verfügung gestanden. Die Überwachung sei nicht unverhältnismäßig gewesen, da sie inhaltlich und zeitlich auf das Notwendigste beschränkt gewesen sei (Bl. 11 bis 16 und 591 bis 604 d. A.).

Die Beteiligte zu 1) beantragt deshalb:

Die Zustimmung des Betriebsrats zur außerordentlichen Kündigung des Beteiligten F. wird ersetzt.

Die Beteiligten zu 2) und 3) beantragen,

diesen Antrag zurückzuweisen.

Der Beteiligte zu 2) führt aus, die Überwachungen des Beteiligten zu 3) seien wesentlich weiter gegangen, als die Beteiligte zu 1) im Anhörungsverfahren gegenüber dem Beteiligten zu 2) angegeben habe. Damit sei die Anhörung unvollständig, fehlerhaft und lückenhaft gewesen und habe den Erfordernissen der § 102 bzw. 103 BetrVG nicht genügt.

Die Betriebsräte sowie der Beteiligte zu 3) hätten mit ihrem Passwort lediglich Einsicht auf Personal- und Zeiterfassungsdaten nehmen können. Sie hätten nicht die Möglichkeit gehabt, an den Stammdaten oder im Zeiterfassungssystem in irgendeiner Art und Weise Änderungen vorzunehmen. Der Beteiligte zu 2) habe auch keinerlei Motiv erkennen können, welches den Beteiligten zu 3) veranlasst haben sollte, die behaupteten Manipulationen vorzunehmen.

Der Beteiligte zu 3) hätte als Festlohnempfänger und nach § 38 BetrVG freigestellter Betriebsratsvorsitzender keinerlei Vermögensvorteil durch die behauptete Datenmanipulation erlangen können. Auf den Betriebsrats-PC könne jedes Betriebsratsmitglied zugreifen und arbeite auch mit diesem. Der Betriebsrats-PC habe nicht gegen den Zugriff Dritter geschützt werden können, zumal er nicht abgeschaltet worden sei, um u. a. auch den Zugriff vom Home-Office aus durch den Beteiligten zu 3) zu ermöglichen. Auch lägen Passwörter, mit denen die Interflex-Zugangsdaten geändert werden könnten, nicht nur in einem Speichermedium, auf welches nur Herr L. zugreifen könne, sondern auch die Personalleitung, die Geschäftsleitung, die EDV und wohl auch die N. könnten hierauf zugreifen. Auch habe der Beteiligten zu 1) zu keinem Zeitpunkt das Recht zugestanden, die Erfassung von Anwesenheitszeiten eines Betriebsratsmitglieds in einer bestimmten Form und nach einem bestimmten Verfahren einzufordern. Die Beteiligte zu 1) habe das Recht des Beteiligten zu 2) auf informationelle Selbstbestimmung und das Besitzrecht des Beteiligten zu 2) an seinen Sachmitteln in eklatantem Maße verletzt. Auch sei die Vorschrift des § 87 Abs. 1 Nr. 1 und 6 BetrVG mit der Folge missachtet worden, dass sämtliche hieraus entstehenden Handlungen rechtswidrig seien und die hieraus erlangten Erkenntnisse einem Verwertungsverbot des Gerichts unterlägen. Die Eingriffe in das Persönlichkeitsrechts des Beteiligten zu 3) sowie die begehrte

außerordentliche Kündigung seien unverhältnismäßig (Bl. 582 bis 584 d. A., 651 bis 653 d. A.).

Der Beteiligte zu 3) führt aus, in der Anhörung werde nicht vorgetragen, dass die Datenänderungen falsch seien. Die Beteiligte zu 1) rüge nur unsubstantiiert, dass der Beteiligte zu 3) Zeiten geändert habe. Auch fehlten in der Anhörung entlastende Argumente. Insbesondere sei nicht angegeben, dass man über den 03. Mai hinaus den Betriebsratscomputer überwacht habe, aber offensichtlich nach diesem Zeitpunkt keinerlei belastende Indizien gegen den Beteiligten zu 3) erlangt habe. Für den Einsatz der Software Interflex fehle eine betriebsverfassungsrechtliche Grundlage. Es bestehe kein System gesicherter Passwortvergabe. Die Betriebsvereinbarung zur Regelung der Arbeitszeitkorrekturen sei zeitlich nach der einseitig durch die Beteiligte zu 1) veranlassten Einführung des elektronischen Zeiterfassungssystems eingeführt worden und könne damit nicht die Einführung und Anwendung einvernehmlich regeln.

Aufgrund der Unwirksamkeit der Einführung dieses Systems müsse ein manipulierender Eingriff von außen stets ohne Sanktion bleiben, da die elektronische Zeiterfassung kein geltendes und somit verpflichtendes Element der betrieblichen Handhabe sei. Auch fehle es bereits an einem konkreten Verdacht, da die Beteiligte zu 1) nicht vortrage, wie der Beteiligte zu 3) sich ein Passwort angeeignet haben solle. Der Datenzugriff auf den PC des Beteiligten zu 23) sei nach Prüfung eines Computerexperten seitens des Beteiligten zu 2) von Dritten Computern möglich. Die Datengewinnung, die auf einer unwirksamen und damit rechtswidrigen mitbestimmungsverletzenden Maßnahme herrühre, führe folgerichtig zu einem Beweisverwertungsverbot (Bl. 540, 634 bis 639 d. A.).

Ergänzend zum Sachvortrag der Beteiligten wird auf die gewechselten Schriftsätze nebst Anlagen sowie auf die Sitzungsniederschrift vom 13.09.2012 (Bl. 669 bis 706 d. A.) Bezug genommen.

Es ist Beweis erhoben worden durch Einvernahme des Zeugen C.. Bezüglich des Ergebnisses dieser Beweisaufnahme wird auf die Niederschrift vom 13.09.2012 (Bl. 703 bis 705 d. A.) verwiesen.

II.

A.

Der Antrag ist zulässig.

Der Rechtsweg zu den Gerichten für Arbeitssachen ist nach den §§ 2 a Abs. 1 Nr. 1 ArbGG, 103 BetrVG gegeben.

Die örtliche Zuständigkeit des Arbeitsgerichts Augsburg ergibt sich aus § 82 Abs. 1 Satz 1 ArbGG.

Das Beschlussverfahren ist vorliegend auch die gebotene Verfahrensart (§§ 80 Abs. 1, 2 a Abs. 1 Nr. 1 ArbGG.

Beteiligter ist, wer von der zu erwartenden Entscheidung in einem betriebsverfassungsrechtlichen Recht oder Rechtsverhältnis unmittelbar betroffen wird.

Die Antrags- und Beteiligungsbefugnis der Beteiligten zu 1) ergibt sich aus § 103 Abs. 2 Satz 1 BetrVG.

Die Beteiligungsbefugnis des Beteiligten zu 2) ergibt sich bereits daraus, dass es vorliegend um die Ersetzung der von ihm nicht erteilten Zustimmung zur beabsichtigten außerordentlichen Kündigung des Beteiligten zu 3) durch die Beteiligte zu 1) geht.

Der Beteiligte zu 3) ist seinerseits nach § 103 Abs. 2 Satz 2 BetrVG zu beteiligen.

B.

Der Antrag ist jedoch unbegründet, weil nach dem Ergebnis der Beweisaufnahme der beabsichtigten außerordentlichen fristlosen Kündigung des Beteiligten zu 3) ein prozessuales Verwertungsverbot entgegensteht.

1.

Die beabsichtigte außerordentliche fristlose Kündigung wäre nicht nach § 102 Abs. 1 Satz 3 BetrVG unwirksam.

Der Betriebsrat ist ordnungsgemäß angehört, wenn ihm der Arbeitgeber die aus seiner Sicht tragenden Umstände unterbreitet hat (BAG AP Nr. 236 zu § 626 BGB).

Entgegen den Ausführungen des Beteiligten zu 2) hat ihm die Beteiligte zu 1) die "Erkenntnisse über die E-Mails und den Posteingang des Beteiligten zu 3)" mitgeteilt. Hierzu heißt es im "Antrag auf Zustimmung zu einer beabsichtigten außerordentlichen fristlosen Verdachtskündigung des Arbeitnehmers F. gem. § 102 Abs. 1, Abs. 2, Satz 3, 103 Abs. 1 BetrVG" auf Seite 7 (Bl. 521 d. A.):

"Während der fünfminütigen Aufzeichnung durch das Programm wurde ebenfalls mit aufgezeichnet, dass sich Herr F. von seinem Arbeitsplatzrechner aus via Internet in seinen privaten EMail-Account einloggte und dort private E-Mails bearbeitete (Anlage 10)".

Die dem Beteiligten zu 2) mit diesem Antragsschreiben u. a. übergebene Anlage 10 enthält auch die vom auf dem Rechner des Beteiligten zu 3) installierten Kontrollprogramm gefertigten Screenshots über die private E-Mail Bearbeitung (Bl. 314 ff. d. A.).

Dem Beteiligten zu 2) wurde darüber hinaus als Anlage 7 die Auswertungsliste (Änderungsprotokoll), aus der sich die rückwirkenden manuellen Arbeitszeitänderungen auf dem Arbeitszeitkonto des Beteiligten zu 3) über den Benutzernamen 79 = "EDV" für den Zeitraum vom 05.05.2010 bis zum 24.04.2012 im Einzelnen entnehmen lassen (Bl. 30 bis 38 d. A.), übergeben.

Weiterhin ergeben sich aus den als Anlage 9 dem Beteiligten zu 2) übergebenen Screenshots u. a. die mit dem Benutzername "EDV" vorgenommenen nachträglichen Änderungen (Bl. 46 ff. d. A.).

Aus der Anhörung ergibt sich auch hinreichend deutlich, dass die von der Beteiligten zu 1) vorgetragenen Datenänderungen von ihr als unzutreffend behauptet worden sind. So heißt es im Zustimmungsantrag u. a.:

"4. Hieraus ergab sich ein sehr konkreter Verdacht, dass Herr F. derjenige war, der die unberechtigten rückwirkenden Änderungen an seinem Arbeitszeitkonto im Interflex-Arbeitszeitprogramm durchgeführt hat" (Bl. 519 d. A.).

"Die unberechtigten Manipulationen des Arbeitszeitkontos von Herrn F. wurden immer unter dem User-Namen "EDV" Nr. 79 vorgenommen" (Bl. 522 d. A.).

"Aus den oben dargestellten Fakten ergibt sich, dass der konkrete Verdacht einer strafbaren Handlung oder aber einer anderen schweren Verfehlung zu unseren Lasten bestand" (Bl. 524 d. A.).

Der Beteiligte zu 2) wendet darüber hinaus ein, in der Anhörung sei insbesondere nicht angegeben, dass man über den 03. Mai hinaus den Betriebsratscomputer überwacht habe, aber offensichtlich nach diesem Zeitpunkt keinerlei belastende Indizien gegen den Betriebsratsvorsitzenden erlangt habe (Bl. 638 d. A.).

Nach dem Ergebnis der Beweisaufnahme erhielt die Beteiligte zu 1) von dem von ihr mit der Installation des Kontrollprogramms beauftragten externen Dienstleister "N." lediglich die am 03.05.2012 mit diesem Programm erfassten Daten (Bl. 704 d. A.). Daten, über die die Beteiligte zu 1) selbst nicht verfügte, konnte sie dem Beteiligten zu 2) naturgemäß nicht mitteilen.

Schließlich führt auch die Rüge des Beteiligtenvertreters zu 3) in der mündlichen Anhörung vor der Kammer, dem Betriebsrat seien entlastende Argumente, dass z. B. auch zur Kürzung von Stunden des Betriebsratsvorsitzenden Arbeitszeiten mit dem Passwort verändert worden sein sollen, nicht mitgeteilt worden seien, was bei einer Verdachtskündigung aber zur Anhörung des Betriebsrats gehöre, zu keinem anderen Ergebnis.

Zum Einen ergibt sich bereits aus der dem Betriebsrat als Anlage 7 übergebenen Änderungsprotokoll, dass auch Stundenkürzungen vorgenommen wurden (Bl. 30 bis 38 d. A.). Zum Anderen handelt es sich dabei entweder offensichtlich lediglich um eine Korrektur von unmittelbar vorher vorgenommenen Arbeitszeitänderungen. So wurde am 20.08.2010 rückwirkend für den 15.08.2010 ein um 4 Stunden vorgezogenes Arbeitszeitende eingetragen, um sodann noch am selben Tag (20.08.2010) für denselben Bezugstag (15.08.2010) das Arbeitszeitende wiederum um diese 4 Stunden zu verlängern (Bl. 30 d. A.). Oder an unterschiedlichen Tagen für unterschiedliche Tage vorgenommene Plus- bzw. Minusänderungen heben sich im Ergebnis jeweils wieder auf (Bl. 32 bis 36 d. A.).

Die Mitteilung an den Betriebsrat, "die Manipulationen erfolgten immer zugunsten von Herrn F." (Bl. 522 d. A.), vermittelt deshalb in der Gesamtbetrachtung keinen falschen Eindruck.

2. Nach § 103 Abs. 1 BetrVG bedarf die außerordentliche Kündigung von Mitgliedern des Betriebsrats der Zustimmung des Betriebsrats. Gem. § 103 Abs. 2 Satz 1 BetrVG i. V. m. § 15 Abs. 1 KSchG hat die Arbeitgeberin einen Anspruch auf Ersetzung der Zustimmung, wenn die beabsichtigte außerordentliche Kündigung unter Berücksichtigung aller Umstände gerechtfertigt ist. Dies setzt einen wichtigen Grund im Sinne von § 626 Abs. 1 BGB voraus. Danach müssen Tatsachen vorliegen, aufgrund derer der Arbeitgeberin unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Der Verdacht, der Arbeitnehmer könne eine strafbare Handlung oder eine schwerwiegende Pflichtverletzung begangen haben, kann nach gefestigter Rechtsprechung des Bundesarbeitsgerichts einen wichtigen Grund für eine außerordentliche Kündigung bilden (BAG, NZA 2009, 1136). Für die kündigungsrechtliche Beurteilung der Pflichtverletzung, auf die sich der Verdacht bezieht, ist ihre strafrechtliche Bewertung nicht maßgebend. Entscheidend ist der Verstoß gegen vertragliche Haupt- oder Nebenpflichten und der mit ihm verbundene Vertrauensbruch (BAG, NZA 2010, 227). Der Verdacht muss objektiv durch Tatsachen begründet sein, die so beschaffen sind, dass sie einen verständigen und gerecht abwägenden Arbeitgeber zum Ausspruch der Kündigung veranlassen können. Der Verdacht muss darüber hinaus dringend sein, d. h. es muss eine große Wahrscheinlichkeit dafür bestehen, dass der gekündigte Arbeitnehmer die Straftat oder die Pflichtverletzung begangen hat (BAG, NZA 2005, 1056). Die Verdachtsmomente und die Verfehlungen, deren der Arbeitnehmer verdächtigt wird, müssen so schwerwiegend sein, dass dem Arbeitgeber die Fortsetzung des Arbeitsverhältnisses nicht zugemutet werden kann. Hierzu rechnen schwere arbeitsvertragliche Pflichtverletzungen wie z. B. Manipulationen an der Stempelkarte (BAG, Urteil vom 09.08.1990 – 2 AZR 127/90).

3. Vorliegend fehlt es für eine Verdachtskündigung an dem Erfordernis des dringenden Verdachtes, weil die Beteiligte zu 1) zur Dokumentierung des für eine Verdachtskündigung erforderlichen dringenden Tatverdachts mit der Anwendung des heimlich installierten Kontrollprogramms nach dem Ergebnis der Beweisaufnahme gegen § 32 Abs. 1 Satz 2 BDSG sowie unverhältnismäßig gegen das allgemeine Persönlichkeitsrecht des Beteiligten zu 3) verstoßen hat mit der Folge, dass die mit dem Kontrollprogramm erhobenen Daten einem prozessualen Verwertungsverbot unterliegen.

a) Entgegen der Auffassung der Beteiligten zu 2) und 3) steht allerdings nicht bereits das Außerachtlassen des Mitbestimmungsrechts des Beteiligten zu 2) nach § 87 Abs. 1 Nr. 6 BetrVG einer prozessualen Verwertung des mit dem Kontrollprogramm gewonnenen Beweismaterials entgegen.

Zwar hat der Betriebsrat nach § 87 Abs. 1 Nr. 6 BetrVG bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, ein Mitbestimmungsrecht. Mit

der Rechtsprechung des Bundesarbeitsgerichts ist jedoch davon auszugehen, dass ein mitbestimmungswidriges Verhalten des Arbeitsgebers bereits ausreichend betriebsverfassungsrechtlich (§ 23 Abs. 3 BetrVG und allgemeiner betriebsverfassungsrechtlicher Unterlassungsanspruch) sowie individualarbeitsrechtlich (Leistungsverweigerungsrechte) sanktioniert ist. Einer darüber hinausgehenden prozessualen Sanktion bedarf es daher nicht (BAG, NZA 2008, 1008 <1011> m. w. N.).

Vorliegend hat die Beteiligte zu 1) mit der heimlichen Installation und Anwendung des Kontrollprogramms auf dem Rechner des Beteiligten zu 3) gegen dessen allgemeines Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung verstoßen. Das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht ist insbesondere im Arbeitsverhältnis zu beachten. Es wird allerdings nicht schrankenlos gewährleistet.

Eingriffe in das Persönlichkeitsrecht des Arbeitnehmers können durch Wahrnehmung überwiegend schutzwürdiger Interessen des Arbeitgebers gerechtfertigt sein. Bei einer Kollision des allgemeinen Persönlichkeitsrechts mit den Interessen des Arbeitgebers ist somit durch eine Güterabwägung im Einzelfall zu ermitteln, ob das allgemeine Persönlichkeitsrecht den Vorrang verdient (BVerfG NJW 2002, 3619).

Im Anschluss an die Rechtsprechung des Bundesarbeitsgerichts zur verdeckten Videoüberwachung (zuletzt BAG Urteil vom 21.06.2012 – 2 AZR 153/11) geht die Kammer davon aus, dass das Interesse der Beteiligten zu 1) an einer prozessualen Verwertung des mit dem heimlich auf dem Rechner des Beteiligten zu 3) installierten Kontrollprogramms gewonnenen Beweismaterials gegenüber dem Schutz des informationellen Selbstbestimmungsrechts des Beteiligten zu 3) nur dann überwiegt, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestand, es keine Möglichkeit zur Aufklärung durch weniger einschneidende Maßnahmen (mehr) gab und die Kontrollmaßnahme insgesamt nicht unverhältnismäßig war. Dieser Maßstab entspricht der gesetzlichen Wertung in § 32 Abs. 1 Satz 2 BDSG, wonach zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

b) Vorliegend bestand aufgrund folgender Umstände ein hinreichend konkreter Verdacht, dass der Beteiligte zu 3) im Zeitraum vom 05.05.2010 bis 14.12.2011 auf seinem Arbeitszeitkonto jeweils nachträglich unberechtigte Änderungen im Umfang von rund 165 Stunden zu seinen Gunsten vorgenommen haben könnte.

aa) Die Änderungen wurden immer unter dem User-Namen "EDV" Nr. 79 vorgenommen, einem Administratorenzugang, der, wie die Beweisaufnahme erbracht hat, nur für das Interflex-Zeitprogramm gilt.

Mit diesem Passwort wurden nur auf dem Arbeitszeitkonto des Beteiligten zu 3) solche Änderungen durchgeführt.

Zu den jeweiligen Zeitpunkten der vorgenommenen Änderungen war mit Ausnahme des 03.09.2011 der Beteiligte zu 3) im Betrieb anwesend.

Der Beteiligte zu 3) kann aufgrund seiner Leseberechtigung mit dem Betriebsratslaptop von zu Hause aus über seinen Router auf sein Arbeitszeitkonto zugreifen.

In Zeiten längerer Abwesenheit des Beteiligten zu 3) (z. B. wegen Urlaub oder Krankheit) erfolgten keine Änderungen auf seinem Arbeitszeitkonto.

bb) Dass der Beteiligte zu 3) unstreitig nur ein Leserecht, nicht jedoch ein Änderungsrecht für das Arbeitszeitprogramm hat und die Beteiligte zu 1) nicht weiß, wie der Beteiligte zu 3) an den Administratorenzugang gelangt sein könnte, steht aufgrund der oben aufgeführten Umstände einem hinreichenden konkreten Verdacht nicht entgegen.

Zumal dieses Zugangspasswort offensichtlich entgegen den eigenen Richtlinien der Beteiligten zu 1) jahrelang nicht verändert wurde und nach dem Sachvortrag des Beteiligten zu 3) bei der Beteiligten zu 1) entgegen deren Ausführungen kein System einer gesicherten Passwortvergabe bestehen solle (Bl. 540 d. A.). Insbesondere muss sich der Verdacht nicht notwendig nur gegen einen einzelnen bestimmten Arbeitnehmer richten (BAG Urteil vom 27.03.2003 – 2 AZR 51/02).

Der Hinweis des Beteiligten zu 2), der Beteiligte zu 3) habe als ein nach § 38 BetrVG freigestellter Betriebsratsvorsitzender und Festlohnempfänger keinerlei Vermögensvorteile durch die behauptete Datenmanipulation erlangen können, übersieht, dass auch ein freigestelltes Betriebsratsmitglied seine einschlägige Arbeitszeit mit Betriebsratsarbeit bzw. der Bereithaltung zur Betriebsratsarbeit einzuhalten hat. Bei Missachtung der Anwesenheitspflicht ohne sachlichen Grund hat das freigestellte Betriebsratsmitglied für diese Zeit keinen Anspruch auf Arbeitsentgelt (BAG AP Nr. 4 zu § 38 BetrVG 1972).

Wenn der Beteiligte zu 2) weiter einwendet, die Beteiligte zu 1) bleibe den Beweis schuldig, dass die vermeintliche und dem Beteiligten zu 3) vorgeworfene Arbeitszeitmanipulation auch tatsächlich zum Nachteil der Beteiligten zu 1) geschehen sei, da sie es unterlasse vorzutragen, dass der Beteiligte zu 3) an jenen Zeiten, welche ihm in diesem Zusammenhang vorgeworfen würden, nicht gearbeitet habe (Bl. 651 d. A.), übersieht er weiterhin, dass die Beteiligte zu 1) im Einzelnen aufgeführt hat, welche Quartalsminuszeiten sich jeweils ohne die vorgenommenen Arbeitszeitänderungen ergeben hätten (Bl. 591 ff.). Damit wäre es zur Verdachtsentkräftung zunächst einmal Sache des Beteiligten zu 3) gewesen, im Einzelnen darzulegen, dass er zu den nachträglich geänderten Zeiten Betriebsratsarbeit geleistet oder sich hierzu im Betrieb bereit gehalten habe.

Dann wäre es wiederum nach der abgestuften Darlegungslast Sache der Beteiligten zu 1) gewesen, Umstände vorzutragen und gegebenenfalls zu beweisen, dass die –

hier nicht vorgetragenen – Einwendungen des Beteiligten zu 3) nicht zuträfen (vgl. auch BAG Urteil vom 19.12.1991 – 2 AZR 367/91).

c) Auch wenn man zugunsten der Beteiligten zu 1) davon ausgeht, dass es zur Eingrenzung des Verdächtigenkreises sowie zur Feststellung, ob der ändernde Zugriff auf das Zeitkonto des Beteiligten zu 3) von dessen Rechner aus stattfand, um damit den für eine Verdachtskündigung notwendigen dringenden Verdacht zu dokumentieren, erforderlich war, ein Kontrollprogramm auf dem Rechner des Beteiligten zu 3) zu installieren, so steht jedoch nach dem Ergebnis der Beweisaufnahme zur Überzeugung der Kammer fest, dass dieses Kontrollprogramm in seiner konkreten Funktionsweise unverhältnismäßig war.

Bei der Prüfung der Verhältnismäßigkeit der Überwachung ist nicht nur die Art der Kontrolle – also mit welchem technischen Mittel die Überwachung erfolgt – sondern auch das Ausmaß der Überwachung relevant. Dabei geht es nicht nur um das zeitliche, sondern auch um das inhaltliche Ausmaß der Kontrolle; also um die Frage, welche Umstände und Inhalte können durch die Kontrolle erfasst werden. Für die Angemessenheit der Maßnahme ist die Eingriffsintensität mit entscheidend (BAG, NZA 2004, 1278, 1281).

Nach der Bekundung des Zeugen C., an dessen Glaubwürdigkeit die Kammer keinen Anlass zu zweifeln hat, funktioniere dieses Programm so, dass bei Zugriff auf die Zeiterfassung vom Computer des Beteiligten zu 3) aus 5 Minuten lang sekündlich eine Abbildung von dem im Vordergrund befindlichen Programm gemacht werde, d. h. von dem Programm, das sich gerade auf dem Bildschirm befinde.

Dieses Programm halte den Zeitpunkt fest, zu dem auf das Zeitkonto zugegriffen worden sei und dokumentiere die entsprechenden Bilder.

Dies hat jedoch zur Folge, das bei einer Beendigung oder Unterbrechung der Nutzung des Zeitprogramms vor Ablauf der vorgesehenen 5 Minuten die folgenden mit dem Arbeitszeitprogramm in keinem Zusammenhang mehr stehenden Bildschirmaktivitäten bis zum Ablauf der 5 Minuten ebenfalls von diesem Kontrollprogramm aufgezeichnet werden. Eine Beschränkung der Kontrollfunktion auf das Arbeitszeitprogramm fand daher nicht statt.

Damit folgte mit diesem Programm ein Übermaß an Kontrolle.

Nach der weiteren Aussage des Zeugen C. wäre mit einem größeren Programmieraufwand auch ein automatisches Abschalten des Kontrollprogramms technisch möglich gewesen, wenn der Nutzer vor Ablauf der 5 Minuten das Zeitprogramm verlässt.

Wie die von der Beteiligten zu 1) vorgelegten Kopien der aufgenommenen Screenshots zeigen, wurden in dem vorgesehenen Zeitintervall auch die private E-Mail-Bearbeitung erfasst. Das installierte Kontrollprogramm stellt sich deshalb jedenfalls in seiner konkreten Funktionsweise als unverhältnismäßige Maßnahme dar. Dies hat zur Folge, dass die mit diesem Kontrollprogramm aufgenommenen Screenshots prozessual nicht verwertet werden können. Insbesondere steht dieser prozessualen Nichtverwertbarkeit nicht entgegen, dass anderenfalls ein größerer

Programmieraufwand erforderlich gewesen wäre. Ein solcher kann den Einsatz des streitgegenständlichen in seiner konkreten Funktionsweise unverhältnismäßigen Kontrollprogramms nicht rechtfertigen.

Der unverhältnismäßige Eingriff in das Persönlichkeitsrecht des Beteiligten zu 3) führt dazu, dass das Interesse der Beteiligten zu 1) an einer prozessualen Verwertung des mit dem heimlich installierten Kontrollprogramms gewonnenen Beweismaterials gegenüber dem Schutz des informationellen Selbstbestimmungsrechts des Beteiligten zu 3) zurückzutreten hat.

Zwar sieht das Bundesdatenschutzgesetz bei einem Verstoß gegen § 32 Abs. 1 Satz 2 BDSG ein eigenständiges Beweiserhebungs- oder Verwertungsverbot nicht vor (Simitis, BDSG 7. Auflage, Rn. 193 zu § 32), jedoch folgt ein solches prozessuales Beweisverwertungsverbot nach den vom Bundesarbeitsgericht aufgestellten Grundsätzen (s. o.).

Nach alledem fehlt es an einem prozessual verwertbaren Nachweis des für eine Verdachtskündigung erforderlichen dringenden Verdachts, der Beteiligte zu 3) habe zum Zwecke des Arbeitszeitbetrugs sein Arbeitszeitkonto rechtswidrig manipuliert.

4. Das Verfahren ist kostenfrei (§ 2 Abs. 2 GKG).

6 ArbG Hamburg, Erhebung und Speicherung von persönlichen Daten mittels GPS

ArbG Hamburg, 13.04.2011, 24 Ca 229/10

Orientierungssatz

1. Soweit eine Dienstvereinbarung zur Einführung eines Flottenmanagements mittels GPS vorliegt, kann die Erforderlichkeit der Datenverarbeitung, sei es Datenerhebung oder sei es Datenspeicherung, im Rahmen von § 28 Abs 2 HmbDSG (juris: DSG HA) unterstellt werden.

2. Die Ortung eines Einsatzfahrzeugs mittels GPS während der Pausenzeit verstößt nicht gegen höherrangiges Recht.

Tenor

1. Die Klage wird abgewiesen.

2. Die Kosten des Rechtsstreits trägt der Kläger.

3. Der Streitwert beträgt 2.500,00 €.

4. Die Berufung wird nicht gesondert zugelassen.

Tatbestand

Die Parteien streiten darüber, ob die Beklagte persönliche Daten des Klägers mittels GPS Ortung erheben und speichern darf.

Der Kläger ist bei der Beklagten seit 1985 beschäftigt, seit dem 15.2.1999 bei der Autobahnmeisterei des L. S., B. und G.. Seine Aufgabe besteht u.a. darin, Einsatzfahrzeuge im Winterstreudienst zu führen. Dafür wird er mittels Dienstplänen eingesetzt.

Bei der Beklagten ist gemäß dem HmbPersVG ein Personalrat gewählt. Am 27.3.2008 schlossen die Betriebsparteien eine Dienstvereinbarung gemäß § 83 HmbPersVG zur „Einführung und Anwendung des Flottenmanagements (Digitaler Bündelfunk und GPS - Global Positioning System) im Straßendienst des L. S., B. und G."(vgl. Anlage K1, Bl. 14 ff d.A.).

Diese sieht u.a. folgende Regelungen vor

„§ 3 Zielsetzung

Der Einsatz des Flottenmanagements dient der Erkennung der Position der Fahrzeuge des Straßenbetriebsdienstes für organisatorische Zwecke im Winterdienst und bei Ereignissen (Unfälle usw.), sowie zur Verbesserung der Dispositionsmöglichkeiten.

§ 4 Leistungs- und Verhaltenskontrolle

Über das Flottenmanagement finden keine personenbezogenen Verhaltens- und Leistungskontrollen statt. Insbesondere findet kein Abgleich zwischen den gespeicherten Daten und den Fahrtenbüchern statt.

§ 5 Datenerfassung und Dokumentation

Der Nutzer des Flottenmanagements (Leiter/in der AM/TBZ, der/die Verwaltungsangestellte, der/die Abteilungsleiter/in, der/die Einsatzleiter/in sowie der/die jeweilige Vertreter/in) kann die aktuellen Zustände (insbesondere geografische Position und Uhrzeit des Datensatzes) und die gespeicherten Daten einsehen. Die Daten des Flottenmanagements werden 3 Monate im System gespeichert. Danach erfolgt eine externe Datensicherung, die Daten werden ein Jahr lang unter Einhaltung des Datenschutzes auf externen Datenträgern aufbewahrt…"

In der Folge wurden alle Einsatzfahrzeuge mit GPS ausgestattet, auch das vom Kläger geführte Fahrzeug. Damit ist die online übertragene Standortbestimmung des Fahrzeugs ermöglicht. Die Beklagte kann über die Dienstpläne feststellen, welcher Fahrer im Dienst ist. Die Fahrzeuge sind den Fahrern fest zugeordnet. Exemplarisch wird auf Anlage K12, Bl. 61 f d.A. verwiesen. Es besteht eine Anweisung, das GPS während der Einsatzzeit stets eingeschaltet zu lassen. Das gilt ausdrücklich auch für die Pausenzeiten.

Ob vor Einführung eine Risikoanalyse gemäß § 8 HmbDSG erforderlich war und auch vor Einführung erstellt worden war, ist streitig. Eine solche liegt jedenfalls jetzt mit Stand 13.1.2011 vor (vgl. Anlage Bl. 96 ff d.A.) und ist vom Datenschutzbeauftragten

nicht beanstandet. Ebenso liegt eine aktuelle Verfahrensbeschreibung gemäß § 9 HmbDSG, zuletzt aktualisiert am 23.4.2011 vor (vgl. Anlage, Bl 104 f d.A.).

Der Kläger trägt vor:

er werde durch die von der Beklagten praktizierte Datenerhebung und Speicherung in seinen Rechten verletzt. Weder sei die Erhebung und Speicherung erlaubt, noch habe er eingewilligt. Die Verarbeitung der Daten sei an den Regelungen im kommenden Gesetz zum Arbeitnehmerdatenschutz zu messen und genüge insoweit den gesetzlichen Anforderungen nicht. Weder sei eine Ortung durch GPS überhaupt erforderlich, weil Funkkontakt ausreichend sei, noch sei die Datenspeicherung und weitere Aufbewahrung der Daten für einen Zeitraum von insgesamt 12 Monaten erforderlich. Jedenfalls aber gelte dies während seiner Pausenzeiten, wenn er nicht im Dienst sei. Er werde unzulässig überwacht.

Die Einführung des GPS gestützten Flottenmanagements sei schon wegen gravierender Verfahrensfehler unwirksam. Denn es habe vor Einführung weder eine vom Datenschutzbeauftragten genehmigte Risikoanalyse noch eine Verfahrensbeschreibung vorgelegen.

Der Kläger beantragt,

die Beklagte zu verurteilen, es zu unterlassen, mittels GPS Ortung laufend persönlichen Daten des Klägers zu erheben, diese drei Monate im System zu speichern und ein Jahr lang auf externen Datenträgern aufzubewahren,

hilfsweise ,

die Beklagte zu verurteilen, es zu unterlassen, mittels GPS Ortung persönliche Daten des Klägers während seiner Pausenzeiten zu erheben, diese drei Monate im System zu speichern und ein Jahr lang auf externen Datenträgern aufzubewahren.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte trägt vor:

weder überwache Sie den Kläger, noch sei dies ihre Intention. Es gehe ausschließlich darum, eine Standortbestimmung der Einsatzfahrzeuge mittels GPS zu ermöglichen, um z.B. bei Blitzeisbildung oder Unfällen bestmöglich reagieren und steuern zu können. Dies tue sie auf der Basis einer rechtswirksamen Dienstvereinbarung.

Die Speicherung der Daten ermögliche ihr die Einsatzplananalyse im Interesse künftiger Verbesserung der Einsatzplanung. Außerdem verbessere dies die Beweislage bei Inanspruchnahme durch Dritte wegen behaupteter Schadensverursachung durch Einsatzfahrzeuge.

Wegen weiterer Einzelheiten des Parteivorbringens wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe

Die Klage ist zulässig, aber weder mit dem Haupt- noch mit dem Hilfsantrag begründet. Die Kammer kann unter keinem rechtlichen Gesichtspunkt feststellen, dass es der Beklagten in Gänze (1.) oder aber jedenfalls während der Pausenzeiten des Klägers (2.) verboten ist, mittels GPS Ortung laufend persönlichen Daten des Klägers zu erheben, diese drei Monate im System zu speichern und ein Jahr lang auf externen Datenträgern aufzubewahren.

1. Ein Anspruch auf Unterlassung gemäß § 1004 Abs. 1 BGB, § 5 HmbDSG, Art. 2 Abs. 1, Art. 1 Abs. 1 GG ist nicht begründet.

a) Die Rechte des Klägers sowie die Pflichten der Beklagten bestimmen sich ausschließlich nach den Regelungen des geltenden Rechts. Möglicherweise künftig geltendes Recht, namentlich das im Gesetzgebungsverfahren befindliche künftige Gesetz zum Arbeitnehmerdatenschutz ist nicht heranzuziehen. Prüfungsmaßstab sind daher zunächst die Regelungen des HmbDSG.

Danach gilt Folgendes.

Es handelt sich um personenbezogene Daten im Sinne von § 4 Abs. 1, HmbDSG. Denn mittel GPS in Abgleich mit den Einsatzplänen ist für die Beklagte nicht nur die Ortung der Einsatzfahrzeuge sondern auch die Ortung des Klägers möglich. Es handelt sich demzufolge um Einzelangaben über sachliche Verhältnisse einer bestimmbaren natürlichen Person, nämlich den jeweiligen Aufenthaltsort des Klägers.

Die Verarbeitung dieser Daten, wobei Verarbeitung gemäß § 4 HmbDSG gesetzlich definiert ist als u.a. die Erhebung von Daten (Abs. 2 Ziffer 1) und die Speicherung von Daten (Abs. 2 Ziffer 2), ist nur zulässig, wenn das Gesetz diese erlaubt, § 5 Abs. 1. HmbDSG. Im vorliegenden Fall bestimmt sich die Zulässigkeit der Datenverarbeitung nicht nach den allgemeinen Rechtsgrundlagen gemäß § 12 ff HmbDSG, sondern die gesetzlichen Sonderregelungen gemäß § 28 Abs. 1 HmbDSG für die Datenverarbeitung bei Beschäftigungsverhältnissen sind einschlägig. Danach dürfen personenbezogene Daten nur verarbeitet werden, wenn u.a. eine Dienstvereinbarung dies vorsieht.

Eine Dienstvereinbarung zur Einführung eines Flottenmanagements mittels GPS ist am 27.3.2008 geschlossen worden (vgl. Anlage K1, Bl. 14 ff d.A.). Diese erlaubt die Verarbeitung der hier streitigen Daten.

Sowohl das in § 3 definierte Regelungsziel ist legitim, als auch sind die Arbeitnehmerrechte gewahrt, indem § 4 ausdrücklich regelt, dass keine personenbezogenen Verhaltens- und Leistungskontrollen stattfinden. Die Rechte der Betroffenen gemäß § 6 HmbDSG bleiben unberührt.

Nur wenn eine Dienstvereinbarung nicht abgeschlossen wäre, gelten die allgemeinen Regeln gemäß den Absätzen § 28 Abs. 2 ff HmbDSG. Das Gericht ist daher daran gehindert, im Rahmen von § 28 Abs. 2 HmbDSG die Erforderlichkeit der GPS Überwachung zu überprüfen. Denn das Gesetz unterstellt erkennbar, dass durch die kollektive Beteiligung die Erforderlichkeit für die Datenverarbeitung, sei es Datenerhebung oder sei es Datenspeicherung, zu unterstellen ist.

b) Die Regelungen der Dienstvereinbarung zur Datenerhebung und Datenspeicherung verstoßen auch nicht gegen höherrangiges Recht.

Dabei ist von folgenden Grundsätzen auszugehen (vgl. BAG 26.8.2008, 1 ABR 16/07, AP Nr. 54 zu § 75 BetrVG 1972). Arbeitgeber und Personalrat haben die Pflicht, die freie Entfaltung der Persönlichkeit der in der Dienststelle beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben daher insbesondere das in Art 2 Abs. 1 GG und Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht zu beachten, was in § 77 HmbPersVG seinen Ausdruck findet. Dazu gehört auch das Recht auf informationelle Selbstbestimmung, was unter den Bedingungen der automatischen Datenverarbeitung des besonderen Schutzes bedarf.

Eingriffe in das allgemeine Persönlichkeitsrecht der Arbeitnehmer müssen durch schutzwürdige Belange anderer Grundrechtsträger gerechtfertigt sein. Das zulässige Maß einer Beschränkung des allgemeinen Persönlichkeitsrechts bestimmt sich nach dem Grundsatz der Verhältnismäßigkeit. Dieser verlangt, dass die von Arbeitgeber und Personalrat getroffene Regelung geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen. Geeignet ist die Regelung, wenn mit ihrer Hilfe der erstrebte Zweck gefördert werden kann, wobei ein gewisser Beurteilungsspielraum zuzugestehen ist. Erforderlich ist die Regelung, wenn kein anderes, gleich wirksames und das Persönlichkeitsrecht weniger einschränkendes Mittel zur Verfügung steht. Auch insoweit darf in einer Dienstvereinbarung ein gewisser Beurteilungsspielraum genutzt werden. Angemessen ist eine Regelung, wenn sie als im engeren Sinn verhältnismäßig erscheint. Um das festzustellen, bedarf es einer Gesamtabwägung der Intensität des Eingriffs und des Gewichts der ihn rechtfertigenden Gründe. Dafür kommt es auf die Gesamtumstände an. Das Gewicht der Beeinträchtigung hängt u.a. davon ab, ob die Betroffenen als Personen anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden und welche Nachteile den Grundrechtsträgern aus der Überwachungsmaßnahme drohen oder von ihnen nicht ohne Grund befürchtet werden.

Danach ergibt sich hier Folgendes.

aa) Erklärter Zweck der Datenerhebung durch den Einsatz von GPS ist die Verbesserung der Dispositionsmöglichkeit im Interesse einer jederzeitigen Ortung und Erreichbarkeit der Einsatzfahrzeuge, um bei Gefahrenlage im Winterdienst (z.B Blitzeis) oder bei Unfällen u.a. auch im Interesse der Allgemeinheit schnellstmöglich durch die Einsatzleitung reagieren zu können.

Unter Berücksichtigung dieses Zwecks und dieser Interessen ist die Datenerhebung mittels GPS geeignet, erforderlich und angemessen.

Dass GPS ein geeignetes System ist, steht außer Frage. Arbeitgeber und Personalrat durften die Nutzung auch für erforderlich halten, weil die online Ortung aller im Einsatz befindlichen Einsatzfahrzeuge erkennbare Vorteile gegenüber Funkverkehr hat, insbesondere auch für den Laien erkennbar schneller sein dürfte.

Die Datenerhebung hält auch einer Angemessenheitsprüfung stand. Anders als z.B. bei einer Videoüberwachung ist der Eingriff in das Persönlichkeitsrecht des Klägers

gering. Die Beklagte kann lediglich ermitteln, wo er sich mit seinem Fahrzeug gerade befindet, noch nicht einmal feststellen, was er gerade tut. Dies ist nicht geeignet, einen erhöhten Überwachungs- und Anpassungsdruck auszulösen.

bb) Auch die Speicherungsdauer der erhobenen Daten verstößt nicht gegen höherrangiges Recht.

Angesichts des legitimen Interesses der Beklagten, die gewonnenen Daten zur Optimierung ihrer Einsatzpläne zu nutzen, ist auch insoweit festzustellen, dass die Speicherung für maximal 1 Jahr geeignet ist, diesem Interesse gerecht zu werden, was Arbeitgeber und Personalrat für erforderlich ansehen durften. Dass das Recht des Klägers auf informationelle Selbstbestimmung gerade durch die Dauer der Speicherung nachhaltig berührt sein könnte, ist weder dargelegt noch ersichtlich.

c) Der Beklagten ist die Datenverarbeitung schließlich auch nicht deshalb untersagt, weil vor Einführung gegen wesentliche Verfahrensgrundsätze verstoßen worden ist. Der Kläger rügt in diesem Zusammenhang, dass die Beklagte es versäumt habe, vor Einführung eine Risikoanalyse zu erheben und eine Verfahrensbeschreibung zu erstellen. Ob dies der Fall ist, musste nicht weiter aufgeklärt werden, desgleichen kann offen bleiben, ob und welche rechtlichen Konsequenzen aus einem derartigen Versäumnis resultieren. Denn unstreitig liegt eine vom Datenschutzbeauftragten nicht beanstandete Risikoanalyse gemäß § 8 Abs. 4 HmbDSG (vgl. Anlage, Bl. 96 ff d.A.) zum jetzigen Zeitpunkt ebenso vor wie eine aktuelle Verfahrensbeschreibung gemäß § 9 Abs. 3 HmbDSG (vgl. Anlage Bl. 104 f d.A.). Mögliche Versäumnisse sind geheilt, stehen einer Anwendung des Systems jedenfalls zum Zeitpunkt der Entscheidung im vorliegenden Rechtsstreit nicht entgegen.

2. Die Klage ist auch mit dem Hilfsantrag nicht erfolgreich.

a) Die GPS Ortung während der Pausenzeit ist durch die Dienstvereinbarung nicht ausgeschlossen. Sie entspricht vielmehr der unter § 3 geregelten Zielsetzung, nämlich die Position der Fahrzeuge während der Einsatzzeit zu erkennen. Das Fahrzeug ist auch dann im Einsatz, wenn der eingesetzte Fahrer Pause hat.

b) Die Ortung mittels GPS während der Pausenzeit verstößt auch nicht gegen höherrangiges Recht. Sie ist nicht unverhältnismäßig und verletzt den Kläger nicht in seinem Persönlichkeitsrecht.

Bei Anlegung der oben dargelegten Grundsätze gilt auch insoweit, dass die Datenerhebung mittels GPS und deren Speicherung geeignet, erforderlich und angemessen sind. Der Kläger verkennt, dass das ihm zur Dienstausübung anvertraute Fahrzeug auch während seiner Pausenzeit sich zum einen in Ansehung der Dispositionsmöglichkeit durch die Beklagte weiterhin im Einsatz befindet, zum anderen unter seiner Obhut verbleibt. In Hinblick auf die insoweit übertragenen Pflichten handelt es sich auch für den Kläger nicht um Freizeit sondern um Einsatzzeit.

3. Die Kostenentscheidung beruht auf §§ 91 Abs. 1 ZPO, 46 Abs. 2 ArbGG.

Der Streitwert für das Urteil ist gemäß §§ 3 ff ZPO, 61 Abs. 1 ArbGG festgesetzt und mit einem Monatsverdienst bewertet worden.

Die Berufung war nicht gesondert zuzulassen, soweit sie nicht ohnehin gemäß § 64 Abs. 2 lit. b) gegeben ist, da die Voraussetzungen gemäß § 64 Abs. Abs. 3 ArbGG nicht vorliegen.