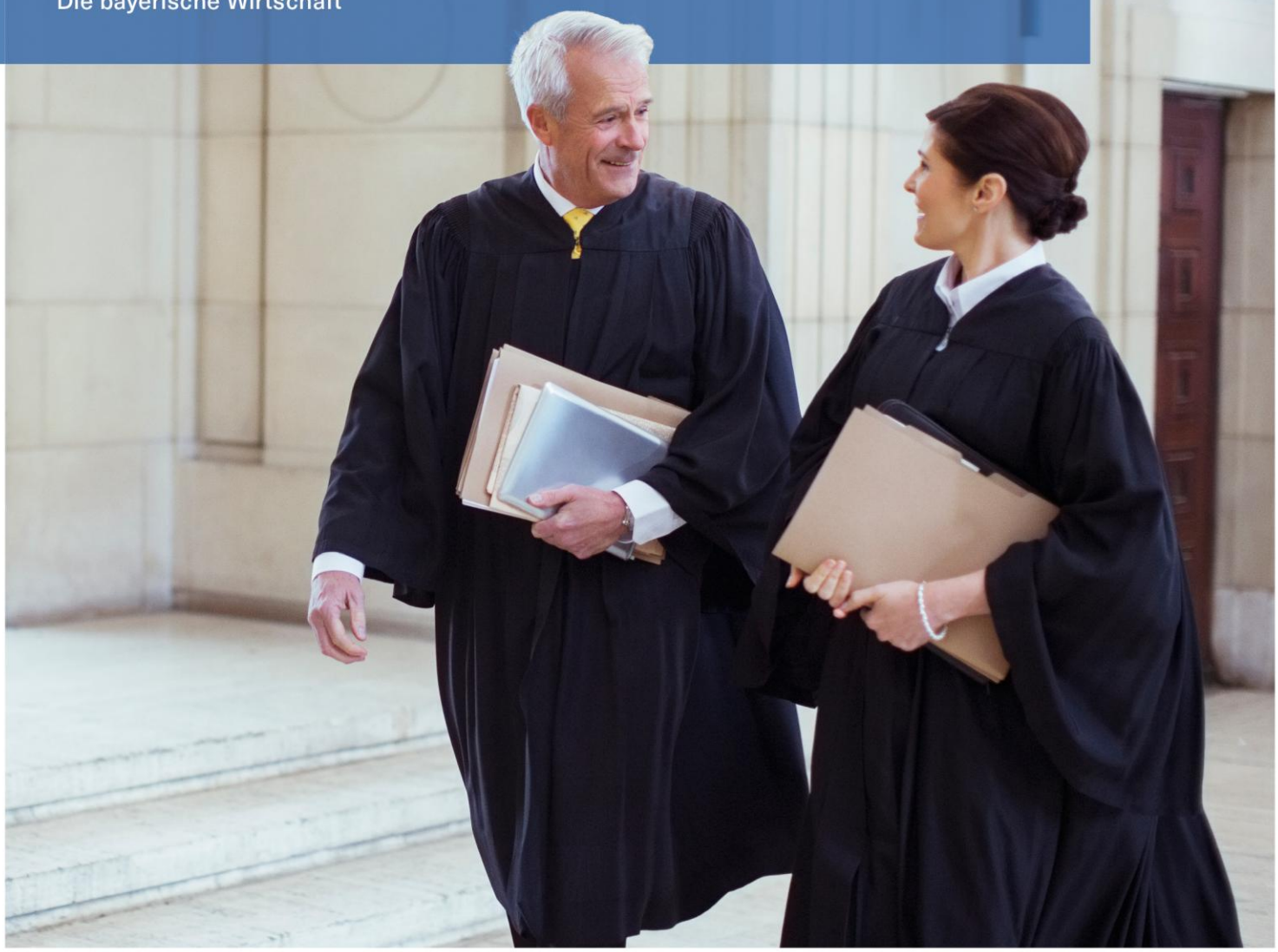
Recht

Privatnutzung von Internet und E-Mail am Arbeitsplatz

vbw

Info Recht
Stand: Januar 2026

Die bayerische Wirtschaft



Hinweis

Diese Information ersetzt keine rechtliche Beratung im Einzelfall. Eine Haftung übernehmen wir mit der Herausgabe dieser Information nicht.

Um die Information an einen sich wandelnden Rechtsrahmen und an die höchstrichterliche Rechtsprechung anzupassen, überarbeiten wir unsere Broschüre regelmäßig. Bitte informieren Sie sich über die aktuelle Version auf unserer Homepage www.vbw-bayern.de/InfoRecht.

Vorwort

Klare Regeln für die private Nutzung von Kommunikationsmitteln

Die Grenze zwischen privatem und beruflichem Bereich verschwindet durch moderne Kommunikationsmittel und flexible Beschäftigungsformen immer mehr. Viele Unternehmen gestatten oder dulden die Nutzung von Betriebsmitteln zur privaten Kommunikation.

Bei Privatnutzung durch den Arbeitnehmer unterliegt der Arbeitgeber jedoch dem Fernmeldegeheimnis – und damit einem strengen Kontrollverbot. Die Einsichtnahme in ein dienstliches E-Mail-Postfach ist deshalb untersagt, sofern keine ausdrückliche Einwilligung des Mitarbeiters vorliegt.

Im Falle der krankheits- oder urlaubsbedingten Abwesenheit von Mitarbeitern besteht aber ein dringendes betriebliches Interesse des Arbeitgebers, Einblick in die Kommunikation zu nehmen, um die eingehenden E-Mails bearbeiten zu können. Es sind daher klare Regelungen notwendig, die sowohl das Persönlichkeitsrecht der Mitarbeiter als auch die berechtigten Interessen der Arbeitgeber berücksichtigen.

Unsere Broschüre erläutert die rechtlichen Fragestellungen und enthält Muster für die individualvertragliche oder kollektive Umsetzung in Ihrem Unternehmen.

Bertram Brossardt
21. Januar 2026

Inhalt

1 Betriebsmittel

Mobile Device Management

Die vorliegende Info Recht Broschüre behandelt die Frage, nach welchen Regeln Betriebsmittel und insbesondere betriebliche Kommunikationsmittel durch Mitarbeiter genutzt werden können und welche Konsequenzen vor allem die private Nutzbarkeit von Betriebsmitteln hat.

Die hier im Zusammenhang zu betrachtenden Betriebsmittel lassen sich zunächst klassisch in Hard- und Software untergliedern.

Die Hardware als zu betrachtendes Betriebsmittel besteht heutzutage aber vielfach nicht mehr in einem (fest eingerichtetem) Rechner mit Tastatur und Bildschirm, sondern u. U. aus mehrfach gleichzeitig dem Arbeitnehmer überlassenen mobilen Geräten, wie Laptops, Notebooks, Tablets, Smartphones etc. Das „Mobile Device Management“ gilt daher nicht nur für die Fälle, in denen der Mitarbeiter eigene Geräte einbringt. Hinsichtlich der Datenschutz- und Datensicherungsmaßnahmen sind hier insbesondere die Hardwarekomponenten zu betrachten, die Daten speichern können. Das sind über die vorgenannten Devices beispielsweise auch USB-Sticks, die ebenfalls dann unter das entsprechende Datensicherungsregime zu stellen sind.

Bei der Software handelt es sich um alle Programme und Anwendungen, die vom Arbeitgeber zur Verfügung gestellt worden sind.

2 Art der Nutzung

Dienstliche oder private Nutzung

Hinsichtlich der Art der Nutzung von Betriebsmitteln ist die rein dienstliche Nutzung von der Nutzung zu unterscheiden, die auch die Nutzung der Betriebsmittel zu privaten Zwecken gestattet. Die ausdrücklich gestattete oder aber zumindest geduldete Nutzung von Betriebsmitteln auch zu privaten Zwecken wirft eine Vielzahl von Rechtsfragen auf, so dass aus rechtlicher Sicht empfohlen wird, arbeitgeberseitig ausdrücklich nur eine rein dienstliche Nutzung von Betriebsmitteln zu gestatten.

Auch die private Nutzung von Betriebsmitteln ist rechtskonform möglich, wenn Fragestellungen aus den verschiedenen Bereichen eines Unternehmens – insbesondere Personal, IT und Recht – beachtet werden.

3 Datenschutzrechtliche Aspekte

Besonderheiten bei der erlaubten Privatnutzung

Bei der rein dienstlichen Nutzung von Betriebsmitteln treten datenschutzrechtlich keine besonderen Probleme auf.

Hinweis

Zu den allgemeinen Regeln zum Datenschutz im Arbeitsverhältnis siehe unsere Info Recht
Info Recht: Datenschutz im Arbeitsverhältnis

Besonderheiten gelten demgegenüber, wenn Betriebsmittel auch zu privaten Zwecken genutzt werden dürfen.

3.1 Nutzung von Betriebsmitteln zu privaten Zwecken

Dem vorgeschaltet werden muss aber die Frage, bei welchen Betriebsmitteln und zu welchen Zwecken eine solche Gestattung überhaupt erfolgen sollte. Denkbar erscheinen zum Beispiel die Nutzung von Betriebsmitteln schlicht zur Speicherung persönlicher Dateien (wie Adresslisten o. ä.) oder die – in der Praxis immer wieder anzutreffende Thematik im Kontext von Urlaubsfotos – Installation privater Software auf betrieblicher Hardware. Insbesondere letzteres sollte untersagt werden, da mit der Installation privater Software auf Betriebsmitteln eventuell Unverträglichkeiten mit den Betriebssystemen und gegebenenfalls auch Sicherheitslücken entstehen können.

Erfolgt eine Gestattung der Nutzung zum Zwecke der privaten Kommunikation, so ist diese Kommunikation mittels der Betriebsmittel Telefon (hier noch einmal unterscheidbar zwischen Festnetz und mobilen Endgeräten), Internet und E-Mail denkbar. Für letztere wird entweder eine festinstallierte Arbeitsplatzstruktur benötigt oder sie erfolgt ebenfalls über mobile Geräte wie Notebooks, Laptops oder Tablets etc. In allen Fällen stellt sich die seit vielen Jahren diskutierte Frage, ob damit der Arbeitgeber zum Anbieter von Telekommunikationsdienstleistungen wird und ob und wie die sich aus der vermeintlichen Anwendbarkeit des Fernmeldegeheimnisses ergebenden Konsequenzen behandelt werden müssen. Diese Frage war Gegenstand landesarbeitsgerichtlicher Entscheidungen, ist aber höchstrichterlich immer noch nicht entschieden. Auch bei der Einführung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz“ (TDDDG) wurde zu dieser Frage keine Klarheit geschaffen.

Zu berücksichtigen ist, dass nach der Rechtsprechung des Bundesverfassungsgerichtes (BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04) das Fernmeldegeheimnis nur den

laufenden Kommunikationsvorgang schützt, dieser aber dann abgeschlossen ist, wenn der Kommunikationsteilnehmer die Gelegenheit hatte, beispielsweise auf die E-Mail zuzugreifen. Wann aber der Kommunikationsvorgang in diesem Sinne abgeschlossen ist, kann ebenso unterschiedlich beurteilt werden. So könnte man hier sowohl auf den Eingang beim Server des Providers als auch auf das Speichern der E-Mail im persönlichen Bereich des Mitarbeiters abstellen. Allerdings ist zu berücksichtigen, dass auch bei Letzterem die Zugriffsmöglichkeit des Arbeitgebers vorhanden bleibt.

Hinweis

Wegen der noch bestehenden Rechtsunsicherheiten wird im Folgenden sowohl die Anwendbarkeit des TDDDG als auch die des Fernmeldegeheimnisses unterstellt.

3.2 Problemstellung für den Arbeitgeber

Für den Arbeitgeber besteht vielfach das Bedürfnis in die Kommunikation seiner Mitarbeiter einzugreifen. Dies können einfache Anlässe sein, beispielsweise die außerplanmäßige Abwesenheit aufgrund von Krankheit oder das Ausscheiden eines Mitarbeiters. In beiden Fällen muss auf den dienstlichen E-Mail-Account des Mitarbeiters zugegriffen und dieser Account gegebenenfalls auf einen anderen Mitarbeiter umgeleitet werden. Damit einher geht typischerweise der Zugriff des Arbeitgebers auf private Kommunikation, sofern diese gestattet ist.

Hinweis

Die vorstehend beschriebenen Szenarien waren und werden immer häufiger Gegenstand von gerichtlichen Auseinandersetzungen zwischen dem Unternehmen und dem betroffenen Mitarbeiter, der aus dem Unternehmen ausgeschieden ist.

Es bestehen aber auch rechtliche Verpflichtungen und Compliance-Anforderungen, die den Arbeitgeber verpflichten, gegebenenfalls in Berührung mit privater E-Mail-Korrespondenz zu kommen. So verpflichten bereits die §§ 130 und 9 OWiG die Unternehmen Maßnahmen zu ergreifen, um Straftaten oder Ordnungswidrigkeiten zu verhindern.

Gesellschaftsrechtlich sind diese Verpflichtungen noch in den § 91 Abs. 2 AktG und § 41 GmbHG und spezialgesetzlich z. B. in den §§ 283 Abs. 1 Nr. 5 und 6 StGB unterlegt. Daneben bestehen Speicherungs- und Archivierungspflichten aus § 257 HGB und den §§ 146 und 147 AO in Verbindung mit den Regeln der GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in

elektronischer Form sowie zum Datenzugriff). Mit allem einher geht aber eine mögliche Kenntnisnahme privater E-Mail-Kommunikation, sofern diese gestattet ist.

Damit stellt sich die Frage, wie diese Verpflichtungen mit einem etwaigen Verstoß gegen das TDDDG oder das Fernmeldegeheimnis in Einklang gebracht werden können, zumal auch Verstöße dagegen bußgeldbewehrt oder sogar strafbewehrt sind (vgl. § 206 StGB).

3.3 Lösungsmöglichkeiten

Um den Interessenkonflikt von notwendigen Compliance-Maßnahmen und der möglichen Anwendbarkeit des Fernmeldegeheimnisses aufzulösen, muss auf eine spezielle gesetzliche Erlaubnis durch eine Rechtsnorm oder durch die Einwilligung des Arbeitnehmers abgestellt werden. Für die Verarbeitung von personenbezogenen Daten gilt nämlich generell das „Verbot mit Erlaubnisvorbehalt“. Das heißt, jeder Umgang mit personenbezogenen Daten ist grundsätzlich verboten, es sei denn

– die DS-GVO oder das BDSG (zum Beispiel Art. 6 Abs. 1 lit. b DS-GVO),
– eine Betriebsvereinbarung (§ 26 Abs. 4 BDSG)
– der betroffene Arbeitnehmer selbst (Einwilligung, Art. 6 Abs.1 lit. a) DS-GVO)

gestatten die Kontrollmaßnahmen.

3.3.1 Erforderlichkeit für Zwecke des Beschäftigungsverhältnisses

Sofern keine Spezialvorschriften greifen (zum Beispiel Fernmeldegeheimnis gem. § 3 TDDDG), richtet sich die Zulässigkeit der Datenverarbeitung im Arbeitsverhältnis nach Art. 6 Abs.1 lit. b).

Hinweis

Der Europäische Gerichtshof hat per Urteil vom 30. März 2023 (Az. C-34/21) entschieden, dass § 26 Abs. 1 S. 1 BDSG (wohl) nicht mit den Vorgaben der DS-GVO vereinbar ist. Da der EuGH allerdings bloß abstrakte Rechtsfragen bei der Auslegung der DS-GVO klärt, bleibt eine abschließende Entscheidung des Verwaltungsgerichts (VG) Frankfurt abzuwarten, welches die entsprechenden Auslegungsfragen zur Beantwortung an den EuGH gestellt hat. Im Kern führt der EuGH aus, dass es der Regelung des § 26 Abs. 1 S. 1 BDSG nicht bedurft hätte, da deckungsgleiche Regelungen bereits in der DS-GVO selbst angelegt sind. Nationale Rechtsvorschriften zum Beschäftigtendatenschutz müssen aufgrund des Anwendungsvorrangs des Unionsrechts unangewendet bleiben, wenn sie die in Art. 88 Abs. 1 und 2 DS-GVO vorgesehenen Voraussetzungen und Grenzen nicht beachten. Insoweit ist zunächst davon auszugehen, dass das VG Frankfurt die Ausführungen des EuGH entsprechend übernehmen wird.

Wo bislang also bei der Verarbeitung von Beschäftigtendaten auf § 26 Abs. 1 S. 1 BDSG abgestellt wurde, müssen verantwortliche Stellen künftig die Regelungen der DS-GVO heranziehen. Im Regelfall wird diese Aufgabe lediglich zu einem redaktionellen Aufwand (etwa in Datenschutzhinweisen gemäß Art. 13 DS-GVO sowie im Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO) führen, da in Art. 6 Abs. 1 lit. b) DS-GVO bereits eine Regelung enthalten ist, welche die Verarbeitung personenbezogener Daten zu Zwecken der Erfüllung eines Vertrages (beispielsweise das Arbeitsverhältnis) legitimiert. „Typische" Verarbeitungstätigkeiten im Beschäftigtenkontext können daher auch künftig ohne intensive Prüfung fortgeführt werden. Gleiches gilt, sofern der Arbeitgeber beispielsweise aufgrund einer gesetzlichen Regelung zur Verarbeitung von Beschäftigtendaten verpflichtet ist, da insoweit auf Art. 6 Abs. 1 lit. c) DS-GVO abgestellt werden kann.

Daneben ist es denkbar, dass gewisse Absätze in § 26 BDSG (insbesondere Abs. 1 S. 2) den Anforderungen der DS-GVO entsprechen und daher weiterhin anwendbar bleiben. Insoweit bleibt die weitere Entwicklung im Auge zu behalten, sodass Unternehmen schnell auf einen etwaigen Anpassungsbedarf reagieren können.

Grundsätzlich gilt, dass zur Durchführung des Arbeitsverhältnisses die Daten bestimmt sind, die der Arbeitgeber zur Erfüllung seiner Pflichten oder Wahrnehmung seiner Rechte gegenüber dem Arbeitnehmer vernünftigerweise benötigt, sofern damit nicht in unverhältnismäßiger Weise in das Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird. Bei der Kontrolle von Verbindungsdaten wird meist das Arbeitgeberinteresse überwiegen, insbesondere wenn er damit die ausschließlich dienstliche Nutzung von Internet und E-Mail überprüfen möchte. Eine Inhaltskontrolle wird somit als zulässig angesehen.

3.3.2 Einwilligung des Arbeitnehmers

Eine Erlaubnis kann sich aus einer Einwilligung des Arbeitnehmers ergeben. Eine Einwilligung ist die vorherige Einverständniserklärung des betroffenen Mitarbeiters. Anforderungen an eine wirksame Einwilligungserklärung sind gemäß Art. 7 DS-GVO:

– Freiwilligkeit
  Die Einwilligung muss auf der freien Entscheidung der betroffenen Person beruhen. In dem Über- / Unterordnungsverhältnis von Arbeitgeber und Beschäftigten ist eine Einwilligung unfreiwillig und daher unwirksam, wenn eine wirtschaftliche Machtposition des Arbeitgebers zur Erlangung der Einwilligung ausgenutzt wurde. Dabei enthält § 26 Abs. 2 S. 2 BDSG Erleichterungen, insbesondere für den Fall, dass dem Beschäftigten durch die Einwilligung ein Vorteil entsteht oder die Interessen der Parteien gleich gelagert sind; hier kann von der Freiwilligkeit der Einwilligung ausgegangen werden. Diese Anforderungen sollten auch im Anwendungsbereich der DS-GVO weiterhin berücksichtigt werden.

– Konkretheit der Einwilligung; Transparenz
  Der Beschäftigte ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Nur

wenn er die vorgesehenen Verarbeitungen kennt, kann er sich frei entscheiden. Eine pauschale Erklärung der betroffenen Person, sie sei mit jeder weiteren Form der Verarbeitung ihrer Daten einverstanden, reicht nicht aus. Das bedeutet, dass eine Einwilligung fallbezogen einzuholen ist.

– Widerrufsrecht
  Der betroffene Beschäftigte ist über sein Widerrufsrecht mit Wirkung für die Zukunft zu informieren. Ab dem Zeitpunkt des Widerrufs wird damit jede zukünftige Verarbeitung durch den Arbeitgeber rechtswidrig, soweit kein sonstiger Erlaubnistatbestand die Verarbeitung rechtfertigt. Auf der Grundlage der konkreten Einwilligung gespeicherte Daten müssen dann gelöscht werden, insbesondere wenn die betroffene Person dies fordert.

– Form
  Die DS-GVO knüpft eine rechtswirksame Einwilligung nicht an eine bestimmte Form. In Art. 7 Abs. 1 DS-GVO wird jedoch klargestellt, dass der Verantwortliche das Vorliegen einer Einwilligung nachweisen können muss. Neben der elektronischen Einwilligung wird daher auch künftig die Einwilligungserklärung in Textform zu empfehlen sein. Da diese Anforderungen letztlich auch in § 26 Abs. 2 S. 3 BDSG aufgestellt werden, sollte – insbesondere aus Gründen der Rechtssicherheit – eine entsprechende Vorgehensweise eingehalten werden.

– Keine Einwilligung im „Kleingedruckten“
  Soll ein Betroffener eine Einwilligung zusammen mit anderen Erklärungen abgegeben, z. B. im Rahmen eines Arbeitsvertrages, darf die Einwilligungserklärung nicht im sogenannten „Kleingedruckten“ versteckt sein. Die Einwilligungserklärung muss dann deutlich sichtbar oder drucktechnisch von dem übrigen Text abgesetzt dargestellt werden (z. B. Fettdruck oder gesondert zu unterzeichnender Anhang), Art. 7 Abs. 2 S. 2 DS-GVO.

Hinweis

Liegt eine wirksame Einwilligung nicht vor, so helfen datenschutzrechtliche Zulässigkeitstatbestände nicht weiter, da es an einer Befreiung vom Fernmeldegeheimnis fehlt. Nach der hier vertretenen Auffassung kann der Ausgleich zwischen Compliance-Anforderungen und dem Schutz von Mitarbeiterdaten wegen der Sperrwirkung des § 3 TDDDG nur aufgrund einer Einwilligung erreicht werden.

Die Zulässigkeit der Durchführung von Compliance-Maßnahmen oder sonstige Kontrollen können sich auch nicht allein aus dem Abschluss einer Betriebsvereinbarung ergeben. Das liegt im Wesentlichen an § 3 Abs. 3 Satz 3 TDDDG, wonach eine Verwendung, insbesondere die Weitergabe an andere, nur zulässig ist, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Eine (noch nicht existierende) Betriebsvereinbarung ist aber keine solche Vorschrift, die eine entsprechende Verwendung „vorsieht“. Daher ist auch bei Vorliegen

einer Betriebsvereinbarung, die Kontrollen etc. regelt, zusätzlich eine Einwilligung zur Befreiung vom Fernmeldegeheimnis nötig.

Andererseits lassen sich durch eine Einwilligung allein nur schwer die Tatbestände etwaiger Kontrollen oder Compliance-Maßnahmen bzw. deren genaue Durchführung abbilden. Die insbesondere von der Rechtsprechung herausgebildeten Grundsätze zur Wahrung der Betroffenenrechte sehen feingranulare Schutzmechanismen, wie die Beteiligung der Mitarbeitervertretung, des betrieblichen Datenschutzbeauftragten jeweils in Abhängigkeit und Abwägung der Interessenlagen des Arbeitgebers und des Arbeitnehmers vor.

Hinweis

Zur Befreiung vom Fernmeldegeheimnis sind sowohl das Vorliegen einer Betriebsvereinbarung, die die Kontrollmaßnahmen regelt als auch eine zusätzlich wirksame Einwilligung des Betroffenen notwendig.

Zur EuGH-Rechtsprechung zur Betriebsvereinbarung als Rechtsgrundlage siehe Kapitel 4.

3.4 Ergebnis

Der Arbeitgeber hat ein berechtigtes Interesse daran, Missbrauch und strafbare Handlungen nicht nur bei dienstlicher, sondern auch bei privater Nutzung des Internets zu unterbinden sowie bei Abwesenheit eines Mitarbeiters Einsicht in die dienstlichen E-Mails des Mitarbeiters zu nehmen. Daher sollte er die private Nutzung an bestimmte Bedingungen, zum Beispiel hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführender Kontrollen knüpfen.

Es empfiehlt sich hierzu, entsprechende Regelungen in einer Betriebsvereinbarung unter Beteiligung des betrieblichen Datenschutzbeauftragten festzulegen. Darüber hinaus ist jeder Arbeitnehmer umfassend über die Bedingungen und Kontrollen bei der privaten Nutzung zu informieren und muss in diese einwilligen. Wenn der Arbeitnehmer diese Kontrollmaßnahmen nicht akzeptieren will, dann muss er die private Nutzung unterlassen.

4 Arbeitsrechtliche Aspekte

Kollektiv- und individualarbeitsrechtliche Fragen

4.1 Betriebsvereinbarung über die Nutzung betrieblicher Kommunikationsmittel zu privaten Zwecken

Arbeitgeber und Betriebsrat können besondere Erlaubnis-, Zweckbindungs- und Verbotsregelungen für die Verarbeitung und Nutzung von Personaldaten in Betriebsvereinbarungen regeln. Eine Betriebsvereinbarung ist eine eigenständige Zulässigkeitsnorm, Art. 88 Abs. 1 DS-GVO. Inhaltlich müssen die Betriebsvereinbarungen den Wertungen und den Grundsätzen der DS-GVO entsprechen. Die Grundsätze der Verarbeitung nach Art. 5 DS-GVO stehen damit grundsätzlich nicht zur Disposition bei Erlass nationaler Regelungen, jedoch kann der nationale Gesetzgeber unter Berücksichtigung der Grundsätze der DS-GVO die betrieblichen Begebenheiten konkretisieren und damit einheitlich für den ganzen Betrieb festlegen. In jedem Fall muss darauf geachtet werden, dass die jeweilige Betriebsvereinbarung den Anforderungen des Art. 88 Abs. 1, 2 DS-GVO entspricht. Eine bloße Wiederholung der Vorgaben der DS-GVO ist – wie bereits aufgezeigt – nicht ausreichend. Gerade bei der Festlegung und Formulierung der technischen und organisatorischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen (vgl. Art. 32 Abs. 1 DS-GVO) sollte daher mit besonderer Gründlichkeit vorgegangen werden. Zulässig ist auch, den Datenschutz zugunsten der Beschäftigten zu verstärken.

EuGH-Urteil vom 19. Dezember 2024 (C-65/23)

- Kollektivvereinbarungen können weiterhin nach § 26 Abs. 4 BDSG und Art. 88 DS-GVO formal als Grundlage für die Verarbeitung von Beschäftigtendaten herangezogen werden.
- Betriebsparteien sollten sich stets (zusätzlich) auf eine der allgemeinen Rechtsgrundlagen der Art. 6 und 9 DS-GVO stützen.
- Arbeitgeber müssen als datenschutzrechtlich Verantwortliche sicherstellen, dass jede Verarbeitung von Beschäftigtendaten den allgemeinen Vorgaben der DS-GVO entspricht, insbesondere den Grundsätzen aus Art. 5 DS-GVO (z. B. Rechtmäßigkeit, Transparenz, Zweckbindung und Erforderlichkeit) sowie den speziellen Anforderungen aus Art. 6 und 9 DS-GVO.

Der Gestaltungsfreiraum bleibt somit für die Betriebsparteien begrenzt. Sie müssen sich an die grundgesetzlichen Wertungen, zwingendes Gesetzesrecht und die allgemeinen Grundsätze des Arbeitsrechts halten. Aus diesem Grund sind in der Praxis kaum Fälle denkbar, in denen durch Betriebsvereinbarung das Schutzniveau der DS-GVO und des BDSG unterschritten werden kann.

Hinweis

- Es ist erforderlich, dass die Betriebsvereinbarung die jeweiligen Verarbeitungsvorgänge von personenbezogenen Beschäftigtendaten ausdrücklich anspricht und regelt. Es genügt nicht, dass die Verarbeitung bestimmter Informationen oder Daten „stillschweigend“ vorausgesetzt wird.
- Die Betriebsparteien sollten bestehende Betriebsvereinbarungen dahingehend prüfen, ob die Anforderungen des EuGH-Urteils eingehalten werden und gegebenenfalls Anpassungen vornehmen.

Kollektivrechtlich ist festzustellen, dass ein Mitbestimmungstatbestand beim Einsatz von betrieblichen Kommunikationsmitteln in aller Regel schon wegen § 87 Abs. 1 Nr. 6 BetrVG erfüllt ist, da Archivierungs- und Kontrollmaßnahmen regelmäßig durch technische Einrichtungen erfolgen, die dazu geeignet sind, Verhalten oder Leistung der Arbeitnehmer zu überwachen.

Von der Struktur her denkbar ist eine Rahmenvereinbarung „Einsatz von betrieblichen Kommunikationsmitteln“, denen dann jeweilige Einzelvereinbarungen „Festnetz“, „Mobile Kommunikation“ und „Internet“ untergeordnet sind und „gerätespezifische“ Regelungen ermöglichen.

4.2 Zuständigkeit des Betriebsrats

Für die Ausübung der Mitbestimmungsrechte ist grundsätzlich der Betriebsrat zuständig. In Unternehmen mit mehreren Betrieben sowie in Konzernunternehmen liegt aus technischen Gründen eine unternehmens- bzw. konzerneinheitliche Betriebsvereinbarung zur Nutzung betrieblicher Kommunikationsmittel zu privaten Zwecken nahe. Der Gesamtbetriebsrat ist nach dem BetrVG jedoch nur dann zuständig, wenn die Angelegenheit das gesamte Unternehmen oder mehrere Betriebe betrifft. Entsprechendes gilt für den Konzernbetriebsrat.

Hinweis

Um rechtliche Risiken zu vermeiden wird empfohlen, dass die örtlichen Betriebsräte oder die Gesamtbetriebsräte das übergeordnete Gremium mit dem Abschluss einer Gesamt- oder Konzernbetriebsvereinbarung beauftragen. Hierdurch wird dann die Zuständigkeit kraft Auftrags begründet (vgl. §§ 50 Abs. 2, 58 Abs. 2 BetrVG).

4.3 Individualarbeitsrechtliche Aspekte

4.3.1 Nutzungsumfang der privaten Nutzung von betrieblichen Kommunikationsmitteln

Soweit im Arbeitsvertrag keine ausdrückliche Regelung enthalten ist, obliegt dem Arbeitgeber ein Direktionsrecht gemäß § 106 GewO. Der Arbeitgeber kann danach frei über das „Ob“ und den Nutzungsumfang der Privatnutzung von betrieblichen Kommunikationsmitteln entscheiden.

Die Festlegung des Umfangs der erlaubten Privatnutzung von betrieblichen Kommunikationsmitteln obliegt allein der Entscheidung des Arbeitgebers. Hat jedoch der Arbeitgeber über den erlaubten Umfang der privaten Nutzung von betrieblichen Kommunikationsmitteln keine klare Regelung getroffen, ist jeweils durch die Auslegung zu ermitteln, welcher Nutzungsumfang im Einzelfall erlaubt ist. Naturgemäß führt eine solche Auslegung im Einzelfall zu einem hohen Streitpotential. Eine klare Regelung ist daher dringend zu empfehlen.

Eine übermäßige Nutzung von betrieblichen Kommunikationsmitteln zu privaten Zwecken wird vom Arbeitgeber keinesfalls gestattet und kann auch nicht durch eine betriebliche Übung erlaubt sein.

4.3.2 Betriebliche Übung durch Duldung der privaten Nutzung

In der Praxis kommt es immer wieder vor, dass die private Nutzung von betrieblichen Kommunikationsmitteln im Unternehmen nicht geregelt ist. Hat der Arbeitgeber die private Nutzung von betrieblichen Kommunikationsmitteln über einen längeren Zeitraum geduldet, kann ein Privatnutzungsrecht des Arbeitnehmers entstehen. Hierbei ist streitig, ob dies durch betriebliche Übung oder aufgrund eines Vertrauenstatbestandes geschieht. Die Rechtsfolge einer betrieblichen Übung durch Duldung der privaten Nutzung ist wiederum, dass bei fehlenden Regelungen Kontrollrechte des Arbeitgebers verboten sind.

Hinweis

Empfehlenswert sind konkrete Regelungen zum „Ob“ und „Wie“ der privaten Nutzung von dienstlichen Kommunikationsmitteln. Hat der Arbeitgeber dies nicht ausdrücklich geregelt, aber die private Nutzung gebilligt, entsteht eine betriebliche Übung, die zu Rechtsrisiken für den Arbeitgeber führt. Insbesondere sind dann Kontrollrechte des Arbeitgebers ausgeschlossen.

Anhang

Muster arbeitsvertragliche Regelung

Vereinbarung über die Nutzung von Internet und E-Mail

zwischen

….
– nachfolgend „Arbeitgeber“ genannt –

und

Herrn / Frau …
– nachfolgend „Arbeitnehmer/in“ genannt –

1 Grundsätzliches Verbot der Privatnutzung

Die Nutzung des betrieblichen Internetanschlusses sowie die Nutzung des E-Mail-Systems dürfen grundsätzlich nur für dienstliche Zwecke erfolgen.

Ausnahmen hiervon stehen unter dem Vorbehalt des Abschlusses dieser Vereinbarung und werden in dieser abschließend geregelt.

Kommt diese Vereinbarung nicht zustande, bleibt es beim Verbot der Privatnutzung.

2 Erlaubte Privatnutzung

Neben der betrieblichen Nutzung ist dem Arbeitnehmer während seiner Pausenzeiten in einem Umfang von täglich [höchstens zehn Minuten] die private Nutzung des Internets auf Grundlage dieser Vereinbarung gestattet.

Pausen sind keine Arbeitszeit und werden nicht als solche bezahlt.

Die private Nutzung darf keine negativen Auswirkungen auf die Arbeitsleistung haben.

Die Nutzung des dienstlichen E-Mail-Accounts und der dienstlichen E-Mail-Adresse zu privaten Zwecken ist untersagt.

Private E-Mails (d. h. sämtliche private elektronische Korrespondenz) dürfen nur über einen eigenen, privat eingerichteten E-Mail-Account abgewickelt werden.

3 Nutzungsverbote

Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet, sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.

Keinesfalls zulässig ist die Nutzung (u. a. Abrufen, Empfangen, Verbreiten, Anbieten und Verarbeiten von Daten, Texten, Äußerungen oder Abbildungen), die

- gegen datenschutzrechtliche, persönlichkeitsrechtliche, lizenz- oder urheberrechtliche oder strafrechtliche Bestimmungen verstößt,
- beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische oder pornographische Inhalte aufweist,
- die Ziele des Arbeitgebers stört oder mit diesem in Wettbewerb steht,
- geschäftsmäßige Werbung beinhaltet,
- Dritten Informationen über oder Listen von Arbeitnehmern, Kunden oder Lieferanten zukommen lässt,
- geschäftsmäßige Verteilerlisten einbezieht,
- sexuell eindeutige Bilder oder Beschreibungen enthält,
- illegale Aktionen oder Intoleranz gegen Andere befürwortet,
- sich gegen die Sicherheit von IT-Systemen richtet (z. B. Angriffe auf externe Webserver)
- die sich gegen das Unternehmen richtet (sog. Compliance-Verstöße z. B. Überlastung des Servers wegen Downloads zu großer Datenmengen)

Ebenfalls unzulässig ist:

- das private Bestellen mit Angabe der dienstlichen E-Mail-Adresse,
- das Aufrufen kostenpflichtiger Internet-Seiten,
- der Abschluss von privaten Kaufverträgen mit Angabe der geschäftlichen E-Mail-Adresse,
- die Teilnahme an Versteigerungen mit Angabe der geschäftlichen E-Mail-Adresse,
- die Nutzung von sozialen Netzwerken mit Angabe der geschäftlichen E-Mail-Adresse.

Es dürfen keine fremden Programme bzw. Dateien auf den IT-Einrichtungen des Arbeitgebers kopiert, bearbeitet, gespeichert oder sonst wie eingesetzt werden.

Es dürfen keine Datenträger oder Speichermedien, die nicht vom Arbeitgeber ausdrücklich freigegeben wurden, an den IT-Einrichtungen des Arbeitgebers eingesetzt werden.

Ggf: Die Nutzung folgender Internetseiten bzw. -dienste ist untersagt und die Seiten sind daher gesperrt: […]

4 Protokollierung / Archivierung / Datensicherung

4.1 Die Nutzung des Internets wird, soweit dies für die Gewährleistung der Systemsicherheit und / oder der Funktionsfähigkeit der eingesetzten IT-Systeme erforderlich ist, mit folgenden Informationen für jedes aufgerufene Objekt protokolliert:

- Datum / Uhrzeit
- Benutzerkennung
- IP-Adresse
- Zieladresse
- übertragene Datenmenge
- *... [abschließende Aufzählung aller Protokolldaten]*

4.2 Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

- Datum / Uhrzeit
- Absender- und Empfängeradresse
- Message ID
- Nachrichtengröße
- Betreff
- *… [abschließende Aufzählung aller Protokolldaten]*

4.3 Die Protokolldaten nach Ziffer 4.1 und 4.2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler
- Gewährleistung der Systemsicherheit
- Optimierung des Netzes und
- Datenschutzkontrolle
- Abrechnung
- ggf. Aktualisierung der Liste gesperrter Internet-Seiten (Black-List)

verwendet.

Die Protokolldaten nach Ziffer 4.1 werden für maximal […] Tage, Protokolldaten nach Ziffer 4.2 werden für maximal […] Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert.

Die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs werden zur Sicherstellung der Funktionsfähigkeit des Systems im Abstand von […] Tagen gespeichert und für maximal [...] Jahre aufbewahrt.

Um gesetzlich vorgegebenen Aufbewahrungspflichten (z. B. gem. § 257 HGB, § 147 AO) gerecht zu werden, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs im Abstand von […] Tagen archiviert. Jeder Mitarbeiter muss hierfür gemäß des Löschkonzepts (Anlage) den Inhalt seines E-Mail-Postfachs

klassifizieren. Die E-Mails werden dann nach der jeweiligen Aufbewahrungs- und Löschfrist aufbewahrt.

5 Widerrufsvorbehalt

Die Erlaubnis zur privaten Nutzung nach Ziffer 2 dieser Vereinbarung erfolgt unter dem ausdrücklichen Vorbehalt eines jederzeitigen Widerrufs. Das Recht auf private Nutzung kann widerrufen werden, wenn eine missbräuchliche Nutzung (Verstoß gegen die Nutzungsverbote gegen Ziffer 3 dieser Vereinbarung, Eröffnung von Sicherheitsrisiken, …) festgestellt wurde.

6 Zugangsberechtigungen

Die IT-Einrichtungen (insbesondere Internet und E-Mail) dürfen nur mit der gültigen persönlichen Zugangsberechtigung genutzt werden. User-ID und Passwort dürfen nicht weitergegeben werden.

7 Regelung bei Abwesenheit

Bei geplanter Abwesenheit ist durch den Arbeitnehmer ein automatisierter Hinweis auf die Abwesenheit des Arbeitnehmers sowie auf seine Vertretung einzurichten. Soweit dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

Wurde eine Abwesenheitsnachricht entgegen nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.

Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Arbeitnehmers für betriebliche Zwecke – etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden – kann erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

8 Schutz personenbezogener Daten

Absender und Empfänger von elektronisch übermittelten personenbezogenen Daten sind allein für deren weitere Verwendung verantwortlich. Sie entscheiden über Löschung oder Weiterleitung im Rahmen der gesetzlichen Vorgaben und betrieblichen Regelungen.

Zum Schutz der Empfängeradressen dürfen E-Mails an Extern bei Verwendung sog. Mailverteiler ausschließlich als Blindkopie („BCC“, „Blind Copy“) adressiert werden.

9 Datensicherung / Kontrolle / Offenlegung

Der Arbeitnehmer willigt ein, dass der Arbeitgeber zur Sicherstellung eines ordnungsgemäßen Gebrauchs der IT-Systeme berechtigt ist, Datensicherungen und Kontrollen – auch in Fällen der privaten Nutzung – vorzunehmen. Dies schließt den Einsatz von sog. „Spam-

Filtern“ (Werkzeuge zur Ermittlung unzulässiger E-Mails) ein. Weiter können Sicherheitssysteme wie sog. Virenscanner, Firewalls, etc. eingesetzt werden.

Erkannte Spammails werden im Betreff mit dem Wort „Spam“ markiert und an den Empfänger weitergeleitet. Dieser hat sorgfältig zu prüfen, inwieweit es sich tatsächlich um eine Spam-Nachricht handelt. Ist dies zutreffend, sollte diese unverzüglich gelöscht werden und der Erhalt derartiger E-Mails möglichst unterbunden werden.

Liegen konkrete Anhaltspunkte dafür vor, dass eine E-Mail Schadsoftware enthält, so wird diese automatisiert herausgefiltert und untersucht. Bestätigt sich der Verdacht, findet eine Weiterleitung an den Empfänger nur statt, wenn zuvor die entsprechenden Teilinhalte oder Anlagen entfernt wurden und Störungen oder Schäden durch die Weiterleitung ausgeschlossen werden können.

Von dieser Vereinbarung unberührt bleibt die Möglichkeit des Arbeitgebers, die dienstliche Nutzung von Internet und E-Mail zu überprüfen. Hierzu gehören insbesondere auch Stichproben zur Kontrolle, ob die tatsächliche Nutzung (insbesondere hinsichtlich Zeit, Umfang und Inhalt) im Rahmen dieser Vereinbarung erfolgt.

Bei behördlichen Aufforderungen zur Offenlegung der elektronischen Daten kann der Zugriff auch auf die gegebenenfalls vorhandenen privaten Daten erfolgen.

……	……	……
Ort, Datum	Unterschrift Arbeitgeber	Unterschrift Arbeitnehmer

Datenschutzrechtliche Einwilligung

Ich willige ein, dass auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe im Rahmen dieser arbeitsvertraglichen Vereinbarung verarbeitet und unter den Voraussetzungen der Ziffern 4 und 9 dieser Vereinbarung protokolliert sowie personenbezogen ausgewertet werden.

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gem. § 3 TDDDG verzichte.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs das Internet nicht mehr privat nutzen darf. Der Widerruf erfolgt durch Mitteilung in Textform an *[verantwortliche Stelle].*

Soweit die Einwilligung nicht widerrufen wird, gilt sie zeitlich unbeschränkt.

Die Erteilung der Einwilligung ist freiwillig.

Meine Betroffenenrechte Recht auf Auskunft (Art. 15 DS-GVO), Recht auf Berichtigung (Art. 16 DS-GVO), Recht auf Löschung (Art. 17 DS-GVO), Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO), Widerspruchsrecht gegen die Verarbeitung (Art. 21 DS-GVO) und Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) sind mir bekannt.

Bei Fragen und Beschwerden kann ich mich an den Arbeitgeber oder an den Datenschutzbeauftragten

[Name, Abteilung bzw. bei externem Datenschutzbeauftragten Name, Adresse]
[E-Mail-Adresse]
[Telefonnummer]

wenden.

……
Ort, Datum, Unterschrift des Einwilligenden

Ansprechpartner/Impressum

Kristina Fink
Grundsatzabteilung Recht

Telefon 089-551 78-234
kristina.fink@vbw-bayern.de

Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de