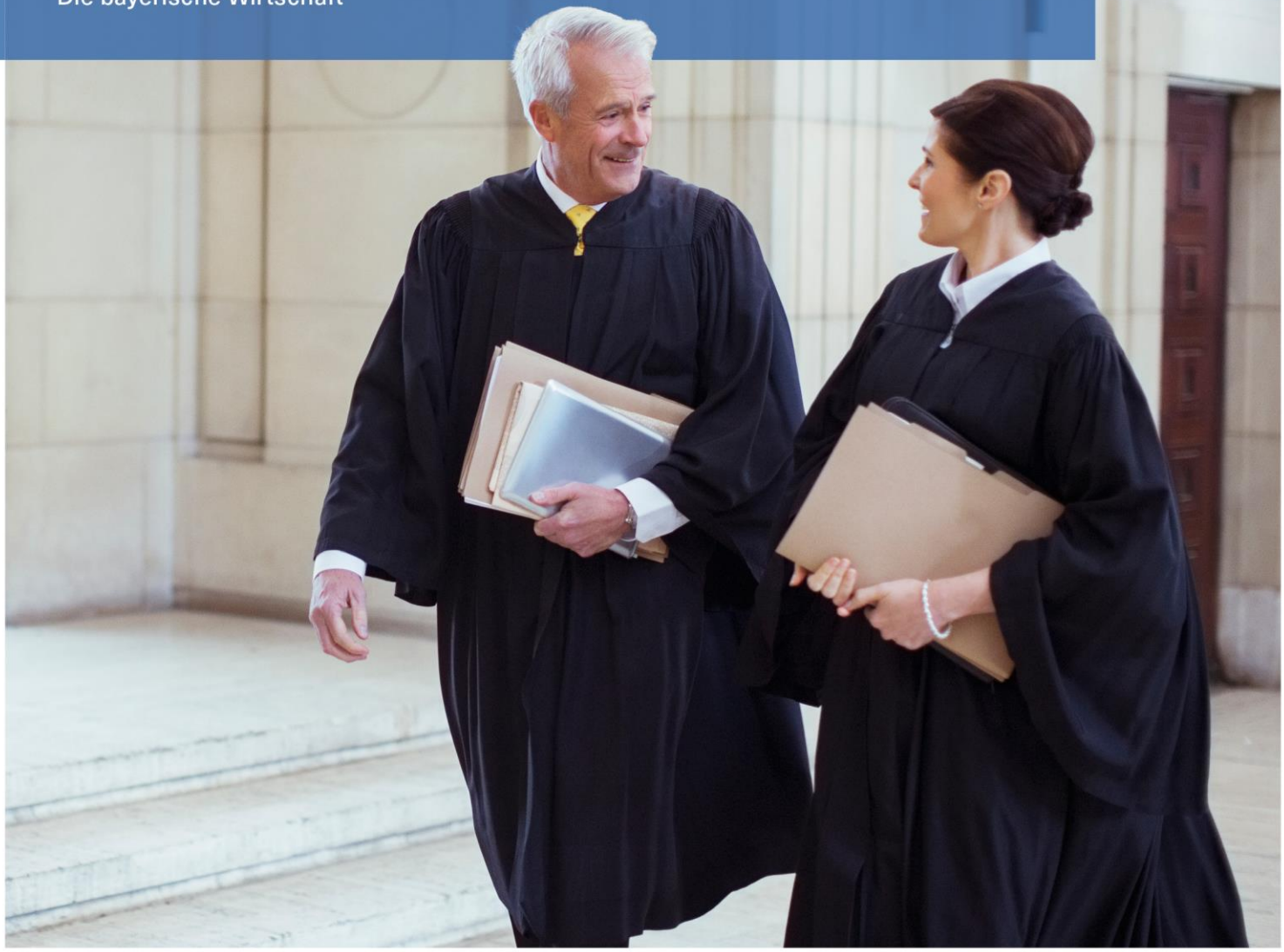
Recht

Privatnutzung von Internet und E-Mail am Arbeitsplatz

vbw

Info Recht
Stand: September 2023

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, beispielsweise bei Krankheit des Mitarbeiters, ist damit untersagt, sofern keine ausdrückliche Einwilligung des Mitarbeiters vorliegt. In diesen und anderen Fällen 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
01. September 2023

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.

Gerade im Mittelstand werden solche Empfehlungen von Geschäftsleitungen allerdings mit Zurückhaltung aufgenommen. Zwar stellt die private Nutzung und Kontrolle des dienstlichen E-Mail-Accounts und Internetzugangs Unternehmen immer wieder vor rechtliche Probleme, die nicht neu sind, deren Lösung sich in der Praxis jedoch häufig schwierig zu gestalten scheint. Andererseits wird von den Geschäftsleitungen die hohe Motivation registriert, die von einer auch privaten Gestattung der Nutzung von Betriebsmitteln auf die Mitarbeiter ausgeht. Hinzu kommt, dass in einer Zeit, in der Arbeit und Freizeit immer mehr ineinander verschwimmen, von den Mitarbeitern (über Mobile Devices) ständige – und teilweise über mehrere Zeitzonen hinweg – Erreichbarkeit verlangt und somit die zumindest gelegentliche Nutzung dieser Mobile Devices für private Zwecke auch als ein Stück Gegenleistung dafür interpretiert wird. Auch Argumente der Sicherung des Betriebsfriedens und das Bedürfnis, die Mitarbeiter durch ein enges Regime der ausschließlichen dienstlichen Nutzung von Betriebsmitteln nicht zu gängeln, finden sich in der Praxis immer wieder.

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 und zur Datensicherheit siehe auch

- Leitfaden *Datenschutz und Datensicherheit*
- 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. Auf das auch seitens der Geschäftsleitungen oftmals akzeptierte Bedürfnis, Betriebsmittel zum Zwecke privater Kommunikation zuzulassen, ist unter Ziffer 2 schon eingegangen worden. Denkbar erscheinen aber auch andere Zwecke, wie 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-Telemedien-Datenschutz-Gesetz (TTDSG) 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 TTDSG 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 TTDSG 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 TTDSG), 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. Für die Praxis sind jedoch bereits jetzt die folgenden Aspekte zu berücksichtigen:

Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedsstaaten spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten vorsehen. Diese Vorschriften müssen nach Art. 88 Abs. 2 DS-GVO zudem geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen, z. B. im Hinblick auf die Transparenz der Datenverarbeitung und die Überwachungssysteme am Arbeitsplatz. Entgegen diesen Vorgaben in Art. 88 DS-GVO handelt es sich bei § 26 Abs. 1 S. 1 BDSG jedoch nicht um eine „spezifischere Vorschrift“, sondern um eine Generalklausel, welche lediglich die Vorgaben der DS-GVO wiederholt und insbesondere keine gesonderten Schutzmaßnahmen zugunsten der betroffenen Personen enthält. 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 sind jedoch Konstellationen denkbar, in denen auch eine gründlichere Prüfung der nunmehr tauglichen Rechtsgrundlage erforderlich werden kann. Einerseits hat sich das oben zitierte Urteil des EuGH ausdrücklich nur auf Abs. 1 S. 1 von § 26 BDSG bezogen. Ob und inwieweit diese Rechtsprechung daher auf die weiteren Absätze von § 26 BDSG übertragbar ist, ist nicht abschließend geklärt. Einige rechtliche Argumente sprechen jedoch dafür, dass zumindest die Kernaussagen des Urteils auch auf weitere Absätze von § 26 BDSG übertragbar sind. Insbesondere bei der Verarbeitung personenbezogener Daten auf Basis einer Betriebsvereinbarung (vgl. hierzu § 26 Abs. 4 BDSG) sollten Unternehmen eine datenschutzrechtliche Prüfung der bisherigen Verarbeitungstätigkeiten veranlassen und die weiteren Entwicklungen im Auge behalten. Hier gilt es genau zu bewerten, ob und inwieweit das zitierte Urteil des EuGH Auswirkungen auf bestehende Prozesse und Betriebsvereinbarungen entfaltet. Da dies jedoch mitunter eine gewisse fachliche Expertise erfordert, sollte in Zweifelsfällen professioneller Rechtsrat eingeholt werden.

Auf der anderen Seite existieren in § 26 BDSG Regelungen, welche lediglich klarstellender Natur sind. 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 schriftliche Einwilligungserklärung 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.

– Fortgeltung von Einwilligungen
  Nach Erwägungsgrund 171 der DS-GVO ist es nicht erforderlich, dass die betroffene Person zu einer gleichartigen fortgesetzten Datenverarbeitung, zu der sie gemäß der Datenschutz-Richtlinie bzw. der entsprechenden Umsetzung durch das BDSG-alt eingewilligt hat, erneut einwilligt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht.

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 TTDSG 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 TTDSG, 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.

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, deren Kenntnisnahme jeder Arbeitnehmer schriftlich bestätigen muss. Darüber hinaus ist jeder Arbeitnehmer umfassend über die Bedingungen und Kontrollen bei der privaten Nutzung zu informieren. 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.

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 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.

Muster

Betriebsvereinbarung für die private Nutzung des Internets[1]

Hinweis

Im folgenden Muster wird davon ausgegangen, dass den Beschäftigten die private Internetnutzung (welche auch die Nutzung von Webmail-Diensten, wie z. B. web.de, gmx.net, umfasst) gestattet wird, eine private Nutzung des betrieblichen E-Mail Accounts jedoch verboten ist.

Zwischen

[Name, gesetzliche Vertretung, Anschrift des Arbeitgebers]

– im folgenden „Arbeitgeber“ –

und

dem (Konzern- / Gesamt) Betriebsrat des

[Name, gesetzliche Vertretung, Anschrift des Arbeitgebers]

– im folgenden „Betriebsrat“ –

wird folgende Betriebsvereinbarung

„Nutzung von Internet und E-Mail“

geschlossen.

[Präambel]

[1] Basierend auf der Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz vom Januar 2016 unter Berücksichtigung des ab 25. Mai 2018 geltenden Datenschutzrechts

1. Gegenstand und Geltungsbereich

1.1 Die Betriebsvereinbarung regelt die Grundsätze für die Nutzung der betrieblichen Kommunikationssysteme E-Mail und Internet.

1.2 Diese Betriebsvereinbarung gilt räumlich für […]

1.3 Die Betriebsvereinbarung gilt persönlich für Beschäftigte der [...].

2. Betriebliche und/oder private Nutzung

2.1 Die Nutzung der vom Arbeitgeber zur Verfügung gestellten Kommunikationssysteme und Endgeräte zur Nutzung von Internet ist grundsätzlich nur zu betrieblichen Zwecken gestattet. Als Endgeräte im Sinne dieser Betriebsvereinbarung gelten insbesondere der Arbeitsplatzrechner, Handys, Smartphones, Tablets oder Laptops.

2.2 Das betriebliche E-Mail-Postfach darf ausschließlich zur betrieblichen Kommunikation genutzt werden.

2.3 Die Gestattung der privaten Nutzung des Internetzugangs nach den Vorgaben dieser Betriebsvereinbarung erfolgt ausschließlich gegenüber denjenigen Beschäftigten, die zuvor gegenüber dem Arbeitgeber eine schriftliche Einwilligung gemäß Anlage 1 abgegeben haben.

2.4 Liegt eine Einwilligung vor, ist die private Nutzung des betrieblichen Internets während der Pausenzeiten in einem Umfang von täglich höchstens *[z. B. zehn Minuten]* zulässig.

2.5 Die Beschäftigten sind frei in ihrer Entscheidung, ob sie eine solche Einwilligung abgeben wollen. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerruflich. Soweit die Einwilligung nicht erteilt wird oder widerrufen wurde, so ist nur eine betriebliche Nutzung zulässig.

3. Verhaltensgrundsätze

3.1 Unzulässig ist jede vorsätzliche Nutzung der betrieblichen Kommunikationssysteme, die den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit schadet oder die gegen geltende Rechtsvorschriften verstößt. Dazu zählen Aktivitäten, die

- sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder
- sich gegen das Unternehmen richten (sog. Compliance-Verstöße *[von Vertragspartnern zu konkretisieren, z. B. Überlastung des Servers wegen Downloads zu großer Datenmengen]*)
- gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche

- oder strafrechtliche Bestimmungen verstoßen,
- Internetseiten betreffen, die beleidigende, verleumderische, verfassungsfeindliche, rassistische, sexistische oder pornographische Inhalte aufweisen,
- Ziele des Arbeitgebers stören oder mit diesem in Wettbewerb stehen,
- geschäftsmäßige Werbung beinhalten,
- Dritten Informationen über oder Listen von Arbeitnehmer, Kunden oder Lieferanten zukommen lassen,
- geschäftsmäßige Verteilerlisten einbeziehen,
- sexuell eindeutige Bilder oder Beschreibungen enthalten,
- illegale Aktionen oder Intoleranz gegen Andere befürworten.

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.

3.2 *[Hinweise, soweit bestimmte Internetseiten/ -dienste gesperrt werden (Black-List)]*

3.3 Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen ist der Download von Programmen aus dem Internet nicht gestattet.

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.

4. Nutzungsregelungen und Zugriffsrechte

4.1 [ggf. allgemeine Regelungen zum Herunterladen von Inhalten, Speicherungen von Anhängen / Dateien, Möglichkeit bzw. Pflicht zur Verschlüsselung von E-Mails etc.]

4.2 Bei geplanter Abwesenheit eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten 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.

4.3 a) Wurde eine Abwesenheitsnachricht entgegen 4.2 nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.

b) Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insbesondere soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.

c) Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Beschäftigten für betriebliche Zwecke – etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden – darf darüber hinaus nur erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

4.4 Derartige Zugriffe können unter Hinzuziehung von Vertrauenspersonen [konkret zu benennen] im Vier-Augen-Prinzip durchgeführt werden. Der Beschäftigte wird über den Zugriff unverzüglich unterrichtet. Erkennbar private E-Mails und solche, die der Kommunikation des Beschäftigten mit den unter 4.6 angesprochenen Stellen dienen, dürfen inhaltlich nicht zur Kenntnis genommen werden.

4.5 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.

4.6 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 2**) den Inhalt seines E-Mail Postfachs klassifizieren. Die E-Mails werden dann nach der jeweiligen Aufbewahrungs- und Löschfrist aufbewahrt.

4.6 Persönliche, aber geschäftlich veranlasste E-Mails (z. B. Kommunikation mit dem Betriebsrat, Betriebsarzt, Sozialberatung, Datenschutz oder Compliance Office) sollten über alternative Kommunikationswege abgewickelt werden (z. B. telefonisch, postalisch, private E-Mail-Adresse). Sollte dennoch derlei Kommunikation über das betriebliche E-Mail-Postfach abgewickelt werden, ist diese zu löschen bzw. lokal abzuspeichern. Bei einem Zugriff erkannte derartige Kommunikation (z. B. anhand des Betreffs bzw. Kommunikationspartners) darf inhaltlich nur durch den vorgesehenen Empfänger zur Kenntnis genommen werden.

5. Funktionspostfächer

E-Mail-Postfächer und die Internetkommunikation von Personen, die einer besonderen Vertraulichkeit unterliegen, sind von den Kontrollen nach dieser Vereinbarung ausgeschlossen. Eine Aufstellung dieser Postfächer findet sich in **Anlage 3.**

6. Spamfilter und Virenschutz

6.1 Durch eine zentrale Spamfilterung können Spammails erkannt werden, indem auf eingehenden E-Mails zugegriffen wird. 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.

6.2 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.

7. Verhaltenskontrolle

Die bei der Nutzung des betrieblichen E-Mail-Postfachs und des Internets anfallenden personenbezogenen Daten werden nur im Rahmen dieser Betriebsvereinbarung kontrolliert; insofern findet eine Verhaltenskontrolle statt. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften. Darüber hinausgehende Leistungs- und Verhaltenskontrollen werden nicht durchgeführt.

8. Protokollierung

8.1 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]*

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

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

8.3 Die Protokolldaten nach Ziffer 8.1 und 8.2 werden ausschließlich zu Zwecken der

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

verwendet.

8.4 Die Protokolldaten nach Ziffer 8.1 werden für maximal […] Tage, Protokolldaten nach Ziffer 8.2 werden für maximal […] Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert.

8.5 Personal, das Zugang zu Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet. Bei der Auswahl des Personals ist dies als Eignungsvoraussetzung zu berücksichtigen. Dafür wird auch (z. B. durch vertragliche Vereinbarung) Sorge getragen, wenn und soweit es sich nicht um eigenes Personal handelt.

9. Kontrollen

9.1 Zur Aktualisierung der gesperrten Internetseiten (Black-List) und zur Analyse von

- deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten oder
- extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externen E-Mail-Domänen

kann die geschäftliche und private Nutzung von Internet und E-Mail mit folgenden Kontrolldaten für einen Zeitraum von einem Monat protokolliert und getrennt von den Protokolldaten nach Ziffer 8.1 und Ziffer 8.2. gespeichert werden:

- Gruppenzugehörigkeit,
- Datum und Uhrzeit,
- genutzte externen E-Mail-Domänen,
- aufgerufene Internetdomänen (URLs),
- übertragene Datenmengen.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domainanalysen). Diese anonymen Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

9.2 Ergeben sich bei der Auswertung der Daten nach Ziffer 9.1 Hinweise auf unzulässige Zugriffe gem. Ziffer 3.1 oder auf eine Überschreitung der erlaubten privaten Nutzung, erfolgt eine gezielte Kontrolle (personenbezogene Auswertung) der in 8.1 und 8.2 genannten Daten. Zweck der Datenerhebung ist die Aufdeckung von Straftaten bzw. von erheblichen Pflichtverletzungen; der Umfang der von der Auswertung erfassten Personen muss dabei auf den Kreis der nach § 26 Abs. 1 S. 2 BDSG Betroffenen begrenzt werden. Es dürfen nicht sämtliche Beschäftigte überwacht werden.

9.3 Die personenbezogenen Daten sind nach Beendigung des Verfahrens zu löschen. Über das Ergebnis der Auswertung wird der Beschäftigte schriftlich in Kenntnis gesetzt. Ihm ist Gelegenheit zur Stellungnahme zu geben. Entsprechend der Ergebnisse der Auswertung ist das weitere Vorgehen abzuwägen:

- Einstellen der Kontrollen/keine weitere Überwachung,
- Verschärfen der Kontrolle, in dem die Protokollierung auf dem Endgerät i. S. v. 2.1 stattfindet

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bis hin zu einer Kündigung bleibt hiervon unberührt.

9.4 Für die Protokollierung auf dem Arbeitsplatzrechner gelten dieselben Anforderungen wie in 9.2. Die Beschäftigten müssen über diese Maßnahme nachträglich aufgeklärt werden.

9.5 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung, Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 über einen Zeitraum bis zu maximal […] Tagen aufzubewahren und personenbezogen auszuwerten.

Erweist sich der Verdacht als unbegründet oder werden die Protokolldateien nicht mehr zu weitergehenden Maßnahmen nach Ziffer 8 dieser Vereinbarung benötigt, so hat die zuständige Abteilung, die eine Speicherung der Protokolldaten über die in 8.4 festgelegte Dauer hinaus veranlasst hat, unverzüglich die Löschung dieser Daten durch die IT-Abteilung zu veranlassen. Die erfolgte Löschung ist schriftlich gegenüber der zuständigen Abteilung durch die IT-Abteilung zu bestätigen. Die Betroffenen werden nach Abschluss der Maßnahmen unverzüglich darüber benachrichtigt.

9.6 Ein Verstoß der Arbeitnehmer gegen diese Betriebsvereinbarung kann arbeitsrechtliche Konsequenzen haben.

Darüber hinaus kann ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen, z. B. bei Nutzung kostenpflichtiger Internetseiten.

Der Arbeitgeber behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs und des betrieblichen E-Mail-Postfachs im Einzelfall zu untersagen.

10. Datenschutz

Bei Fragen und Beschwerden können sich die Arbeitnehmer an den Arbeitgeber oder an den Datenschutzbeauftragten

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

wenden.

11. Betroffenenrechte

Sie haben die Rechte aus den Art. 15 – 22 DS-GVO:

- 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)
- Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)
- Widerspruchsrecht gegen die Verarbeitung (Art. 21 DS-GVO)

Bitte wenden Sie sich hierzu an folgende Stelle:

[Name / Abteilung, Kontaktdaten]

12. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten rechtzeitig mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden.

13. Schlussbestimmungen

13.1 Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden Betriebsrat und Arbeitgeberin unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

13.2 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist […] gekündigt werden.

13.3 Im Falle einer Kündigung dieser Betriebsvereinbarung gelten diese Regelungen bis zum Abschluss einer neuen Vereinbarung. Nach Eingang der Kündigung verpflichten sich die Betriebsparteien, unverzüglich Verhandlungen über eine neue Betriebsvereinbarung aufzunehmen.

Ort, Datum ……..	Ort, Datum ……..
……	……
Arbeitgeber	Betriebsrat

Anlagen:
Anlage 1: Einwilligungserklärung zur privaten Nutzung des betrieblichen Internets
Anlage 2: Löschkonzept
Anlage 3: Von den Kontrollen ausgenommene E-Mail-Postfächer

Anlage 1: Einwilligungserklärung zur privaten Nutzung der betrieblichen Kommunikationssysteme

Verwendungszweck:
Datenerhebung zur Kontrolle der im Rahmen der Betriebsvereinbarung *[Bezeichnung]* geregelten Privatnutzung von betrieblichen Kommunikationssystemen und Endgeräten

Ich,

……
Vor- und Nachname

……
Funktion

bei

……
Bezeichnung des Unternehmens / der Organisation

möchte von dem Angebot Gebrauch machen, die betrieblichen Kommunikationssysteme während der Pausenzeiten in einem Umfang von täglich höchstens *[z. B. zehn Minuten - entsprechend 2.4 der BV]* auch für private Zwecke zu nutzen.

Ich habe die Betriebsvereinbarung *[Bezeichnung]* zur Kenntnis genommen und bin mit folgenden, mit der Privatnutzung der betrieblichen Kommunikationssysteme verbundenen Nutzungsbedingungen, einverstanden:

- Die private Nutzung ist nur in den Pausenzeiten in einem Umfang von *[höchstens zehn Minuten]* täglich gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.
- 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.
- Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, ist unzulässig, insbesondere
  - der Abruf für den Arbeitgeber kostenpflichtigen Internetseiten,
  - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
  - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder

- Aktivitäten, die sich gegen das Unternehmen richten (sog. Compliance-Verstöße *z. B. Überlastung des Servers wegen Downloads zu großer Datenmengen*)
- 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.

Ich willige ein, dass auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe im Rahmen der Betriebsvereinbarung [Bezeichnung] vom [Datum einsetzen] verarbeitet und unter den Voraussetzungen der Ziffern 8. und 9. der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden.

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gem. § 3 TTDSG 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; aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile.

……
Ort, Datum, Unterschrift des Einwilligenden

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; Passwörter sind regelmäßig, d. h. alle […] Monate zu wechseln.

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 TTDSG 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; aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile.

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