Karl-Hermann Böker / Ute Demuth

E-Mail-Nutzung und Internetdienste

3. Auflage

Betriebs- und Dienstvereinbarungen

Analyse und Handlungsempfehlungen

BUND VERLAG

Hans Böckler Stiftung

Karl-Hermann Böker/Ute Demuth

E-Mail-Nutzung und Internetdienste

Betriebs- und Dienstvereinbarungen
Analyse und Handlungsempfehlungen

Eine Schriftenreihe der Hans-Böckler-Stiftung

Karl-Hermann Böker/Ute Demuth

E-Mail-Nutzung und Internetdienste

3., aktualisierte Auflage

BUND VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

3., aktualisierte Auflage

Redaktion: Dr. Manuela Maschke, Hans-Böckler-Stiftung
Herstellung: Birgit Fieber
Umschlaggestaltung: Neil McBeath, Stuttgart
Satz: Dörlemann Satz, Lemförde
Druck: CPI books GmbH, Leck
Printed in Germany 2014
ISBN 978-3-7663-6371-8

www.bund-verlag.de
www.boeckler.de/betriebsvereinbarungen

Inhaltsverzeichnis

Vorwort

Informations- und Kommunikationstechnik ist einem sehr schnellen Wandel unterworfen. Elektronische Kommunikation mit E-Mail über das Internet am stationären PC im Büro ist heute noch Standard, wird aber schon abgelöst von mobiler Internetkommunikation auf Online-Plattformen oder Social-Media-Anwendungen. Die E-Mail von heute wird es morgen womöglich nicht mehr geben. Leistungsfähige mobile Notebooks, Smartphones, Tablets etc. fördern das Arbeiten unterwegs. Der Arbeitsort ist flexibel, der Arbeitsinhalt aufgrund digitaler Zugangswege auch und der Mensch ohnehin. Die Grenzen zwischen privater und beruflicher Welt weichen immer stärker auf. Teils ist diese Grenzverwischung gewollt und wird aktiv von Beschäftigten vorangetrieben, teils ist sie nicht gewollt, aber kaum zu verhindern.

Mit diesen Entwicklungen ändern sich Arbeitsabläufe, aufgrund wachsender Geschwindigkeiten und Erwartungshaltungen verdichtet sich die Leistungserbringung zusehends. Nicht zuletzt wächst auch das Kontrollpotenzial. Es ist daher Zeit, danach zu fragen, ob und wie betriebliche Vereinbarungen diese Entwicklung aufnehmen, um Beschäftigte zu schützen und Gestaltungsspielräume für die betriebliche Mitbestimmung zu erwirken.

Die vorliegenden Vereinbarungen sind sehr unterschiedlich in ihrer Reichweite und Ausgestaltung. Erreichbar zu sein außerhalb der vereinbarten Arbeitszeiten, ist inzwischen ein Thema. Sehr unterschiedlich geregelt wird die Möglichkeit der privaten Nutzung von Internetdiensten und elektronischer Post durch die Beschäftigten. Es gibt Regelungen für das vollständige Verbot bis hin zur Unterstützung und Förderung der Privatnutzung. Gesundheitsschutz wird bislang nicht unbedingt sehr groß geschrieben.

Mit dieser dritten Aktualisierung der Auswertung wurden insgesamt 192 betriebliche Vereinbarungen der Jahre 1996–2013 ausgewertet. Es wird gezeigt, welche Regelungstrends zur Gestaltung der Arbeit mit In-

ternet und E-Mail-Anwendungen bestehen und wie die betrieblichen Akteure das Thema aufgreifen. Mit den Analysen verfolgen wir nicht das Ziel, Regelungen zu bewerten, die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen, Hinweise und Anregungen für die Gestaltung eigener Vereinbarungen zu geben.
Weitere Hinweise und Informationen zu unseren Auswertungen finden Sie im Internet unter www.boeckler.de/betriebsvereinbarungen.

Wir wünschen eine anregende Lektüre!

Dr. Manuela Maschke

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BildschArbV	Bildschirmarbeitsverordnung
BV	Betriebsvereinbarung
EDV	Elektronische Datenverarbeitung
IKT	Informations- und Kommunikationstechnik
IP	Internet-Protokoll
IuK-Technik	Informations- und Kommunikationstechnik
KBV	Konzernbetriebsvereinbarung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
VPN	Virtual Private Network

1. Veränderte Rahmenbedingungen der betrieblichen Nutzung von Internetdiensten

Die betriebliche Nutzung von Internetdiensten wurde in den letzten Jahren nicht nur selbstverständlich, sondern bestimmend für die meisten Büroarbeitsplätze. Die Beschäftigten müssen über die Qualifikationen verfügen, diese Technik zu nutzen und sie müssen mit den damit einhergehenden arbeitsorganisatorischen Veränderungen umgehen.
Die Kommunikation sowie die Informationsbeschaffung und -verteilung sind durch den Einsatz der Internetdienste schneller geworden. Das ermöglicht in vielen Bereichen immer zügigere Vorgangsbearbeitungen. Häufig ist eine Verdichtung von Arbeit die Folge: Besteht eine Möglichkeit, Vorgänge schneller zu bearbeiten, muss sie in der Regel auch genutzt werden; die Erwartungen der Kunden, Bürger und natürlich des Arbeitgebers steigen. Die verstärkte Nutzung der Internetdienste verbindet viele Arbeitsplätze noch intensiver mit Bildschirmarbeit – Mischarbeit ist dadurch immer schwieriger zu ermöglichen. Aus all dem resultieren neue Herausforderungen für den betrieblichen Gesundheitsschutz.
Beschäftigte müssen lernen, mit der räumlichen und zeitlichen Entgrenzung von Arbeit umzugehen, die eng mit der technischen Entwicklung verwoben ist. Private Nutzung, Arbeit im Homeoffice und die Nutzung von Geräten, die den Arbeitnehmerinnen und Arbeitnehmern gehören, weichen die Grenzen zwischen Arbeit und Privatsphäre auf. Beschleunigt wird diese Entwicklung immer wieder durch die Technik selbst: Soziale Medien werden im betrieblichen Zusammenhang zunehmend relevant, weil Arbeitgeber deren Potenziale für das Marketing und die Rekrutierung neuer Mitarbeiterinnen und Mitarbeiter entdecken. Die Beschäftigten selbst sollen zu (positiven) Botschaftern des Unternehmens werden. Zudem ermöglichen Smartphones und Tablet-PCs die mobile Nutzung zu jeder Zeit an jedem Ort. Viele der bisher vereinbarten betrieblichen Regelungen, die sich mit der privaten Nutzung der Internetdienste auf den vom Unternehmen bereitgestellten technischen

Geräten befassen, laufen zunehmend ins Leere und verlieren ihre Bedeutung, weil eine private Nutzung betrieblicher Geräte nicht mehr notwendig ist. Dennoch ist die juristische Auseinandersetzung mit der Frage der privaten Nutzung noch längst nicht abgeschlossen.

Die Einschätzung der Bedeutung von Datenschutz und Privatsphäre hat sich verändert: Die in jüngster Vergangenheit aufgedeckten staatlich und teilweise auch betrieblich angeordneten und durchgeführten massenhaften, anlasslosen Auswertungen personenbezogener Daten in den Telekommunikations- und Internetdiensten scheinen das Nutzungsverhalten kaum zu ändern. Es bleibt abzuwarten, wie sich Unternehmen auf lange Sicht gegen Wirtschaftsspionage schützen werden – möglicherweise führt das wiederum zu einem besseren Schutz der personenbezogenen Daten, die in Unternehmen anfallen.

Unternehmen, die eine sichere Netznutzung gewährleisten möchten, müssen den Datenverkehr detailliert protokollieren. Dies stellt jedoch ein Einfallstor dar für vielfältige Leistungs- und Verhaltenskontrollen und eine mögliche Gefährdung der Persönlichkeitsrechte der Beschäftigten. Betriebliche Vereinbarungen zu E-Mail und Internet hebeln teilweise elementare Grundrechte von Arbeitnehmerinnen und Arbeitnehmern aus, um vermeintlich großen und unternehmensgefährdenden Risiken zu begegnen.

Die vorliegende Auswertung von 192 neueren betrieblichen Regelungen zu E-Mail-Nutzung und Internetdiensten belegt, dass das Thema weiterhin aktuell ist. Für Arbeitgeber ist es wichtig, dass sie hinsichtlich der Protokollierung und Auswertung personenbezogener Daten der Beschäftigten Rechtssicherheit erhalten, die ihnen die aktuellen Gesetze und die Rechtsprechung nicht bieten. Für die Arbeitnehmerinnen und Arbeitnehmer und ihre Vertreter ist es wichtig, dass möglichst klare Verhaltensregeln geschaffen werden und der Schutz der Persönlichkeitsrechte gewährleistet ist.

2. Wesentliche Regelungsinhalte der aktuellen Vereinbarungen

2.1 Allgemeine Regelungen zu Internetdiensten

Zunächst werden die Inhalte betrieblicher Regelungen dargestellt, die für alle Internetdienste gültig sind, anschließend – sofern notwendig – spezielle Regelungen zu Internet, Intranet und E-Mail. Gelegentlich sind diese Regelungen Teil einer EDV- oder IKT-Rahmenvereinbarung oder sie wurden mit Regelungen zur Telefonnutzung zusammengefasst; diese Themen werden jedoch in dieser Auswertung nicht betrachtet. Hingegen enthalten neuere Vereinbarungen Regelungen zum betrieblichen Einsatz von Social Media bzw. sozialen Medien (→ Glossar). Besondere Beachtung fanden zudem in dieser Auswertung die Einwilligungserklärungen, die im Zusammenhang mit der privaten Nutzung betrieblicher Internetdienste häufig anzutreffen und von den Beschäftigten zu unterschreiben sind.

2.1.1 Regelungsgegenstand und Ziele der Vereinbarung

Der Einsatz von Internetdiensten im Unternehmen muss durch eine Betriebs- bzw. Dienstvereinbarung geregelt werden. Dies ergibt sich aus § 87 Abs. 1 Nr. 6 BetrVG, da die technischen Systeme, mit denen die Internet-, Intranet- und E-Mail-Dienste realisiert werden, grundsätzlich personenbezogene und -beziehbare Daten speichern, die zur Leistungs- und Verhaltenskontrolle geeignet sind. Personal- und Mitarbeitervertretungsgesetze enthalten vergleichbare Bestimmungen, so dass auch die Arbeitnehmervertretungen in deren Geltungsbereichen entsprechende Vereinbarungen abschließen sollten. In dieser Broschüre werden weiterhin nur die Paragrafen des Betriebsverfassungsgesetzes genannt.

Regelungsgegenstand

Viele Vereinbarungen nennen als Regelungsgegenstand die Nutzung technischer Systeme, z. B. des E-Mail-Systems, ohne sie genauer zu bezeichnen.

»Gegenstand dieser Vereinbarung ist:
– die Regelung zur Nutzung von Daten aus dem Internet und für die Bereitstellung von Daten für Internetnutzer,
– der Schutz des Datennetzes der [Firma],
– die Verfahrensweise bei der Nutzung und Auswertung der Protokollierung der Firewall und der Proxyserver [→ Glossar].«

Baugewerbe, 090300/187/2008

Die folgende Vereinbarung benennt zusätzlich explizit die Beteiligung der Betriebsräte als Regelungsgegenstand. Das deutet darauf hin, dass in der Vereinbarung die gesetzlichen Rechte der Betriebsräte und ihre Umsetzung genau festgeschrieben sind.

»Gegenstand dieser Betriebsvereinbarung sind die:
– Regelung der privaten Nutzung (§ 2),
– Nutzung des Abwesenheitsagenten (§ 3),
– Einhaltung des Datenschutzes (§ 4),
– Vermeidung von Leistungs- und Verhaltenskontrollen (§ 4),
– Regelung der Speicherung und Löschung von Daten (§ 4),
– Beteiligung des Gesamtbetriebsrates und des örtlichen Betriebsrates (§§ 4, 5, 6).«

Kreditgewerbe, 090300/136/2007

Ziele der Vereinbarung

Schutz

Das zentrale Interesse von Arbeitnehmervertretungen besteht darin, Kontrollmöglichkeiten zu regeln. Die Arbeitgeberseite zeigt ebenfalls großes Interesse an derartigen Regelungen. Die folgende Vereinbarung drückt dies bildhaft aus.

»Das Internet ist ein virtuelles Werkstor, das wie jeder andere Zugang einer Kontrolle bedarf. Diese Kontrollen führen zu Interessenskonflikten zwischen [... dem] Arbeitgeber bez. zweck- und bedarfsgerechten Einsatzes des Internets – abgeleitet aus dem Eigentumsrecht des Arbeitgebers (Art. 14 GG) – und den Mitarbeitern (Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 GG). Eigentumsrecht und Persönlichkeitsrecht müssen daher bei der Durchführung von Kontrollmaßnahmen zu einem Ausgleich gebracht werden.«

Kultur, Sport und Unterhaltung, 090300/135/2003

In Präambeln ist beispielsweise das Ziel genannt, die beiden unterschiedlichen Interessen miteinander zu verbinden.

»Durch diese Regelungen soll eine Balance zwischen den arbeitgeberseitigen Interessen des verantwortungsvollen Umgangs mit den zur Verfügung gestellten elektronischen Hilfsmitteln einerseits und dem Schutz der Persönlichkeitsrechte der Beschäftigten andererseits sichergestellt werden.«

Grundstücks- und Wohnungswesen, 090300/205/2009

Mit den Vereinbarungen beabsichtigen die betrieblichen Partner nicht nur, die Beschäftigten zu schützen, sondern auch Angriffe aus dem Internet abzuwehren und somit den Schutz des Unternehmens sowie der gespeicherten Daten und der informations- und kommunikationstechnischen Infrastruktur zu gewährleisten.

»Ziel und Inhalt dieser Betriebsvereinbarung ist die genaue Festlegung von Maßnahmen für die Sicherheit und den Schutz unserer Unternehmensdaten, die Einhaltung von Lizenzen und Urheberrechten sowie die Festlegung von Regeln im Umgang mit Internet und E-Mail.«

Möbelhersteller, 090300/170/2007

Mitarbeiterorientierung

Einige Vereinbarungen zielen insbesondere darauf ab, den Beschäftigten mehr Transparenz hinsichtlich der Datenverarbeitung zu bieten. Dies korrespondiert teilweise damit, dass sowohl arbeitgeber- als auch

arbeitnehmerseitig festgestellt und anerkannt wird, dass die umfangreiche Speicherung personenbezogener Daten der Beschäftigten unvermeidbar ist.

> »Diese BV soll den Mitarbeitern transparent machen, welche der von ihnen oder über sie erzeugten Daten gespeichert werden und wer Zugriff auf diese hat.«
>
> Versicherungsgewerbe, 090201/504/2011

Die Mitarbeiterorientierung geht in der folgenden Regelung weit darüber hinaus; derlei Präambeln oder Zielformulierungen finden sich jedoch selten in den vorliegenden Vereinbarungen.

> »An die Beschäftigten werden hinsichtlich Flexibilität und Mobilität hohe Anforderungen gestellt und es entspricht dem Selbstverständnis des [Konzerns], ihnen auch unter dem Gesichtspunkt der Vereinbarkeit von Beruf und Familie die Nutzung von geschäftlichen IT-Ressourcen im Rahmen der nachstehenden Grundsätze zu gestatten. Für den [Konzern] ist dies ein Baustein auf dem Weg, die Kompetenzen der Beschäftigten hinsichtlich einer effizienten IT-Nutzung zu erhöhen.«
>
> Landverkehr, 090300/322/2012

Rechtliche Absicherung

Ein weiteres gelegentlich vereinbartes Ziel besteht darin, rechtliche Sicherheit zu schaffen (vgl. Kap. 6.3). Einige der anzuwendenden Gesetze wurden in den letzten Jahren mehrfach geändert. Zusammen mit uneinheitlicher Rechtsprechung hat dies sowohl Beschäftigte als auch Arbeitgeber verunsichert. Die Vereinbarungen sollen zumindest auf der betrieblichen Ebene Sicherheit herstellen. Das Interesse der Arbeitgeber scheint diesbezüglich groß zu sein, wie die folgende Regelung vermuten lässt.

> »Sie dient auch zum Schutz des Arbeitgebers vor Schadenersatzansprüchen wegen Verletzungen des Urheberrechts oder anderer Rechte durch Beschäftigte.«
>
> Einzelhandel (ohne Kfz.), 090300/276/2005

Auch im öffentlichen Bereich bestehen vergleichbare Unsicherheiten, so dass die folgende Dienstvereinbarung ebenso die rechtliche Klärung zum Ziel hat.

> »Es soll verhindert werden, dass straf- oder zivilrechtlich relevante Handlungen bei der Nutzung begangen und die Sicherheitsbelange der Stadt [...] unzureichend beachtet werden.«
>
> Öffentliche Verwaltung, 090300/274/2012

2.1.2 Ziele der Nutzung von Internetdiensten

Für Unternehmen ist es inzwischen nicht nur selbstverständlich, sondern auch von hoher strategischer Bedeutung, das Internet zu nutzen. Die folgende Präambel einer Betriebsvereinbarung drückt dies beispielhaft aus.

> »Der Einsatz der Internet- und Intranet-Technologie sowie von E-Mail in den Konzerngesellschaften ist eine der Voraussetzungen, um als modernes und leistungsorientiertes Unternehmen erfolgreich am Markt tätig sein zu können.«
>
> Bekleidungsgewerbe, 090300/317/0

In den Vereinbarungen werden die Ziele formuliert, die mit der Nutzung der Internetdienste in Betrieben und Verwaltungen verfolgt werden – die wichtigsten sind aus Sicht der Arbeitgeber Wirtschaftlichkeit und Erfolg.

> »Die Nutzung des Internets und der anderen Dienste soll die Produktivität sowie die Ergebnisqualität bei der Aufgabenerledigung durch schnelle, effiziente und kostengünstige Informationsgewinnung und entsprechenden Informationsaustausch steigern.«
>
> Öffentliche Verwaltung, 090300/164/2009

Verbesserte Produktivität und Kundenorientierung werden ebenso häufig als Ziele genannt. Sie sind aber eher als Mittel anzusehen, um wirtschaftlichen Erfolg zu erreichen.

So manchem betrieblichen Partner ist unklar, wie sich die Internetdienste und deren Bedeutung in den nächsten Jahren fortentwickeln werden. Die Vereinbarungen sind daher gelegentlich zeitlich begrenzt und bei Bedarf zu aktualisieren. Aus denselben Gründen einigen sich Arbeitgeber und Betriebsrat auf Grundsätze und verzichten damit auf Detailregelungen.

> »Weil die Entwicklungsrichtung dieser Technologien nicht voraussehbar ist und Internet, Intranet und E-Mail durch Offenheit und wenig Einschränkungen gekennzeichnet sind, werden in dieser BV im Wesentlichen Grundsätze für die Nutzung vereinbart.«
>
> Bekleidungsgewerbe, 090300/317/0

Der eigene Internetauftritt des Unternehmens als ein Weg der besseren Kundenorientierung ist kein herausragendes Thema in den Vereinbarungen. Eine Bank bezeichnet es als vorteilhaft, wenn Daten und Bilder der Ansprechpartner für die Kunden im Internet sichtbar sind.

> »Durch die Hinterlegung von Kontaktdaten und Bildern der Beschäftigten kann der Internetauftritt der Bank persönlicher gestaltet werden.«
>
> Kreditgewerbe, 090300/223/2011

Im Sinne einer Win-win-Situation stellen die Vereinbarungen die Vorteile für die Beschäftigten heraus. An erster Stelle steht hier die verbesserte Kommunikation, intern und extern. Geht es hingegen um die persönlichen Vorteile für die Beschäftigten, wird die Argumentation bereits dünner. Genannt werden verbesserte Qualifikationsmöglichkeiten durch kontinuierliche Information und Schulung der Beschäftigten sowie bessere Arbeitsbedingungen durch Vereinfachung und Harmonisierung von medienbruchfreien Geschäftsprozessen. Die folgende Regelung aus der Rahmendienstvereinbarung einer öffentlichen Verwaltung nennt übergreifende Ziele.

> »Dabei sind im Rahmen der vorgegebenen Zuständigkeiten
> – die Handlungs- und Entscheidungsspielräume der an den IT-Arbeitsplätzen eingesetzten Beschäftigten zu erweitern,

– der Anteil der schematischen und manuellen Arbeitsabläufe zu verringern,
– die Fähigkeiten der an den IT-Arbeitsplätzen eingesetzten Beschäftigten weiterzuentwickeln und ihre IT-Kenntnisse bedarfsorientiert zu erweitern und zu vertiefen sowie
– die Zusammenarbeit der Beschäftigten zu verbessern.«

Öffentliche Verwaltung, 090300/209/2004

Eines der zentralen Probleme bei der Nutzung von Internetdiensten ist die Abwägung zwischen beruflicher und privater Nutzung. Dies schlägt sich bereits in den Zielformulierungen nieder, wie das folgende Beispiel zeigt (vgl. Kap. 2.1.12., 2.2.3 und 2.4.3).

»Die betrieblichen DV-Anlagen können für betriebliche Zwecke, zum kollegialen Austausch sowie zur Information und Kommunikation über berufliche (Brancheninformation, Marktrecherchen etc.) bzw. arbeitsbezogene (Arbeitsrechte und -pflichten, Gewerkschaften etc.) Themen genutzt werden.«

Anonym, 090300/146/0

2.1.3 Risiken der Internetdienste

Die Nutzung von Internetdiensten bringt für Unternehmen und Beschäftigte vielfältige Risiken mit sich, beispielsweise Folgende:

- Das Internet garantiert keine Vertraulichkeit beim Datenaustausch, das heißt: Per Internet versandte Daten können von anderen eingesehen und zurückverfolgt werden.
- Direkte Angriffe oder ein Eindringen von außen auf die unternehmensinternen Rechnersysteme, Netze und Daten mit dem Ziel der Ausspähung, Veränderung oder Zerstörung sind möglich.
- Vom Anwender können unbemerkt Viren, »Logikbomben« (→ Glossar) oder Ähnliches bei Benutzeraktivitäten im Internet eingeschleust werden, etwa durch Verstecken oder Tarnung in Bildschirmschonern, Bildern, Spielen etc.
- Durch Kettenbriefe, Grüße und Glückwunschaktionen können die Datennetze und Rechner des Unternehmens lahmgelegt werden.

- Gesetzliche Bestimmungen wie das Bundesdatenschutzgesetz (BDSG) können bei der Übermittlung von personenbezogenen Daten verletzt werden.
- Lizenzrechte, Wiedergaberechte und Eigentumsrechte können durch die Benutzung von Programmen, Bildern, Symbolen oder Warenzeichen aus dem Internet verletzt werden.
- Interne Unternehmensinformationen, die nicht für Dritte bestimmt sind, können (unbeabsichtigt) offengelegt werden.
- Imageschäden für das Unternehmen können entstehen: Beispielsweise können Meinungen, die in Internet-Foren von Beschäftigten geäußert werden, jedoch nicht mit den Unternehmenszielen und dem Unternehmensbild übereinstimmen, von Dritten fälschlicherweise als Unternehmensstandpunkt interpretiert werden. Beschäftigte können inzwischen auch durch Verwendung von Smartphones und Tablet-PCs geortet werden, was damit verbundene Persönlichkeitsrechte gefährdet.
- Eingescannte Unterschriften werden möglicherweise missbraucht.

Die Risiken haben sich in den letzten Jahren nicht grundlegend geändert. Sie scheinen aber zunehmend als Normalität angesehen zu werden, die mit technischen Mitteln und Maßnahmen zur Netzsicherheit zu bewältigen ist. Insbesondere begründet die notwendige Gefahrenabwehr, dass a) diverse technische Komponenten (Firewall, Proxyserver, Virenscanner etc.) alle Benutzeraktivitäten protokollieren, b) die Protokolle über einen begrenzten Zeitraum gespeichert bleiben und c) die digitale Kommunikation gescannt und gefiltert werden darf. Zusätzlich verweisen einige Vereinbarungen auf sensibilisierende Qualifizierungsmaßnahmen für die Beschäftigten.

> »Die zur Nutzung des Internets berechtigten Arbeitnehmer werden [...] in die mögliche Gefährdung des Datennetzes der [Firma] und unter Hinzuziehung des Datenschutzbeauftragten in die Gefahr der Abschöpfung von persönlichen Daten eingewiesen.«
>
> Baugewerbe, 090300/187/2008

Aktuell ausgewertete Vereinbarungen weisen – ebenso wie frühere – auf Gefahren und getroffene technische Abwehrmaßnahmen hin, ohne jedoch die Beschäftigten von einer Mitschuld für eventuell entstehende

Schäden zu entlasten. Insbesondere rufe die private Nutzung der betrieblichen Internetzugänge besondere Gefahren hervor. Mit dieser – nicht immer vollständig nachvollziehbaren – Argumentation begründen die Betriebsparteien gelegentlich, dass die Privatnutzung vollständig verboten wird (vgl. Kap. 2.1.12).
Vermehrt enthalten neuere Vereinbarungen Hinweise darauf, dass durch private Nutzung – insbesondere durch soziale Medien – Arbeitszeiten verschwendet und berufliche Verpflichtungen vernachlässigt werden könnten. Für diese Art der Gefährdung sind bisher nur appellierende Regelungen wie die Folgende anzutreffen.

> »Die Nutzung von Internet-Diensten muss – angesichts der hierfür erforderlichen Arbeitszeit – in einem wirtschaftlichen Verhältnis stehen.«
>
> Verlags- und Druckgewerbe, 090300/272/2005

Die berufliche Nutzung sozialer Medien wird zunehmend von Arbeitgebern eingefordert und teilweise auch von Arbeitnehmern gewünscht. Dies stellt schließlich eine weitere Gefahr dar, die in der folgenden Regelung angesprochen wird.

> »Die Einführung, Weiterentwicklung und Nutzung von Social Media im Unternehmen darf nicht zu einer Arbeitsverdichtung und damit zu einer höheren Belastung der Beschäftigten führen. Hiermit ist insbesondere die Entgrenzung von Arbeitsort, Arbeitsinhalten und Arbeitszeiten gemeint.«
>
> Anonym, 090300/295/0

2.1.4 Sicherungsmaßnahmen

Die Nutzung des Internets stellt in mehrfacher Hinsicht ein Risiko dar (vgl. Kap. 2.1.3), sowohl für die Unternehmen und Verwaltungen als auch für deren Beschäftigte. Die Betriebs- und Dienstvereinbarungen regeln auf vielfältige Weise und unterschiedlich detailliert, wie Sicherungen aussehen dürfen. Dies ist notwendig, weil technische Sicherungsmaßnahmen immer personenbezogene und personenbeziehbare Daten

von Beschäftigten speichern und verarbeiten. Demnach müssen Regelungen gemäß §87 Abs. 1 Nr. 6 BetrVG getroffen werden, damit diese Systeme rechtmäßig eingesetzt werden. Auch organisatorische Maßnahmen zur Sicherung gegen die im Zusammenhang mit dem Internet bekannten Gefahren sind regelmäßig mitbestimmungspflichtig. Denn sie berühren Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb (§87 Abs. 1 Nr. 2 BetrVG).

Dieses Kapitel behandelt die technischen Sicherungsmaßnahmen, die in den vorliegenden Vereinbarungen beschrieben werden; außerdem übergreifende organisatorische Maßnahmen, die keine direkten Verhaltensregeln für Mitarbeiter darstellen. Letztere sind in Kapitel 2.1.16 und in den speziellen Kapiteln zur Internet-, Intranet- und E-Mail-Nutzung beschrieben.

Technische und globale organisatorische Sicherungsmaßnahmen dienen mehreren Zwecken:

- das Unternehmen und seine Datennetze gegen externe Angriffe zu schützen
- die Mitarbeiter vor Verletzungen ihrer Persönlichkeitsrechte zu schützen
- Kontrollen durchführen zu können.

Diese Zwecke sind in den vorliegenden Vereinbarungen jedoch nicht explizit unterschieden, so dass hier eine eher künstliche Trennung vorgenommen wird. Nicht alle Maßnahmen lassen sich eindeutig einem der drei Aspekte zuordnen.

Neueren Vereinbarungen ist gelegentlich anzusehen, dass die Herausforderungen größer geworden sind bzw. sich verändert haben. Daher nennen sie die folgenden zu regelnden Problembereiche:

- Neuere Rechner sind zunehmend leistungsfähig bei gleichzeitiger Miniaturisierung der Geräte und Datenspeicher. Sie sind Telefon, Fotoapparat und Computer zugleich. Durch die ständige Verfügbarkeit von Funknetzen ist der Zugang zum Internet praktisch immer gegeben.
- Beruflich genutzte private Hardware, mobile Geräte und die Verbreitung der Datenspeicherung in externen Speichern (Cloud Computing, → Glossar) machen es zunehmend schwieriger, klare Grenzen zu vereinbaren.
- Mit technischen Maßnahmen allein lassen sich die Herausforderungen nicht bewältigen, so dass sie durch organisatorische Maßnahmen

begleitet bzw. in einen sicheren organisatorischen Rahmen eingebettet sein müssen.

Den Vereinbarungen ist zu entnehmen, dass die Zentralisierung der Unternehmens-IT bzw. der Zugänge zum Internet das wesentliche Merkmal der Sicherheitsorganisation darstellt. Dies steht übrigens nicht völlig im Gegensatz zur Dezentralisierung der IT, die in den 1980er Jahren mit dem Aufkommen von Personal Computern einherging: Weiterhin werden PCs an den Arbeitsplätzen benutzt, doch sind sie in globale Datennetze der Unternehmen und Verwaltungen integriert und darüber mit dem Internet verbunden. Einige Unternehmen und Verwaltungen gehen aus Gründen der Sicherheit so weit, dass sie die Anwendung mobiler und privater Geräte nicht zulassen.

Technische Sicherungsmaßnahmen zur Lösung der genannten Probleme werden in einigen vorliegenden Vereinbarungen geregelt:

- Sicherung gegen externe Angriffe
  - Firewall
  - Proxyserver.

> »Die Schnittstelle zum Internet wird mit einer Firewall und Proxyservern abgesichert. Die Firewall und die Maßnahmen für die innere Netzsicherheit gewährleisten, dass sowohl jeder von außen geführte Angriff auf Daten, Hard- und Software im Netz als auch eine Gefährdung für das Netz von innen abgewehrt werden. Die Proxyserver werden zum Schutz gegen Viren, Spam, zur Authentifizierung und als Zugriffskontrolle eingesetzt.«
>
> Baugewerbe, 090300/187/2008

> »Um die Risiken zu minimieren, die der Anschluss der Gesellschaften an die Informations- und Kommunikationssysteme in sich birgt, erfolgt der Zugang über eine zentrale Schnittstelle (Firewall). Auf dieser Firewall sind verschiedene technische Sicherheitsmechanismen installiert.«
>
> Verlags- und Druckgewerbe, 090201/422/2009

- Sicherung gegen Abfluss/Diebstahl von Unternehmensdaten
  - Virtual Private Network (VPN)
  - Zertifizierung (Public Key Infrastructure)

– Verschlüsselung
– Zugangssicherung
– Fernzugriffsschutz
– Fernlöschen von Laptop-Daten.

»Der externe Zugriff auf Unternehmensdaten erfolgt ausschließlich über gesicherte Netzwerkverbindungen (z. B. VPN). Dabei ist der Arbeitnehmer verpflichtet, das IT-Equipment direkt über ein Netzwerkkabel an das Modem anzuschließen und WLAN (Wireless Local Area Network) zu vermeiden.«

Mess-, Steuer- und Regelungstechnik, 090300/212/2010

»Eine Verschlüsselung, z. B. gemäß dem Advanced Encryption Standard (AES) oder dem Data Encryption Standard (DES), ist sowohl auf dem Gerät als auch bei den Sicherungen des Gerätes anzuwenden. Sie wird durch das MDM-Provisioning-Zertifikat der betreffenden IT-Abteilung verwaltet.«

Chemische Industrie, 090202/190/2012

In jedem Einzelfall ist zu prüfen, welche Regelungstiefe anzustreben ist. Je genauer die technischen Sicherungsmaßnahmen in den Vereinbarungen aufgeführt sind, desto sicherer mag die IT-Landschaft des Unternehmens bzw. der Verwaltung gestaltet sein; Anpassungen im Zuge technischer Weiterentwicklungen erfordern dann jedoch, dass die Vereinbarung jeweils erneuert werden muss. Wichtig ist regelmäßig, dass den Arbeitnehmervertretungen und den Beschäftigten die Maßnahmen transparent gemacht werden, wie es die folgende Regelung vorsieht.

»Art und Zweck solcher Maßnahmen werden rechtzeitig betriebsintern veröffentlicht.«

Verbände und Gewerkschaften, 090300/273/2010

2.1.5 Systemadministration

Eine zentrale Rolle in Bezug auf die Risiken der Internetdienste und deren Abwehr kommt den Systemadministratoren zu, die die Informati-

onstechnik kontrollieren, steuern und verwalten und deswegen regelmäßig keinen oder nur wenigen Zugangs- und Zugriffsbeschränkungen unterliegen. Somit haben sie Zugriff auf Beschäftigtendaten, so dass die Vereinbarungen die Rechte und Pflichten der Administratoren beschreiben und begrenzen.
Die Systemadministration wird meist ausgeführt von einem bzw. mehreren Beschäftigten, ganzen Abteilungen oder sogar externen Personen und/oder Firmen, beispielsweise ehemaligen IT-Abteilungen, die outgesourct wurden. Die Vereinbarungen beschreiben diese Personen bzw. Gruppen meist in einer Anlage zur Vereinbarung, wobei teilweise sogar Namen genannt werden.

> »Für die Verwaltung der Netzwerke, E-Mail-, Intranet- und Internet-Systeme sind die vom Arbeitgeber zu benennenden Systemadministratoren (Anlage 5) zuständig. Jede personelle Änderung der Systemadministratoren muss dem Betriebsrat mitgeteilt werden.«
>
> Verlags- und Druckgewerbe, 090300/272/2005

§ 5 BDSG verlangt, dass die betreffenden Personen auf das Datengeheimnis verpflichtet werden: »Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.«
Regelmäßig wiederholen die Vereinbarungen die Verpflichtung, oft ergänzt um den Hinweis auf das Fernmeldegeheimnis gemäß § 88 Telekommunikationsgesetz (TKG): »Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.«
Die zuletzt zitierte Vereinbarung fordert zusätzlich die Vertrautheit mit den zu beachtenden rechtlichen Vorschriften.

> »Sie müssen mit den Bestimmungen des Fernmeldegeheimnisses im TKG (Telekommunikationsgesetz), der IuKD-Gesetzgebung (In-

formations- und Kommunikationsdienst-Gesetzgebung) und den entsprechenden europäischen Richtlinien und den Vorschriften des Bundesdatenschutzgesetzes vertraut sein und sind auf das Datengeheimnis gemäß § 5 BDSG zu verpflichten.«

Verlags- und Druckgewerbe, 090300/272/2005

Mit einer großen Regelungsdichte versuchen viele betriebliche Partner offenbar, einerseits die Gefahren so weit wie möglich abzuwenden, andererseits die Machtpotenziale, die sich bei den Administratoren konzentrieren, zu begrenzen. Dazu listen einige Vereinbarungen sehr genau auf, welche Aufgaben die Administratoren haben und zu welchen Zwecken sie Benutzeraktivitäten auswerten dürfen, die sie in Protokollen (vgl. Kap. 2.1.7) erkennen können. Dies zeigt ebenfalls an, dass die dazu grundlegende Bestimmung in § 31 BDSG betrieblich konkretisiert werden muss: »Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.«

»Diese Protokolle, die ausschließlich zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Informations- und Kommunikationssysteme, z. B.
- zur Analyse und Korrektur technischer Fehler,
- zur Gewährleistung der Systemsicherheit,
- zur Systemoptimierung, einschließlich Kapazitätsplanung,
- zur statistischen Feststellung der Nutzungsdauer und -häufigkeit und
- für Zwecke der Auswertungen nach den Vorgaben [...] dieser Vereinbarung (Missbrauchskontrolle)

laufend gespeichert werden, werden nur für diese Zwecke verwendet und nach drei Monaten automatisch gelöscht. Der Zugriff ist auf die mit der Netzwerkadministration für die Informations- und Kommunikationstechniken betrauten Personen begrenzt.«

Grundstücks- und Wohnungswesen, 090201/292/2006

Des Weiteren stellen einige Vereinbarungen die Administratoren unter die Kontrolle von betrieblichen Datenschutzbeauftragten und Betriebsräten.

> »Der betriebliche Datenschutzbeauftragte und der Betriebsrat werden beteiligt, wenn sie dies wünschen.«
>
> Ernährungsgewerbe, 090300/174/2008

2.1.6 Datenschutz(-Beauftragte)

Der Datenschutz ist ein zentraler Regelungsaspekt in allen Betriebs- und Dienstvereinbarungen zu Bereichen der Informations- und Kommunikationstechnik (IKT). Insbesondere IKT-Rahmenvereinbarungen enthalten regelmäßig umfassende Regelungen zum Datenschutz und zum betrieblichen Datenschutzbeauftragten (vgl. Böker/Demuth 2013).
Rund zehn Prozent der vorliegenden Dokumente sind IKT-Rahmenvereinbarungen, die auch Regelungen zu den Internetdiensten enthalten. Der Datenschutz ist dort in allgemeiner Form geregelt, das heißt: nicht speziell auf die Internet-, Intranet- und E-Mail-Nutzung bezogen. Die spezifischen Regelungen zum Datenschutz bei E-Mail und Internetdiensten werden in den Kapiteln 2.2 bis 2.4 dargestellt.

2.1.7 Protokollierungen

Alle Aktivitäten der Nutzerinnen und Nutzer von Internetdiensten werden automatisch in Protokolldateien aufgezeichnet. Ein Personenbezug und damit die Identifizierung eines bzw. einer Beschäftigten zu einem Protokolleintrag ergibt sich regelmäßig durch personalisierte E-Mail-Adressen, durch den Internetzugang nach Eingabe einer Benutzerkennung, durch eindeutige Zuordnung von Bildschirmarbeitsplätzen zu Mitarbeitern etc. Die Protokollierung ist in den meisten Standardprogrammen, die für Internetzugang, E-Mail-Kommunikation und Intranetnutzung verwendet werden, vorgesehen. Oft bestehen nur wenige Möglichkeiten, sie abzuschalten oder vom Umfang her einzuschränken.

Die Aufzeichnung personenbezogener Daten in Logdateien akzeptieren die Betriebspartner regelmäßig, nicht jedoch den uneingeschränkten Zugriff auf die Protokolldateien, wie das folgende Beispiel zeigt.

> »Die Erfassung der bei der Nutzung der Internet- und E-Mail-Dienste anfallenden personenbezogenen Daten ist zulässig. [...] Eine stichprobenartige Missbrauchskontrolle der Verbindungsdaten ist nur auf Anweisung eines Vorstandsmitglieds zulässig.«
>
> Grundstücks- und Wohnungswesen, 090300/184/2010

Der freizügigen Einsichtnahme und Auswertung dieser Protokolldateien schieben die meisten Vereinbarungen einen Riegel vor. Sie begrenzen den zugriffsberechtigten Personenkreis und den Umfang der personenbezogenen oder -beziehbaren Auswertungen. Als Begründung dient regelmäßig der gemäß § 28 BDSG zu benennende Zweck der Datenauswertung. Für diese Art von Daten/Dateien sehen die Datenschutzgesetze einen besonderen Schutz vor, beispielsweise folgenden: »Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.« (§ 31 BDSG) Die betrieblichen Verhandlungspartner sehen es gelegentlich als notwendig an, diese Bestimmung zu konkretisieren. Sehr unterschiedlich ausführlich regeln sie die Details, indem sie die zu protokollierenden Daten und die Zwecke des Protokollierens benennen. Die folgende Regelung belässt es jedoch bei einem Hinweis auf das Datenschutzgesetz.

> »Personenbezogene Daten (im Sinne des Bundesdatenschutzgesetzes, BDSG), die zur Sicherstellung eines ordnungsgemäßen Betriebs der E-Mail- und Internet-Dienste erhoben und gespeichert werden, unterliegen der besonderen Zweckbindung nach § 31 Bundesdatenschutzgesetz und dürfen deshalb nicht für andere Zwecke, insbesondere auch nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.«
>
> Grosshandel (ohne Kfz.), 090300/159/2009

Mehrere Vereinbarungen beschreiben den Umfang der Protokollierung, wie das folgende Beispiel zeigt. Dies dient u. a. der Transparenz (vgl. Kap. 2.1.1).

»Die Protokollierung der Firewall wird zur Auswertung der Internetzugriffe von außen und innen benutzt.
Die Protokollierung von Proxyservern dient zur Auswertung der Internetzugriffe.
Die Firewall-Protokolle enthalten pro Ereignis:
– Datum,
– Zeit,
– Hardwareanschluss,
– Aktion der Firewall,
dazu
– Datenweiterleitung, -stopp
– Fehlererkennung,
– Datenverschlüsselung,
– Authentifizierung erfolgreich/nicht erfolgreich,
– Absender- und Zieladresse,
– Übertragungsprotokoll,
– Nutzername.
Die Proxy-Protokolle enthalten:
– Datum,
– Zeit,
– IP-Adresse [→ Glossar] vom Proxy,
– IP-Adresse vom PC,
– Benutzeranmeldename,
– Ziel-Adresse (URL),
– Protokoll-Status,
– Größe.«

Baugewerbe, 090300/187/2008

Ausführlich beschreibt die folgende Regelung die Zwecke, zu denen die Protokolldaten ausgewertet werden dürfen.

»Die Protokolle [...] werden ausschließlich zu Zwecken der
– Analyse und Korrektur technischer Fehler,

– Gewährleistung der Systemsicherheit,
– Optimierung des Netzes,
– statistischen Feststellung des Gesamtnutzungsvolumens,
– Stichprobenkontrollen [...],
– Auswertungen [...] (Missbrauchskontrolle)
verwendet.«

Gesundheit und Soziales, 090201/400/2010

Die meisten der vorliegenden Betriebs- und Dienstvereinbarungen, Richtlinien und Dienstanweisungen bleiben dahinter zurück: Sie regeln dies oberflächlich und interpretierbar.
Des Weiteren werden Prozesse bzw. Verfahren festgelegt, nach denen in bestimmten, klar umrissenen Verdachtssituationen Protokolle ausgewertet werden können.

»Die Internet-, Mailnutzung unterliegt einer automatischen Protokollierung. Die Protokolldaten werden für zwei Monate aufbewahrt und können im Rahmen einer Revision oder im Fall eines Verdachts auf einen Sicherheitsverstoß durch autorisierte Personen ausgewertet werden.
Dieser Personenkreis setzt sich wie folgt zusammen:
– Arbeitgebervertreter: 1 Person
– Betriebsratsmitglied: 2 Personen
– Datenschutzbeauftragter: 1 Person
Im Falle des begründeten Missbrauchsverdachts wird der Benutzer auf diesen Verdacht hingewiesen und zu einer Erklärung aufgefordert. Wird dabei kein zufriedenstellendes Ergebnis erreicht, so können die Systemprotokolle eingesehen werden. Zu diesem Zweck wird eine Berechtigung geschaffen, die unter Eingabe der Benutzer- oder Geräteidentifizierung die Protokolldatensätze für den ausgewählten Zeitraum anzeigt. Nachgewiesener Missbrauch kann arbeits- und/oder strafrechtliche Konsequenzen zur Folge haben.«

Gummi- und Kunststoffherstellung, 090300/178/2009

Zusätzliche Regelungen zur maximalen Aufbewahrungszeit von Protokolldaten sind eine weitere Möglichkeit, die Auswertungen zu begrenzen (vgl. Kap. 2.1.8).

Als spezielles Problemfeld benennt eine Betriebsvereinbarung den Umgang mit Protokolldaten, wenn die Datenverarbeitung von externen Dienstleistern durchgeführt wird.

> »Die Zurverfügungstellung der IT-Systeme erfolgt durch [externe Dienstleister]. Sämtliche Protokollierungen und Speicherungen erfolgen auch an deren Sitz [Ort] und/oder in [...]-Niederlassungen in der EU.
> Wenn Mitarbeiter sich entscheiden, einen Proxyserver zu nutzen, der sich außerhalb der USA und der EU befindet, kann die Protokollierung auch außerhalb dieser Gebiete stattfinden.«
>
> Datenverarbeitung u. Softwareentwicklung, 090300/242/0

Überzeugend ist diese Regelung nicht, da sie den Beschäftigten keinen Schutz bietet. Vermutlich haben sie keinen Einfluss darauf, welchen Server sie verwenden. Weitere Beispiele liegen uns nicht vor; dies deutet darauf hin, dass hier Unsicherheiten zu Form und Inhalt von Regelungen bestehen (vgl. Kap. 4).

2.1.8 Aufbewahrungsfristen

Das BDSG schreibt vor, dass gespeicherte personenbezogene und personenbeziehbare Daten zu löschen sind, wenn sie zu keinem Zweck mehr benötigt werden. Dies gilt auch für Protokolle der Internet- und E-Mail-Nutzung. Einige Vereinbarungen wiederholen den Gesetzestext, teilweise einleitend zu konkreteren Regeln, teilweise aber auch ohne weitere Konkretisierungen, wie das folgende Beispiel zeigt.

> »Die entsprechenden Daten sind unverzüglich zu löschen, soweit sie für diese Zwecke nicht mehr benötigt werden.«
>
> Verlags- und Druckgewerbe, 090300/196/2010

In der betrieblichen Praxis ist offenbar schwer zu entscheiden, wann Daten tatsächlich nicht mehr benötigt werden. Als Lösung wählen die betrieblichen Partner gern Regelungen zu zeitlich bestimmten Aufbewahrungs- oder Löschfristen. Hierbei gehen die Meinungen jedoch weit

auseinander, so dass Fristen von wenigen Tagen bis zu einem halben Jahr oder länger vereinbart sind.

> »Im laufenden Betrieb des [...]-Systems werden Log-Dateien mit personenbezogenen Daten erzeugt, die ausschließlich im Falle von Störungen zur Fehleranalyse durch die Systemadministration herangezogen werden. Diese werden täglich rotiert und nach maximal 10 Werktagen automatisch gelöscht.«
>
> Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/231/2010

Gelegentlich ist in den Vereinbarungen ein allgemeiner Verweis auf gesetzliche Vorschriften zu lesen, die angeblich eine bestimmte Aufbewahrungsdauer verlangen. Dies läuft regelmäßig ins Leere, da in der betrieblichen Praxis genaue Angaben aus Gesetzen weitgehend unbekannt sind.
Ausnahmen von den vereinbarten Löschfristen – das heißt: eine längere Aufbewahrungsdauer der Daten – erlauben Vereinbarungen meist, wenn ein Missbrauch der Internetdienste festgestellt wird oder ein entsprechender Verdacht besteht. Das folgende Beispiel wurde bereits in der letzten, zweiten Auflage dieser Auswertung (2008) zitiert; eine entsprechend interessante Regelung ist in den aktuell vorliegenden Vereinbarungen nicht enthalten.

> »Sämtliche im Rahmen der Systemprotokollierung gespeicherten Daten werden automatisch nach fünf Werktagen gelöscht. Eine Ausnahme von der Löschfrist gilt dann, wenn Fehler aufgetreten sind, bei deren Ursachensuche bzw. Auswertung und Behebung die protokollierten Daten notwendig sind. Die Löschung der Protokolle ist zu dokumentieren, so dass Abweichungen nachvollziehbar sind.«
>
> Versicherungsgewerbe, 090300/81/2001

Diese Regelung bildet in mehrfacher Hinsicht eine positive Ausnahme: a) Die Löschfrist von fünf Werktagen ist im Vergleich zu vielen anderen Vereinbarungen sehr kurz. b) Die Ausnahme wird auf Fehler, nicht auf Missbrauchsverdacht bezogen. c) Die Dokumentation schafft Transparenz für Arbeitnehmervertreter und Beschäftigte.

Leider finden sich auch negative Ausnahmen: Beispielsweise ist eine Aufbewahrungsfrist von »mindestens 6 Monaten« keine wirkliche Grenze und ermöglicht ebenso eine grenzenlose Aufbewahrung wie eine Regelung, nach der die Protokolldaten zehn Jahre aufbewahrt werden sollen. Diese Regelung wäre unwirksam, weil gesetzliche Bestimmungen durch betriebliche Vereinbarungen nicht unterlaufen werden dürfen, sofern die Gesetze keine entsprechende Öffnungsklausel enthalten.

2.1.9 Leistungs- und Verhaltenskontrolle

Rund die Hälfte der vorliegenden Vereinbarungen enthalten Regelungen zum Thema Leistungs- und Verhaltenskontrolle. Um Beschäftigte in diesem Sinne zu überwachen, eignen sich insbesondere die von den Systemen zur E-Mail-Kommunikation und zur Internetnutzung gespeicherten Protokolle. Darin sind sämtliche Aktivitäten der Beschäftigten sekundengenau und vollständig aufgezeichnet. Die folgende Vereinbarung definiert genau, welche Daten zur Überwachung geeignet sind und beschränkt dies nicht nur auf Protokolldaten.

> »Unter Daten über das Verhalten oder die Leistung von Beschäftigten werden alle Informationen verstanden, die Aussagen darüber erlauben, was Beschäftigte zu einem bestimmten oder unbestimmten Zeitpunkt getan oder unterlassen haben.«
>
> Gummi- und Kunststoffherstellung, 090201/463/2010

Die meisten, aber längst nicht alle Regelungen verbieten die Nutzung der Daten für eine Leistungs- und Verhaltenskontrolle.

> »Die bei der Nutzung der Internetdienste anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle erhoben, verarbeitet oder genutzt. Die protokollierten Daten unterliegen der Zweckbindung dieser Betriebsvereinbarung und den einschlägigen Datenschutzbestimmungen.«
>
> Verlags- und Druckgewerbe, 090300/226/2011

Die »Zweckbindung dieser Betriebsvereinbarung« ist möglicherweise eine Öffnungsklausel, die in bestimmten Fällen, welche in der Vereinbarung geregelt sind, eine Auswertung zulässt. Ebenso formulieren es mehrere Vereinbarungen, die ein »grundsätzliches« Verbot enthalten.

> »Eine Leistungs- und Verhaltenskontrolle findet grundsätzlich nicht statt. Ausnahmen bedürfen der vorherigen Genehmigung des Betriebsrats und des betrieblichen Datenschutzbeauftragten.«
>
> Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/231/2010

»Grundsätzlich« bedeutet im juristischen Sinne, dass es Ausnahmen geben kann, die hier im zweiten Satz genannt werden. Typisch für Vereinbarungen und Richtlinien zu E-Mail- und Internetdiensten ist, dass Protokolle meist zum Auffinden von Missbrauchsfällen personenbezogen ausgewertet werden dürfen (vgl. Kap. 2.1.10).
Gelegentlich werden die Bedingungen, unter denen personenbezogene Auswertungen erlaubt sind, detaillierter beschrieben und eingegrenzt. Dies war bereits im letzten Textauszug erkennbar und wird besonders genau in folgender Vereinbarung geregelt.

> »Die Einsicht und die Bewertung eines erstellten Internetnutzerprotokolls mit der Absicht, das Verhalten eines Mitarbeiters zu kontrollieren, zu bewerten oder zu beweisen, darf nur auf besonderen Antrag an den CSO [Chief Security Officer] unter Einbeziehung des lokalen Betriebsrats sowie des zuständigen bDSB [betrieblichen Datenschutzbeauftragten] und nur bei erheblichem, begründetem Verdacht eines Fehlverhaltens oder einer möglichen Schädigung des Firmennetzwerks erfolgen.«
>
> Branchenübergreifend, 090300/189/2010

Für die Arbeitnehmervertretung dürfte es allerdings problematisch sein zu überprüfen, ob die Regelungen eingehalten werden. Während die meisten Vereinbarungen zur Kontrollierbarkeit keine Aussagen enthalten, zeigt das folgende Beispiel, dass man sich zumindest Gedanken dazu gemacht hat.

»Jegliches Öffnen von E-Mail-Konten durch den Systemadministrator wird mit Datum und Uhrzeit in einer Datenbank protokolliert. Diese Protokolldaten werden aufbewahrt, bis die Speichergrenze der Datenbank erreicht ist. Sodann werden die ältesten Protokolldaten von den neuesten überschrieben. Je nach Häufigkeit der Zugriffe auf das jeweilige E-Mail-Konto ist ein Rückblick von mindestens zwei Jahren möglich.«

Maschinenbau, 090201/511/2011

Eine der vorliegenden Vereinbarungen sieht eine Stufenregelung vor: Sie erlaubt die Einsicht in Protokolldaten nur in einem festgelegten Verfahren und mit Zustimmung einer paritätisch besetzten Kommission, die aus drei Arbeitgeber- und drei Arbeitnehmervertretern sowie dem unparteiischen Datenschutzbeauftragten besteht.

»Die paritätische [...]-Kommission hat folgende Aufgaben:
a. Sichtung und Auswertung der anonymen Kontrolldaten [...]
b. Feststellen eines besonderen Ereignisses nach § [...]
c. Entscheidung über Stichprobenkontrollen und Umfang sowie Auswertung gem. [...]
d. Entscheidung über Heranziehung und Auswertung der Kontrolldaten und ggf. Inhaltsdaten im Rahmen der Missbrauchsregelung gem. [...].«

Landverkehr, 090300/322/2012

Eine weitere Besonderheit in dieser Regelung ist die Organisation der Systemadministration (vgl. Kap. 2.1.5). Sie ist in zwei personell wie organisatorisch voneinander getrennte Bereiche gegliedert. So hat der für die Betriebsdaten zuständige Systemadministrator nichts mit den Kontrolldaten zu tun, die herangezogen werden, wenn Auffälligkeiten analysiert werden sollen.

2.1.10 Sanktionen/Maßnahmen bei Missbrauch bzw. Missbrauchsverdacht

Betriebs- und Dienstvereinbarungen zu E-Mail und Internetdiensten erlauben regelmäßig, in Einzelfällen und bei begründetem Verdacht auf missbräuchliche Nutzung Protokolldaten, E-Mail-Postfächer oder andere Speicherbereiche in Computersystemen personenbezogen auszuwerten. Eine derartige Regelung, die das Verbot von Leistungs- und Verhaltenskontrolle relativiert, findet sich in beinahe jeder Vereinbarung. Doch die Formulierungen sind sehr unterschiedlich (vgl. Kap. 2.1.9).
Sehr detailliert und restriktiv beschreibt die folgende Konzernbetriebsvereinbarung (KBV), welche Personen unter welchen Bedingungen welche Datenbereiche auswerten dürfen.

> »Bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte für einen schwerwiegenden Missbrauch durch schwerwiegendes vertragswidriges Verhalten oder erhebliche Verstöße gegen diese KBV oder relevante Richtlinien, können nur nach Zustimmung der paritätischen KBV IT-Kommission Kontrolldaten herangezogen und ausgewertet werden. Sofern zur Aufklärung dieser Handlungen die Verarbeitung personenbezogener Daten erforderlich ist, ist vor Heranziehung und Auswertung von Kontrolldaten eine Verhältnismäßigkeitsprüfung nach dem Prozess zur doppelten Verhältnismäßigkeitsprüfung [...] durchzuführen.«
>
> Landverkehr, 090300/322/2012

Neben den hier genannten Beteiligten sehen andere Vereinbarungen insbesondere vor, dass der bzw. die betroffene Beschäftigte sowie die Arbeitnehmervertretung über einen Verdacht und vor einer Auswertung informiert werden müssen. Meist sind Betriebs- bzw. Personalrat auch am weiteren Verfahren zu beteiligen.

> »Bei Verdacht einer missbräuchlichen Nutzung informiert [die Firma] den zuständigen Betriebsrat schriftlich unter Darlegung der Verdachtsgründe. Über das weitere Vorgehen ist Einvernehmen mit dem zuständigen Betriebsrat zu erzielen. Eine eventuelle Untersuchung unter Auswertung der entsprechenden Protokolldaten darf

sich nur auf die im Schreiben an den Betriebsrat dargelegten Verdachtsmomente beziehen.«

Unternehmensbezogene Dienstleistungen, 090201/445/2008

Das Verfahren beschreiben die Vereinbarungen ebenfalls sehr unterschiedlich differenziert. Einige juristisch gut ausformulierte und praxisgerechte Regelungen sind auf der beigefügten CD-ROM und in der Online-Datenbank der Hans-Böckler-Stiftung dokumentiert (www.boeckler.de/betriebsvereinbarungen).
Bestätigt die Auswertung personenbezogener Daten einen Verdacht, dann erlauben die Vereinbarungen unterschiedlichste rechtliche Konsequenzen – bis hin zur Androhung einer fristlosen Kündigung der bzw. des Betroffenen. Sofern die private Nutzung von E-Mail und Internetdiensten akzeptiert oder zugelassen ist, wird als Bestrafung auch gelegentlich der Entzug dieser Rechte angedroht. Ein vollständiges Verbot der Internetnutzung, wie es einige wenige Vereinbarungen vorsehen, dürfte hingegen im heutigen Arbeitsleben nicht realisierbar sein.

»Ein Verstoß gegen diese Dienstvereinbarung kann neben arbeitsrechtlichen Folgen, insbesondere Abmahnung und Kündigung, auch haftungsrechtliche und strafrechtliche Konsequenzen haben.
Die [Firma] behält sich außerdem vor, nach Anhörung des Gesamtpersonalrats bei Verstößen gegen diese Dienstvereinbarung die Nutzung ihrer Internet- und E-Mail-Dienste für den privaten Gebrauch im Einzelfall einzuschränken oder zu untersagen.«

Kreditgewerbe, 090300/182/2008

Missbräuchlich gewonnene Daten dürfen in der Regel nicht für weitere Zwecke verwendet werden, insbesondere nicht für personelle Maßnahmen. Dies gilt auch dann, wenn ein Verdacht durch Prüfung der Datenlage nicht bestätigt wurde.

»Beweisverwertungsverbot
Die Verwendung von Tatsachen, die aufgrund einer unzulässigen Datenauswertung gewonnen werden, ist unzulässig. Der Arbeitgeber darf auf solche Tatsachen keine personellen Maßnahmen stützen, die zu einer Veränderung der Beschäftigungsbedingungen, zu

Beendigung des Arbeitsverhältnisses oder zu Er- oder Abmahnungen oder sonstigen Sanktionen gegenüber dem Beschäftigten führen. Der Arbeitgeber ist verpflichtet, eine derartige personelle Maßnahme zurückzunehmen und keinerlei Rechte aus dieser herzuleiten.«

Landverkehr, 090300/322/2012

2.1.11 Kostenregelungen

Die Kosten der Internetnutzung thematisieren nur wenige Vereinbarungen. Selten geschieht dies mit dem Hinweis, dass Protokolle ausgewertet werden müssen, um die Kosten den Kostenstellen zuordnen zu können (vgl. Kap. 2.1.7).

»Zu Zwecken der internen Kostenverrechnung werden die Protokolldaten zu monatlichen Summensätzen pro Kostenstelle verdichtet.«

Anonym, 090300/149/0

Häufiger ist die zulässige private Nutzung der Internetdienste ein Anlass dafür, Kostenregelungen zu formulieren. Die meisten Vereinbarungen bestimmen, dass die private Nutzung keine besondere Kostenbelastung verursachen darf, z. B. durch umfangreiche Downloads oder durch Einkäufe im Internet.

»Durch die private Nutzung des Internets dürfen [...] keine weiteren Kosten entstehen. Im Rahmen der privaten Nutzung des Internets dürfen keine kommerziellen Zwecke verfolgt werden.«

Elektro, 090300/185/2010

Dass es auch anders geht, zeigt die folgende Regelung in einem Unternehmen des Finanzsektors, das insgesamt sehr freizügig mit der (privaten) Internetnutzung verfährt.

»Die Kosten für die private Nutzung trägt die [Firma].«

Kreditgewerbe, 090300/136/2007

Abschließend sei erwähnt, dass einige Vereinbarungen die Beschäftigten dazu anhalten, die Internetdienste »kostenbewusst und ressourcenschonend« zu nutzen. Wie dies in der Praxis, wo den meisten Beschäftigten die Kostenstrukturen vermutlich nicht bekannt sind, umzusetzen ist, wird allerdings nicht näher ausgeführt.

2.1.12 Private Nutzung

Das zentrale Regelungsthema in rund zwei Drittel der vorliegenden Betriebs- und Dienstvereinbarungen ist die private Nutzung betrieblicher Internetdienste. Die Spannbreite der Regelungen reicht vom vollständigen, ausnahmslosen Verbot bis hin zur betrieblichen Förderung der privaten Nutzung. Ein Trend in die eine oder andere Richtung ist schwer zu erkennen.
Die Privatnutzung während der Arbeitszeit erlauben die aktuell ausgewerteten Vereinbarungen zu rund 70 Prozent. Dies ist ein leichter Rückgang gegenüber der Auswertung aus dem Jahr 2008 (vgl. dort Kap. 2.1.12, Seite 41). Regelungen, die die private Nutzung betrieblicher Internetdienste ausschließlich in der Freizeit und in den Pausenzeiten erlauben, sind häufiger zu finden als in der früheren Auswertung. Einige Vereinbarungen grenzen die berufliche Nutzung der Internetdienste von der privaten Nutzung ab. Sie definieren eine dienstliche Nutzung in erweiterter Form, wie etwa folgende Formulierung.

> »Elektronische Kommunikationssysteme sind grundsätzlich für den dienstlichen Zweck bestimmt. Dazu zählen auch mit dem dienstlichen Zweck in einem sachlogischen Zusammenhang stehende Nutzungen wie zum Beispiel Informationen über aktuelle Nachrichten, Politik, Geschichte, Kultur des Reiselandes oder über die Wetter- und Verkehrslage.«
>
> Anonym, 090300/193/0

Nicht eindeutig zuzuordnende Nutzungsformen werden dadurch als »dienstlich« bezeichnet und somit zulässig. Die folgende Dienstvereinbarung erlaubt zusätzlich den Zugriff auf Internetseiten mit Bezug zur Interessenvertretung und zum Arbeitsrecht.

»Der Internet-Zugang aller Beschäftigten umfasst auch den Zugriff auf Gewerkschaftsseiten und auf andere Informationen über Rechte am Arbeitsplatz.«

Öffentliche Verwaltung, 090300/293/2012

Nachrichten an die Familie über kurzfristig notwendige Arbeitszeitverlängerungen oder »sonstige Kurzinformationen« dürfen gelegentlich per E-Mail (oder SMS) versandt werden und stellen ebenfalls keine private Nutzung dar. Allgemeiner formulieren es drei Vereinbarungen, die die »Dringlichkeit einer Angelegenheit, die keinen Aufschub in die Freizeit gestattet« oder die »Vereinbarkeit von Familie und Beruf« als Erlaubnisgrund nennen.
Andere Vereinbarungen definieren in gleichem Sinn den Begriff Privatnutzung. Diese liegt beispielsweise vor, wenn die Nutzung nicht der Erledigung und der Organisation von Arbeitsaufgaben, sondern überwiegend persönlichen Interessen dient, wie in folgender Dienstvereinbarung.

»Private Nutzung von Internet und E-Mail liegt dann vor, wenn sie zum jeweiligen konkreten Aufgabenbereich des Beschäftigten keinen Bezug aufweist.«

Öffentliche Verwaltung, 090300/151/2008

Aufwändiger und mit konkreten Beispielen ausformuliert ist die folgende Definition von privater Nutzung in einer Betriebsvereinbarung.

»Die private Nutzung der informationstechnischen Arbeitsmittel, insbesondere des Internetzuganges, der elektronischen Kommunikationssysteme und der informationstechnischen Speicherkapazitäten der [Firma] ist nicht zulässig.
Eine private Nutzung liegt insbesondere dann vor, wenn
– für die betreffenden Daten, Kommunikationsinhalte, Verbindungen oder Kontaktpartner ein Vertraulichkeitsanspruch gegenüber dem Arbeitgeber und seinen Beschäftigten erhoben wird;
– außerbetriebliche Rechtsgeschäfte abgewickelt werden; dazu zählen insbesondere Einkäufe, Verkäufe, Teilnahmen an Auktionen

und Tauschbörsen, der Abruf kostenpflichtiger Seiten, Bankgeschäfte, Börsengeschäfte und sonstige Geschäfte, die nicht betrieblich veranlasst sind;
– Dateien, insbesondere Programm-, Text-, Audio-, Bild- oder Videodateien, zu anderen als zu betrieblichen Zwecken heruntergeladen oder gespeichert werden;
– eine Teilnahme an öffentlichen Kommunikationsplattformen (z. B. Foren, Blogs, Chaträume) zu anderen als zu betrieblichen Zwecken erfolgt.«

Verbände und Gewerkschaften, 090300/273/2010

Zwei der vorliegenden Vereinbarungen stellen klar, dass eine Grenzziehung zwischen dienstlicher und privater Nutzung schwierig und vor allem interpretationsbedürftig ist. Daraus leiten die Betriebsparteien folgende Regelung ab.

»Daher wird die [Firma] eine nicht eindeutig als dienstliche Verwendung qualifizierte Nutzung von Internet-Zugang und Mail-System dann nicht als missbräuchlich ansehen, wenn sie geringfügigen Umfangs ist und die Arbeitsabläufe nicht beeinträchtigt sowie nicht mit der Verursachung zusätzlicher Kosten aufgrund zusätzlicher Ressourcenbelastung des Netzes verbunden ist.«

Bildungseinrichtung, 090300/154/2006

Ein »Recht auf Irrtum« wird den Beschäftigten nur in seltenen Fällen ausdrücklich zugebilligt.

»Keine private Nutzung bzw. Verstoß liegt vor, wenn jemand bei einer dienstlichen Recherche etwa aufgrund unzulänglicher Benutzung einer Suchmaschine auf die falschen Seiten gerät.«

Versicherungsgewerbe, 090300/206/2007

Die rechtlichen Grundlagen sind ausführlich in Kapitel 6.3 dargestellt. Die Vereinbarungen, die für diese Auswertung vorliegen, orientieren sich jedoch nur teilweise an dem im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG) formulierten geltenden Recht. Da das Thema Privatnutzung in den Vereinbarungen eine herausragende Rolle

einnimmt, wird die Auswertung im Folgenden besonders ausführlich dargestellt.

Die ausschließliche Nutzung von Internetdiensten zu betrieblichen bzw. dienstlichen Zwecken, verbunden mit dem Verbot einer privaten Nutzung, formulieren rund 14 Vereinbarungen. Weitaus mehr Vereinbarungen schränken eine private Nutzung auf die Freizeit ein, das heißt: Vor und nach der Arbeitszeit und während der Pausen ist die private Nutzung von Internetdiensten erlaubt bzw. akzeptiert; dazu liegen rund 25 Vereinbarungen vor. Ein »grundsätzliches Verbot« sprechen rund 16 Vereinbarungen aus; dabei ist zu berücksichtigen, dass im juristischen Sinne der Begriff »grundsätzlich« so zu verstehen ist, dass Ausnahmen zugelassen sind, während im alltäglichen Sprachgebrauch damit oft eine strikte Einhaltung formuliert wird. Man weiß demnach nicht, wie die betrieblichen Partner diese Regelung verstanden wissen wollen. Nicht von Verbot, sondern von Zulässigkeit sprechen ca. 30 Vereinbarungen, die jedoch Bedingungen formulieren oder zumindest den zeitlichen Umfang der privaten Nutzung von Internetdiensten durch Begriffe wie »angemessen«, »geringfügig«, »unerheblich« oder »gelegentlich« einzuschränken versuchen. Laut Polenz/Thomsen (2010) sei allerdings zu beachten, »dass solche unbestimmten Vorgaben bei der Festlegung der erforderlichen Kontrollen und insbesondere für Fälle, in denen arbeitsrechtliche Konsequenzen bei Verstößen erfolgen sollen, klarer definiert werden müssen«. Nur vier der vorliegenden Vereinbarungen wollen die Privatnutzung unterstützen, um damit beispielsweise den Umgang der Beschäftigten mit diesen Medien zu fördern.

Als Bedingungen für eine zugelassene Privatnutzung formulieren die Betriebsparteien ganz unterschiedliche Aspekte. Am häufigsten ist genannt, dass nicht gegen geltendes Recht verstoßen werden darf und dass keine kostenpflichtigen Downloads vorgenommen sowie keine kommerziellen oder sonstigen geschäftlichen Zwecke verfolgt werden dürfen. Ebenso wichtig ist den Betriebsparteien, dass private Interessen den Belangen der Firma unterzuordnen sind, so dass Arbeitsabläufe nicht beeinträchtigt werden. Sechs Vereinbarungen legen einen Zeitrahmen fest, der für die private Nutzung von Internetdiensten während der Arbeitszeit nicht überschritten werden darf. Dieser Zeitraum muss von »untergeordneter Bedeutung« sein oder er reicht von fünf Minuten pro Tag über eine Stunde pro Woche bis zu acht Stunden pro

Monat (»Bei Teilzeitbeschäftigten ist diese Zeit entsprechend anzupassen.«).
Nur wenige Vereinbarungen regeln, dass eine private Nutzung von E-Mail oder Internet nicht als Arbeitszeit zu werten und deswegen »auszustempeln« ist, oder dass »die notwendige Erholung in den Pausen nicht leiden darf«.
Formell machen relativ viele Vereinbarungen die Privatnutzung davon abhängig, ob die Beschäftigten eine Einwilligungs- bzw. Verpflichtungserklärung unterzeichnet haben. Mit dieser Erklärung akzeptieren sie in der Regel die genannten oder zusätzlichen Bedingungen und stimmen einer Protokollierung und möglichen Kontrollen der Verbindungsdaten inklusive der persönlichen Daten zu (Details zu den Einwilligungserklärungen vgl. Kap. 2.1.13).
Einige Vereinbarungen sehen Sanktionen des Arbeitgebers bei Verstoß gegen die Bedingungen der privaten Nutzung vor. Dies sind meist arbeitsrechtliche, gelegentlich auch strafrechtliche Maßnahmen, beispielsweise wie folgt formuliert: »Die [Firma] behält sich vor, bei Verstößen gegen diese Bedingungen die private Nutzung des Internetzugangs im Einzelfall zu untersagen.« (Näheres zu Sanktionen vgl. Kap. 2.1.10)
In vielen Fällen sichert sich der Arbeitgeber die Möglichkeit, die zugelassene private Nutzung allen Beschäftigten wieder entziehen zu können.

> »Die Gewährung der privaten Nutzung der Kommunikationsdienste (E-Mail/Internet) erfolgt freiwillig. Die Gewährung steht im freien Ermessen des Arbeitgebers. Auch bei wiederholter vorbehaltloser Gewährung der Privatnutzung entsteht kein Rechtsanspruch auf Gewährung für die Zukunft.«
>
> Wasserversorger, 090300/176/2010

Relativ neu ist die »Privatnutzung« in der Form, dass Beschäftigte ihre private IT-Ausstattung in den Betrieb mitbringen und während der Arbeitszeit für die Erledigung von Arbeitsaufgaben nutzen. Dieses Konzept, benannt »Bring Your Own Device« (BYOD, → Glossar), wird von Arbeitgebern laut einer Studie des IT-Branchenverbandes BITKOM überwiegend positiv beurteilt (Bitkom 2013). Die vorliegenden Vereinbarungen vermitteln ein anderes Bild: Nur in rund zehn Prozent der Vereinbarungen wird dieses Thema aufgegriffen und dies zu mehr als

80 Prozent ablehnend. Der Rest erlaubt die dienstliche Nutzung von Privatgeräten nur im Einzelfall und nach entsprechender Prüfung. Die folgende Dienstvereinbarung nennt einen speziellen Fall der Erlaubnis.

> »Eventuelle Ausnahmen können nach Prüfung durch das IT-Referat gestattet werden. Dies gilt insbesondere für technische Hilfsmittel für schwerbehinderte Beschäftigte.«
>
> Öffentliche Verwaltung, 090201/433/2006

2.1.13 Einwilligungserklärungen

Zunehmend scheint sich durchzusetzen, dass die Beschäftigten eine Einwilligungs- und Verpflichtungserklärung zur E-Mail- und Internetnutzung unterzeichnen müssen, bevor ihnen die private Nutzung erlaubt wird. Diese Annahme beruht auf der relativ großen Anzahl von Erklärungen, die den Vereinbarungen als Anlage beigefügt sind. Die rund 30 vorliegenden Dokumente fallen höchst unterschiedlich aus. Ausführliche Analysen führten zu den im Folgenden dargelegten Erkenntnissen.
Die Erklärungen entsprechen inhaltlich meistens dem folgenden Beispieltext, der vergleichsweise knapp gefasst ist.

> »Einwilligungserklärung der/des Beschäftigten
> Einwilligungserklärung in Bezug auf die Internet-Nutzung
> In Bezug auf die private Nutzung des Internets der [Firma] willige ich in die Protokollierung und Kontrolle der Internet-Nutzung ein, wie diese in §§ [...] der Betriebsvereinbarung Internet geregelt sind. Des Weiteren stimme ich einer automatisierten Kontrolle der abgerufenen Inhalte zu und erhebe keinen Anspruch auf ständige Verfügbarkeit der Internetverbindung.
> Mir ist bekannt, dass ich diese Einwilligungserklärung jederzeit widerrufen kann. In diesem Fall ist mir die Nutzung des Internets für dienstliche Zwecke gestattet.
> Mir ist ebenfalls bekannt, dass ohne unterschriebene und an die Personalabteilung übersandte Einwilligungserklärung nur die dienstliche Nutzung des Internets gestattet ist.

[Ort, den]
Betrieb: [...]
Name, Vorname (in Druckbuchstaben): [...]
Geburtsdatum: [...]
Unterschrift [...].«

Gesundheit und Soziales, 090300/167/2010

Mehrere Beispiele der meist sehr viel ausführlicher formulierten Erklärungen stehen auf der CD-ROM und in der Online-Datenbank zur Verfügung.

Die Form der Erklärungen

Jeder Beschäftigte, der den betrieblichen Internetzugang zu privaten Zwecken nutzen möchte, unterzeichnet die Erklärung. Verweigert er dies oder widerruft er seine Unterschrift zu einem späteren Zeitpunkt, wird ihm die private Nutzung untersagt. Die unterzeichneten Erklärungen werden regelmäßig zu den Personalakten genommen. Aus der Weigerung oder dem Widerruf entsteht dem Beschäftigten kein Nachteil, wie einige Erklärungen beteuern.
Die wesentlichen Inhalte der Einwilligungs- und Verpflichtungserklärungen sind:

Widerruf

- Arbeitgeber bestehen gelegentlich darauf, dass die Gewährung des privaten Internetzugangs nur freiwillig besteht und jederzeit ohne Angabe von Gründen widerrufen werden kann. Damit sichern sie sich gegen das Argument der »betrieblichen Übung« ab, mit dem bereits in juristischen Auseinandersetzungen ein Widerrufen der Privatnutzung der betrieblichen Internetdienste gerichtlich abgewiesen wurde.
- Ebenso oft wird den Beschäftigten das Recht eingeräumt, eine einmal unterzeichnete Erklärung jederzeit und ohne Angabe von Gründen zu widerrufen. Diese Erlaubnis ist regelmäßig mit dem Hinweis verbunden, dass mit dem Widerruf die Erlaubnis zur Privatnutzung sofort erlischt.

Einschränkungen

- Die Erlaubnis wird gelegentlich mit der Einschränkung verknüpft, dass der dienstliche Internetzugang nur in geringem Umfang, vornehmlich oder ausschließlich in den Arbeitspausen bzw. außerhalb der Arbeitszeit genutzt wird.
- Keinesfalls dürfen die berufliche Tätigkeit, die Qualität und die Quantität der Arbeitsleistung negativ beeinflusst werden. Dies gilt für die Beschäftigten selbst sowie für die Arbeit der Kolleginnen und Kollegen.
- Zusätzliche Kosten dürfen nicht entstehen; kostenpflichtige Angebote im Internet dürfen nicht genutzt werden. Ausnahmen sind in seltenen Fällen durch Vorgesetzte zu genehmigen.
- Die Beschäftigten dürfen aus der Erlaubnis der Privatnutzung nicht ableiten, dass die Internetdienste und der technische Support jederzeit verfügbar sind. Dies ließe sich aus § 84 TKG ableiten, weshalb einige Erklärungen diese Einschränkung bewusst formulieren.
- Die Beschäftigten müssen über die Gefahren und Risiken der Internetnutzung belehrt werden bzw. sich dessen bewusst sein. Die betrieblichen Anweisungen zur Benutzung des Internets müssen sie auch bei privater Nutzung einhalten.
- Inhaltliche Einschränkungen
  - Viele Arbeitgeber sichern sich durch vielfältige Verbote ab, um juristischen Klagen aufgrund von Fehlverhalten ihrer Beschäftigten vorzubeugen. In diesem Sinne werden Inhalte mit folgendem Charakter verboten: beleidigend, diskriminierend, intolerant, verleumderisch, sittenwidrig, sexistisch, (kinder-)pornografisch, rassistisch, gewaltverherrlichend, kriminell, verfassungsfeindlich; gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenzrechtliche oder urheberrechtliche Bestimmungen verstoßend.
  - Einige Arbeitgeber verbieten bestimmte Inhalte, um keine betrieblichen und wirtschaftlichen Nachteile zu erleiden:
    - Allgemein dürfen die dienstlichen Internetdienste auch privat nur im Rahmen der Treuepflicht zum Arbeitgeber – das heißt im Sinne und Interesse des Arbeitgebers – genutzt werden und nicht für (eigene) kommerzielle und geschäftsmäßige Zwecke, z. B. für eigene Werbemaßnahmen oder Geschäftstätigkeiten. Sie dürfen

auch nicht für weltanschauliche oder politische Werbung genutzt werden, wobei in Einzelfällen die gewerkschaftliche Betätigung nicht unter die Privatnutzung fällt.
    - Das Ansehen des Unternehmens in der Öffentlichkeit darf nicht leiden, Rufschädigungen müssen vermieden werden.
    - Betriebsgeheimnisse und sicherheitsrelevante Informationen dürfen nicht übermittelt werden; teilweise bezieht sich dies weitergehend auf alle betrieblichen Informationen sowie auf personenbezogene Daten der Beschäftigten oder auf Daten von Kunden und Lieferanten.
- Verbote werden auch ausgesprochen, um die Verfügbarkeit und Sicherheit der IKT-Systeme nicht zu beeinträchtigen. Jegliche Nutzung, die geeignet erscheint, dem Unternehmen Schaden zuzufügen, soll unterbleiben. Bekannte Gefahrenquellen sollen durch die folgenden Einschränkungen ausgeschlossen werden:
    - Private Hard- und Software und Programme, die aus dem Internet geladen werden können, dürfen nicht verwendet werden, es sei denn, der Arbeitgeber genehmigt Ausnahmen und/oder die IT-Organisation hat dies geprüft und zugelassen.
    - Die betrieblichen Sicherheitsmaßnahmen dürfen nicht umgangen werden; unter anderem dürfen die vom Arbeitgeber bereitgestellten Programme nicht verändert werden und der Einsatz von Anonymisierungs-Software ist unzulässig (vgl. BAG-Urteil vom 12. 01. 2006, Az.: 2 AZR 179/05).
    - Im Internet dürfen nur »seriöse« Adressen aufgerufen werden. Per E-Mail dürfen keine Verteilerlisten einbezogen, keine Kettenbriefe und Massenmails versendet werden.
    - Private Daten dürfen gar nicht oder nicht für längere Zeit gespeichert werden.
    - Chat und Instant-Messaging sind grundsätzlich verboten, sofern sie nicht von Vorgesetzten genehmigt wurden.
    - Web-Mail-Accounts (→ Glossar) dürfen nicht verwendet werden.

Handlungsanleitungen

- Wenige Erklärungen sind zudem als Handlungshilfen zu verstehen, wobei sich dies überwiegend auf das Nutzen von E-Mails – auch der

dienstlichen – bezieht. So enthalten die Erklärungen unter anderem folgende Hinweise:

– Bei der Eingabe von E-Mail-Adressen ist besondere Sorgfalt anzuwenden. Dienstliche E-Mail-Adressen sind nur für dienstliche Anlässe zu verwenden. Privat genutzte E-Mail-Adressen werden nach Ausscheiden aus dem Betrieb gelöscht, E-Mails werden nicht mehr zugestellt und nicht weitergeleitet. Für den Fall von Abwesenheiten werden Vertretungen eingerichtet, an die die E-Mails weitergeleitet werden. Dies gilt auch für private E-Mails.
– E-Mails mit unbekannten oder zweifelhaften Absendern oder Anhängen sind vorsichtig zu behandeln und eventuell nur nach Prüfung durch die IT-Organisation zu öffnen. Private E-Mails, die empfangen wurden, sind nach Kenntnisnahme zu löschen, dürfen aber an private E-Mail-Accounts weitergeleitet werden. Für die Vertraulichkeit privater E-Mails sind die Beschäftigten selbst verantwortlich, sie können diese z. B. löschen oder verschlüsseln. Persönliche Zugangsberechtigungen dürfen nicht an Dritte gegeben werden; umgekehrt dürfen fremde Berechtigungen nicht genutzt werden.

Protokollierung und Kontrolle

- Der Aspekt, der in den Erklärungen am häufigsten genannt wird, ist die Einwilligung in die Protokollierung der privaten Internetnutzung. Dies bezieht sich sowohl auf die Internetzugriffe als auch auf die E-Mails und umfasst regelmäßig die Verbindungs- sowie die Inhaltsdaten.
- Einige Vereinbarungen weisen in diesem Zusammenhang darauf hin, dass zwischen geschäftlicher und privater Internet- und E-Mail-Aktivität keine Unterscheidung möglich ist bzw. vorgenommen wird.
- Direkt damit verbunden ist die Einwilligung in die Auswertung der Protokolle; in Einzelfällen dürfen auch sonstige Speichermedien ausgewertet werden. Die Beschäftigten willigen durch ihre Erklärung ein, dass auch die private Nutzung ausgewertet werden darf. Die Bedingungen, unter denen die Auswertungen stattfinden dürfen, sind in den entsprechenden Vereinbarungen geregelt. Bisweilen werden sie in den Erklärungen wiederholt, ansonsten wird auf die Vereinbarung verwiesen. Diese muss der Beschäftigte gelesen und verstanden haben, was er mit seiner Unterschrift bestätigt.

- In einigen Erklärungstexten wird darauf hingewiesen, dass die Beschäftigten hiermit auch einer Einschränkung ihrer gesetzlichen Rechte gemäß §88 TKG (Fernmeldegeheimnis), §97 TKG (Nutzung der Verkehrsdaten zur Entgeltermittlung und -abrechnung) und/oder §100 TKG (Nutzung von Daten zur Störungs- und Fehlerbehandlung) sowie §§11 bis 15a TMG (Datenschutz) zustimmen. Wenige Erklärungen weisen allgemein darauf hin, dass Datenschutz- und Persönlichkeitsrechte eingeschränkt werden.
- Dazu gehört auch, dass mehrere Erklärungen darauf hinweisen, dass über Spam-Filter auch private E-Mails gelöscht werden können.

Maßnahmen bei Missbrauch und unzulässiger Nutzung

- Die Beschäftigten willigen durch ihre Unterschrift schließlich auch darin ein, dass bei Verstößen gegen die Vereinbarung bestimmte Maßnahmen ergriffen werden können. Diese können sich auf mehreren Ebenen bewegen und mehrere Elemente enthalten:
  - arbeitsrechtliche, disziplinarische, strafrechtliche
  - Teilweise wird darauf hingewiesen, dass die Maßnahmen angemessen bzw. verhältnismäßig sein sollen und im Arbeitsrecht von einer Belehrung bis zur fristlosen Kündigung reichen können; darüber hinaus werden oft Schadensersatzforderungen angedroht.
  - Als erste Maßnahme wird oft der sofortige Widerruf der Privatnutzung und der Entzug der Internet-Zugangsberechtigungen angedroht (ohne zu klären, wie Beschäftigte dann ihre Arbeit erledigen sollen).
  - Wenn der Verdacht des Missbrauchs auftritt, sollen die Betroffenen vor oder zeitgleich mit den Kontrollmaßnahmen darüber unterrichtet werden; dies sehen zumindest einige Regelungen vor.
  - In einigen Erklärungen willigen die Beschäftigten ein, dass die Informationen über Missbrauch oder unzulässige Nutzung an die Arbeitnehmervertretung, den Datenschutzbeauftragten und/oder an die Geschäftsführung weitergeleitet werden.

Zusammenfassung

Hier sind fast alle Regelungsaspekte aufgeführt, die in den vorliegenden Einwilligungs- und Verpflichtungserklärungen enthalten sind. Keine der Erklärungen beinhaltet jedoch alle diese Regelungen. Somit entstehen –

so könnte man daraus schließen – in jedem Unternehmen und in jeder Verwaltung Regelungslücken. Dies wird jedoch dadurch abgemildert, dass viele Erklärungstexte mit allgemeinen Formulierungen grundsätzlich dasselbe ausdrücken wie die Texte mit Detailregelungen, nur dass sie dadurch größere Spielräume für die Auslegung eröffnen. Aus Sicht der Beschäftigten sind detailliert formulierte Regeln im Sinne von eindeutigen Handlungsanleitungen einerseits zu begrüßen, um potenzielle Unsicherheiten im Umgang mit E-Mail und Internetdiensten zu minimieren. Andererseits sind sie in einer Erklärung, die zu unterschreiben ist und bei Missachtung schwerwiegende rechtliche Folgen haben kann, eher abschreckend. Ein gutes Beispiel für einen möglicherweise akzeptablen Kompromiss liegt leider nicht vor. Dieser könnte etwa so aussehen, dass eine knapp formulierte Erklärung zu unterzeichnen ist, die den unbedingt notwendigen juristischen Rahmen abdeckt (siehe das zuletzt zitierte Beispiel Gesundheit und Soziales, 090300/167/2010). Ergänzend dazu sollten die konkreten Leitlinien für das Handeln der Beschäftigten im Dialog mit ihnen und aus der betrieblichen Praxis heraus (weiter-)entwickelt werden. Dazu könnten das Intranet bzw. die innerbetrieblich etablierten sozialen Medien genutzt werden (vgl. Böker u. a. 2013).

2.1.14 Information und Qualifizierung der Beschäftigten

In der letzten Auswertung wurde aus einer Vereinbarung zitiert, dass »es sich bei der Internet-Technologie um eine mittlerweile relativ weit verbreitete Technik handelt«, so dass »lediglich eine Einweisung in die Nutzung des Browsers« erforderlich sei. Formulierungen wie diese sind in aktuellen Vereinbarungen nicht anzutreffen. Obwohl weiterhin lediglich rund ein Drittel der Vereinbarungen das Thema Qualifizierung aufgreift, lassen mehrere den Schluss zu, dass die in der Freizeit erworbenen Fähigkeiten nicht auf die beruflichen Anforderungen übertragbar sind: Sie betonen – wie in folgendem Beispiel – die »dienstlichen Anforderungen«.

> »Die Beschäftigten werden bei Bedarf für die dienstliche Nutzung des Internets umfassend geschult.«
>
> Gesundheit und Soziales, 090300/167/2010

Zudem sind die Regelungsinhalte und Formulierungen teilweise ausführlicher und konkreter als in früheren Vereinbarungen. Die zuletzt zitierte Vereinbarung regelt dazu beispielsweise Folgendes.

»[...] insbesondere folgende Themen:
– Bedienung des Internet-Browsers
– Aufbau des Internets, Nutzungsmöglichkeiten
– Datensicherheitsprobleme bei der Nutzung des Internets
– Besondere Datenschutzanforderungen in der [Firma] und sich daraus ergebende Vorschriften zum Datenschutz und Datensicherheit (vgl. Datenschutzkonzept)
– Sonstige dienstliche und gesetzliche Vorschriften bei Nutzung des Internets.«

Gesundheit und Soziales, 090300/167/2010

Am häufigsten werden Sicherheitsaspekte und die wirtschaftliche Nutzung der Internetdienste zusätzlich zur Anwendung der Softwarewerkzeuge als Schulungsinhalte genannt.
Nur selten bestimmen die betrieblichen Partner Lernziele, so dass die folgende Regelung, die sich auf Informations- und Kommunikationstechnik allgemein bezieht, eine Ausnahme unter den vorliegenden Vereinbarungen darstellt.

»Ziel der Qualifizierung ist die Vermittlung einer fundierten Anwenderkompetenz, die es ermöglicht, die technischen Leistungsmerkmale der IuK-Systeme souverän, d. h. ohne Stress und Angst vor Fehlern zu nutzen sowie auf ihre Gestaltung und Verbesserung aktiv Einfluss nehmen zu können.«

Ernährungsgewerbe, 090201/494/2008

Angesichts der schnellen Entwicklung der IuK-Technik ist es erforderlich, Qualifizierungen regelmäßig anzupassen. Nur wenige Vereinbarungen fordern jedoch, dass Schulungsmaßnahmen bzw. regelmäßig Bedarfsanalysen durchgeführt werden. Auch folgende Regelung stellt eine Ausnahme dar.

»Die Planung von Qualifizierungsmaßnahmen erfolgt auf der Grundlage einer vorher durchgeführten Bedarfsermittlung.«

Ernährungsgewerbe, 090201/494/2008

Während einige Vereinbarungen lediglich auf das betriebliche Schulungsangebot verweisen und den Mitarbeitern die Nutzung der Angebote empfehlen, sind andere in dieser Hinsicht rigoroser und erzwingen die Schulungsteilnahme vor Beginn der Nutzung. Möglicherweise hängt dies von der Unternehmensgröße ab: Auffallend restriktiv ist die folgende Regelung eines relativ kleinen Unternehmens aus dem Kreditgewerbe.

»Alle Vorgesetzten haben einmal jährlich ihre Mitarbeiter im Rahmen eines Mitarbeitergespräches auf die Bedeutung der Dienstvereinbarung zur Nutzung von elektronischen Kommunikations- und Informationsmedien hinzuweisen und eine aktuelle Version der Dienstvereinbarung (s. Intranet) in Umlauf zu geben. Die Mitarbeiter sind aufzufordern, sich mit dem aktuellen Stand der Dienstvereinbarung zur Nutzung von elektronischen Kommunikations- und Informationsmedien vertraut zu machen.
Die Mitarbeiter bestätigen mit Unterschrift und Datum, dass sie die Dienstvereinbarung zur Nutzung von elektronischen Kommunikations- und Informationsmedien zur Kenntnis genommen haben und diese beachten werden. Die Dokumentation gilt als Nachweis zur Mitarbeitersensibilisierung gegenüber dem Personalbereich.«

Kreditgewerbe, 090201/385/2009

Weitere spezielle Regelungen mit Bezug zur Internet- oder E-Mail-Nutzung finden sich in den Kapiteln 2.2 und 2.4.

2.1.15 Erreichbarkeit

Internetdienste sind grundsätzlich immer und überall verfügbar; sie sind nicht an Arbeitszeiten und Arbeitsorte gebunden. Die Verfügbarkeit von Computern und Internetzugängen in privaten Wohnungen sowie die zunehmende Verbreitung von Smartphones und mobilen Com-

putern mit Internetzugang über WLAN- und Mobilfunknetze an fast allen Orten heben die Grenzen zwischen Arbeit und Privatleben potenziell auf. Nach Einführung umfassender Flatrate-Angebote ist auch die Kostenbelastung als vielleicht letzte Hürde gefallen. Arbeitnehmer sind somit prinzipiell jederzeit und überall für berufliche bzw. dienstliche Belange erreichbar, können um Rat gefragt oder von Kunden, Lieferanten etc. erreicht werden.
In den letzten Jahren wird daher verstärkt darüber diskutiert, wie Arbeitszeit und Freizeit voneinander abgegrenzt werden können, beispielsweise indem die Nutzung der Kommunikationstechniken und Internetdienste technisch eingeschränkt wird. Aufsehen erregen Vereinbarungen, die E-Mail-Server zu bestimmten Zeiten abschalten. Andererseits verweist die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin auch auf Chancen für Beschäftigten, die durch Flexibilität entstehen (vgl. Pangert/Schüpbach 2013).
Die folgende Dienstvereinbarung einer öffentlichen Verwaltung regelte bereits vor rund zehn Jahren die Frage der Erreichbarkeit.

> »Der Internetzugang wird bis auf E-Mail an Feiertagen, Wochenenden und Zeiten der Betriebsruhe grundsätzlich abgeschaltet.«
>
> Öffentliche Verwaltung, 090300/209/2004

Auch diese Vereinbarung regelt die Frage offensiv.

> »Während des Zeitfensters von 18.15 Uhr bis 07.00 Uhr und an Wochenenden steht die Telefonfunktion zur Verfügung, alle anderen Anwendungen nicht. [...] Über besondere Einzelfälle, die durch diese Verfahrensregelung nicht ausreichend abgedeckt sind, werden Unternehmen und Betriebsrat einvernehmlich entscheiden.«
>
> Fahrzeughersteller Kraftwagen, 090202/174/2011

Die folgende Vereinbarung geht einen etwas anderen Weg und regelt Reaktionszeiten und Abwesenheitsfreiräume.

> »Der Mitarbeiter stimmt mit seinem Vorgesetzten unter Berücksichtigung und Abwägung betrieblicher und privater Erfordernisse seine Erreichbarkeit ab. Diese orientiert sich an der im jeweiligen Team üb-

lichen Lage der Arbeitszeit, kann aber auf Wunsch des Mitarbeiters davon abweichen. Außerhalb der abgestimmten Zeiten der Erreichbarkeit hat der Mitarbeiter im Sinne der Ruhe und Erholung das Recht, nicht erreichbar zu sein. Dazu zählen in der Regel – soweit nicht Bestandteile des jeweiligen Arbeitszeitmodells – die Abend- und Morgenstunden sowie Samstage, Sonn- und Feiertage.
Der Mitarbeiter muss außerdem die Möglichkeit haben, die ihm übertragenen Aufgaben in einer angemessenen Zeit innerhalb der üblichen Arbeitszeiten oder innerhalb der mit seinem Vorgesetzen abgestimmten Mobilarbeitszeiten erledigen zu können (Reaktionszeit).«

Fahrzeughersteller Kraftwagen, 080102/219/2013

Andere Regelungen erlauben den Beschäftigten, außerhalb der Arbeitszeit und des Betriebsgeländes die dienstlichen mobilen Kommunikationsgeräte zu nutzen; sie verpflichten sie jedoch nicht dazu.

»Es besteht ausdrücklich keine Verpflichtung, außerhalb der Rahmenarbeitszeit für die [Firma] mittels dieser Kommunikationsmittel erreichbar zu sein.«

Grundstücks- und Wohnungswesen, 090300/205/2009

Thannheiser (2014) befasst sich in seiner Auswertung zum Thema mobile Endgeräte ausführlich mit Aspekten mobiler Endgeräte, u. a. auch mit Fragen der Erreichbarkeit.

2.1.16 Verhaltensregeln und Netiquette

Rund die Hälfte der vorliegenden Vereinbarungen enthalten für die Beschäftigten Informationen, die ihnen den angemessenen und sicherheitsorientierten Umgang mit E-Mail und Internetdiensten empfehlen, meist jedoch zwingend vorschreiben. Diese Verhaltensregeln werden im Folgenden behandelt, während die technischen Sicherheitsmaßnahmen in Kapitel 2.1.4 beschrieben wurden.

Sicherheit

Der größte Teil der Verhaltensregeln schreibt den Beschäftigten vor, was sie im Sinne der Sicherheit der Datenverarbeitung tun müssen bzw. nicht tun dürfen. Damit übertragen einige Unternehmen eine Mitverantwortung für die Datensicherheit auf ihre Beschäftigten. Dies sollten Arbeitnehmervertretungen jedoch weitgehend zurückweisen, da die technischen Maßnahmen durch das Unternehmen so gestaltet sein müssen, dass Fehler der Beschäftigten keine schwerwiegenden Auswirkungen haben können. Es empfiehlt sich, Regelungen wie beispielsweise die folgende zu treffen, die einen angstfreien Umgang mit den Internetdiensten ermöglichen.

> »Den Mitarbeiterinnen/Mitarbeitern darf aus irrtümlicher Anwendung des Internets und der E-Mail kein arbeitsrechtlicher Nachteil entstehen.«
>
> Verbände und Gewerkschaften, 090300/168/2007

Auch organisatorisch können Arbeitgeber dafür sorgen, dass die Beschäftigten von Verantwortung befreit werden, wie die folgende Richtlinie aus dem öffentlichen Dienst zeigt.

> »Um die Beschäftigten weitgehend von technischen Aufgaben zu entlasten und eine geordnete einheitliche Weiterentwicklung des Nutzungskonzeptes für Informationstechnik zu gewährleisten, ist in der Verwaltung eine Koordinierungsstelle beim Personal- und Organisationsamt eingerichtet, die für diese Aufgaben zuständig ist.«
>
> Öffentliche Verwaltung, 090201/508/2010

Die folgende Regelung in einer Betriebsvereinbarung fordert die Beschäftigten auf, bestimmte Sicherheitsregeln zu beachten. Sie stellt ein akzeptables Maß dar, das von den Beschäftigten zusätzlich zu den zwingend notwendigen technisch-organisatorischen Sicherheitsvorkehrungen des Arbeitgebers verlangt werden kann.

> »Die folgenden Regeln und Richtlinien müssen zum Schutze der IT-Ressourcen und Daten eingehalten werden:

– Der PC ist in geeigneter Weise vor unberechtigten Zugriffen zu schützen (z. B. Einschalten des Bildschirmschoners beim Verlassen des Arbeitsplatzes).
– Bei der Speicherung personenbezogener Daten sind die gesetzlichen Bestimmungen zu beachten.
– Die Passwörter müssen stets geheim gehalten werden, um Missbrauch vorzubeugen.
– Daten auf lokalen Datenträgern sind vom Mitarbeiter zu sichern, Daten innerhalb des Netzwerks werden durch IS gesichert.
– Die Mitnahme von Daten in jeglicher Form (externe Speichermedien, Notebook, PDA etc.) ist ausschließlich für dienstliche Zwecke gestattet. Der Mitarbeiter trägt bei der Mitnahme selbst die Verantwortung für einen geeigneten Schutz der Daten. IS unterstützt dabei die Mitarbeiter mit z. B. Sicherheitsrichtlinien für Laptops oder Handhelds.«

Metallverarbeitung, 090300/271/2008

Darüber hinaus regeln einige Vereinbarungen, dass vertrauliche Informationen des Unternehmens nicht über elektronische Medien verbreitet werden dürfen. Dies sollte selbstverständlich sein, jedoch sehen einige betriebliche Verhandlungspartner wegen der Offenheit der Internet-Kommunikation hier die Notwendigkeit, dies besonders zu betonen.

»Vertrauliche Informationen dürfen nicht mit unbefugten Personen (weder mit Unternehmensangehörigen noch mit Personen außerhalb des Unternehmens) besprochen oder an diese weitergegeben werden. Werden Unterlagen mit vertraulichen Informationen per Fax oder mittels anderer elektronischer Medien verschickt, sind alle erforderlichen Maßnahmen zu ergreifen, damit unbefugte Personen (weder Unternehmensangehörige noch Personen außerhalb des Unternehmens) nicht davon Kenntnis nehmen können. Beim Vernichten von Unterlagen, die vertrauliche Informationen enthalten, sind (ungeachtet des Mediums, auf dem diese Dokumente festgehalten sind) die entsprechenden Sicherheitsmaßnahmen zu ergreifen.«

Metallerzeugung und -bearbeitung, 080600/51/2009

Netiquette

Ein Teil der Verhaltensregeln, die auch als Netiquette (→ Glossar) bezeichnet werden, empfiehlt den Beschäftigten, auch im Internet die Umgangsformen der »normalen« Kommunikation beizubehalten.
Die Regeln werden oft zusammen mit der Einverständniserklärung formuliert, die von Beschäftigten bei Erlaubnis zur Privatnutzung unterschrieben werden muss (vgl. Kap. 2.1.13).

> »Die Dienststellenleitung und der Personalrat sind sich darin einig, dass Aktivitäten und Äußerungen mit
> – rassistischen (dies bedeutet übersteigertes Rassenbewusstsein, Rassendenken, Rassenhetze),
> – sexistischen (dies umfasst Handlungen und Äußerungen, die darin bestehen, einen Menschen allein aufgrund seines Geschlechts zu benachteiligen und zu diskriminieren, insbesondere diskriminierendes Verhalten gegenüber Frauen),
> – diskriminierenden (dies bedeutet, durch unzutreffende Äußerungen, Behauptungen in der Öffentlichkeit dem Ansehen oder dem Ruf einer Person zu schaden, sie herabzusetzen oder durch unterschiedliche Behandlung zu benachteiligen oder zurückzusetzen),
> – gewaltverherrlichenden (dies bedeutet, Gewalt in jeder Hinsicht glorifizierend darzustellen)
> Inhalten nicht toleriert werden und ausdrücklich verboten sind.«
>
> Öffentliche Verwaltung, 090300/202/0

Dazu gehört laut manchen Vereinbarungen auch ein verantwortungsvoller und pfleglicher Umgang mit technischen Geräten.

> »Die Mitarbeiter/-innen sind verpflichtet, mit den ihnen zur Verfügung gestellten Informations- und Kommunikationstechniken verantwortungsvoll umzugehen und sie im Interesse der [Firma] einzusetzen.«
>
> Grundstücks- und Wohnungswesen, 090201/292/2006

Eindeutige Verhaltensregeln, auch für spezielle Situationen wie in folgendem Beispiel, sind selten anzutreffen. Sie zeigen jedoch, dass die betrieblichen Partner klare Handlungshilfen zur Verfügung stellen möchten.

»Verlust oder Diebstahl eines Gerätes ist der IT-Abteilung innerhalb eines Arbeitstages zu melden. [...] Mobile Firmengeräte sind Eigentum des Unternehmens und müssen nach Beendigung des Arbeitsverhältnisses zurückgegeben werden.«

Chemische Industrie, 090202/190/2012

2.1.17 Social-Media-Regelungen in Vereinbarungen zu Internet und E-Mail

Soziale Medien stellen seit einigen Jahren eine wesentliche Nutzungsform der Internetdienste dar. Unter den Schlagworten Social Media, Web 2.0 oder auch Produktnamen wie Facebook, Xing, Twitter etc. sind diese Anwendungen vielen Internetnutzern geläufig. Innerhalb und außerhalb von Betrieben wird Social Media zu Datenaustausch, Kommunikation und Zusammenarbeit genutzt. In Deutschland nutzen rund 27 Millionen Menschen Facebook aktiv (vgl. Buggisch 2014). Darüber hinaus nutzten im Jahr 2013 37 Prozent aller Unternehmen in Deutschland mit Internetzugang soziale Medien (vgl. Statistisches Bundesamt 2013). In der Realität der betrieblichen Vereinbarungen zu E-Mail und Internetdiensten scheint dies jedoch noch nicht angekommen zu sein, denn eine Auseinandersetzung mit den Möglichkeiten und Problemen dieser Techniken und darauf basierende möglichst eindeutige Regelungen für die Beschäftigten fehlen im ausgewerteten Material weitgehend.
Einzig ein Medienunternehmen beschreibt in seiner Vereinbarung zur Nutzung von E-Mail und Internet Folgendes.

»Die Nutzung sozialer Netzwerke wie Twitter, Facebook, Xing oder Wikipedia gewinnt eine immer größere Bedeutung [...]. Die [Firma] kann sich hier darstellen, ihre Produkte verbreiten und für sie werben. Es liegt im Interesse der [Firma], das Engagement der Mitarbeiter im Bereich der sozialen Medien zu fördern.«

Verlags- und Druckgewerbe, 090300/226/2011

Dieses Unternehmen steht dem Einsatz sozialer Medien positiv gegenüber, verweist jedoch im weiteren Verlauf der Regelung auch auf die dadurch entstehenden Probleme. Die Regeln, nach denen die Beschäftig-

ten ihr Verhalten ausrichten sollen, sind in einem Zusatzdokument vereinbart und veröffentlicht, das der Vereinbarung als Anlage beigefügt ist.

> »Um den Beschäftigten Sicherheit im Umgang mit den sozialen Netzwerken zu geben und darüber hinaus die Interessen beider Seiten gleichermaßen zu wahren, haben die Betriebsparteien einen Kodex erstellt als Regelwerk für das digitale Miteinander im Internet.«
>
> Verlags- und Druckgewerbe, 090300/226/2011

Auch andere Vereinbarungen verweisen auf gesonderte Regelwerke. Teilweise scheinen diese jedoch ohne Beteiligung der Arbeitnehmervertretung entwickelt und veröffentlicht worden zu sein, da sie als Dienstanweisung, Richtlinie oder Ähnliches vorliegen.
Zudem findet sich auch der umgekehrte Fall: In einem vorliegenden »Social Media Guide« wird bezüglich der Privatnutzung auf die Vereinbarung zu Internet und E-Mail verwiesen. Es lässt sich nur vermuten, weshalb die Nutzung von Social Media nicht in mehr Vereinbarungen explizit thematisiert wird. Ein Grund ist sicher, dass die Realität, wie erwähnt, erst zeitlich verzögert in den Vereinbarungen abgebildet wird. Zudem wird das Mitbestimmungsrecht des Betriebsrats bei Regelungen zu Facebook und Co. nicht immer erkannt.
Möglicherweise reichen aus Sicht der Betriebsparteien die vorhandenen Regelungen auch aus. Denn viele Vereinbarungsgegenstände aus gängigen Social-Media-Richtlinien überschneiden sich inhaltlich mit denen aus IKT-Rahmenbetriebsvereinbarungen oder Vereinbarungen, wie sie hier ausgewertet wurden. Beispielhaft seien genannt:

- Privatnutzung der Internetdienste
- Nutzung der vom Arbeitgeber gestellten Hardware
- Nutzung der eigenen Geräte in den Pausen bzw. in der Arbeitszeit
- Nutzung mobiler Geräte: Dürfen private Geräte genutzt werden? Wem wird ein Gerät vom Arbeitgeber gestellt? etc.
- Betriebs- und Geschäftsgeheimnisse wahren
- Imageschaden für das Unternehmen verhindern
- Hinweise zur Einhaltung des Urheberrechts, des Datenschutzrechts und anderer allgemeiner gesetzlicher Regelungen
- Umgangsformen/Netiquette
- Verfahrensweise bei Verstößen gegen die Regelungen

Für weiterführende Informationen sei auf die Auswertung von Social-Media-Guidelines (Greve/Wedde 2014) sowie auf die (mitbestimmungs-)rechtliche Bewertung von Böker u. a. 2013 verwiesen.

2.2 Spezielle Regelungen zum Internet

In diesem Kapitel werden nun spezielle Aspekte der Internetnutzung herausgearbeitet.

2.2.1 Ziele der Internetnutzung

Der Zugang zum Internet wird den Beschäftigten mit dem Ziel zur Verfügung gestellt, Arbeitsprozesse effizienter zu machen. In einigen der vorliegenden Vereinbarungen wird explizit von Beschleunigung gesprochen. Der Zugang wird als Arbeitsmittel zur Verfügung gestellt, Freiwilligkeit wird im Gegensatz zur letzten Auswertung nicht mehr thematisiert.

> »Der Internet-Zugang steht den Beschäftigen als Arbeitsmittel im Rahmen der Aufgabenerfüllung zur Verfügung. Er dient dazu, die Kommunikation zu verbessern, die Effizienz zu steigern und die Informationsbeschaffung sowie die Arbeitsprozesse zu beschleunigen.«
>
> Öffentliche Verwaltung, 090300/294/2005

2.2.2 Aufgaben und Inhalte der Internetnutzung

Schnellere und bessere Erledigung der Arbeitsaufgaben werden als Hauptzweck der Internetnutzung genannt, generell sollen die betrieblichen Abläufe unterstützt werden. Beispielsweise sollen Mitarbeiterinnen und Mitarbeiter die Zugänge zu Homepages und Datenbanken von Lieferanten, Kunden usw. nutzen. In den neueren vorliegenden Verein-

barungen ist auch das Nennen von Beschäftigtendaten auf der Homepage des Arbeitgebers geregelt, wenngleich eher selten.

> »Auf der Homepage der [Firma] können Daten der Beschäftigten aufgeführt werden, soweit sie zur Erfüllung der Aufgaben (Funktion, Ansprechpartner, Kundeninformation, Angebote Vertrieb etc.) benötigt werden.«
>
> Grundstücks- und Wohnungswesen, 090201/292/2006

2.2.3 Nicht erlaubte Internetnutzung

Viele Unternehmen und Verwaltungen sorgen sich um ihr Image, wenn Beschäftigte das Netz nutzen. Aus einer Richtlinie stammt folgendes Verbot.

> »Unzulässig ist jede Internetnutzung, die geeignet erscheint, den Interessen der [Firma] oder deren Ansehen in der Öffentlichkeit zu schaden, oder die gegen geltende Gesetze oder Verordnungen verstößt.«
>
> Versicherungsgewerbe, 010502/62/2010

Einschränkungen oder Verbote findet man in Zusammenhang mit der kostenpflichtigen Nutzung von Angeboten oder Downloads im Netz. Wie in älteren Vereinbarungen auch, ist verboten, was die IT-Sicherheit gefährden könnte.

> »Nicht erlaubt ist das Beschaffen und Verbreiten von Software und Programmen (z. B. .exe-Dateien) aus dem Internet durch Herunterladen (Download) und deren Versand (Upload) u. a. wegen der Gefahr des Einschleppens und Verbreitens von Computerviren.«
>
> Versicherungsgewerbe, 010502/62/2010

Ebenso ist untersagt, was den Betrieb stört, beispielsweise Videos, Musik und interaktive Spiele herunterzuladen. Gelegentlich werden einzelne Dienste verboten.

»Die Teilnahme an Chatrooms ist untersagt.«

Möbelhersteller, 090300/170/2007

Das wirkt anachronistisch und wird in der Umsetzung problematisch, spätestens dann, wenn soziale Medien im Spiel sind.
Weitere Beispiele für nicht erlaubte Internetnutzung sind: mit einer falschen Identität im Netz agieren oder eigene Geschäfte erledigen. In einigen Vereinbarungen ist auch geregelt, dass der Zugang zum Netz nicht über andere Wege als die vorgesehenen erfolgen darf. Das kann den Netzzugang über das private Smartphone einschließen.
Zusammenfassend lässt sich sagen, dass in Betrieben verboten ist, was dem Ansehen des Arbeitgebers schaden kann und/oder gegen geltendes Recht verstößt: Verhalten, das gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt, ist in den Vereinbarungen meist ausführlich aufgeführt.

2.2.4 Zugangs- und Nutzungsberechtigungen, Verantwortlichkeiten

Im Vergleich zur letzten Auswertung (2008) ist der Zugang zum Internet selbstverständlicher geworden. Diesen Schluss lassen folgende Formulierungen zu.

»Um die Teilnahme an der internen und externen Kommunikation sicherzustellen, stellt der Verlag allen Beschäftigten einen dienstlichen E-Mail-Zugang (personalisierte E-Mail-Adresse) und einen Internetzugang zur Verfügung.«

Verlags- und Druckgewerbe, 090300/315/0

»Alle PC-Arbeitsplätze sind mit Kommunikationssoftware für E-Mail, Intranet und Internet ausgestattet.«

Versicherungsgewerbe, 010502/62/2010

Regelungen, in denen der Vorgesetzte entscheidet, ob Beschäftigte einen Zugang erhalten oder nicht, sind seltener geworden. In dieser Regelung wird versucht, den »Nasenfaktor« zu minimieren.

»Bei der Festlegung der Beschäftigten, die Zugriff auf das Internet haben, entscheiden allein sachliche, aus der Art der Arbeit zu begründende Kriterien.«

Gesundheit und Soziales, 090300/157/2005

Nachstehend stellt der Zugang zum Netz sogar ein Recht der Beschäftigten dar.

»Alle zugelassenen Beschäftigten haben das Recht, im Rahmen ihrer beruflichen Tätigkeit den Zugang zum Internet zu nutzen.«

Gesundheit und Soziales, 090300/167/2010

In dieser bereits etwas älteren Regelung wird den Mitarbeitern die Initiative übertragen, auf einen Internetanschluss hinzuwirken.

»Alle Benutzerinnen und Benutzer, für deren Arbeitsgebiet die Nutzung des Internets nützlich ist, erhalten auf Antrag einen Internet-Zugang.«

Metallerzeugung und -bearbeitung, 090201/424/2000

Viele Regelungen greifen das Thema Gleichberechtigung auf: Was ist mit den Beschäftigten, die keinen PC-Arbeitsplatz haben?

»Gleichheitsgrundsatz
Alle Mitarbeiter an computerunterstützten Arbeitsplätzen haben an mindestens einem ihnen persönlich zugeordneten Rechner Zugang zum Internet sowie zu den E-Mail-Funktionen.
Allen übrigen Mitarbeitern wird die Möglichkeit eingeräumt, an zentral aufgestellten Terminals Internet und E-Mail-Funktionalität zu nutzen und auf die betrieblichen elektronischen Informationssysteme zuzugreifen.«

Anonym, 090300/156/2002

Die Frage der Zuordnung von Daten zu Personen ist nach wie vor ein wichtiger Regelungspunkt.

»Die Systeme dürfen nur mit der gültigen persönlichen Zugangsberechtigung genutzt werden. Passwörter dürfen nicht an Dritte weitergeben werden.«

Gesundheit und Soziales, 090300/167/2010

2.2.5 Sicherheit der Internetnutzung

Um eine sichere Internetnutzung zu ermöglichen, werden Firewallsysteme zwischen dem Unternehmensnetzwerk und dem öffentlichen Internet aufgebaut. Diese dienen insbesondere zur Abwehr externer Angriffe auf das Unternehmensnetzwerk. Um derartige Angriffe erkennen zu können, werden im Firewallsystem Daten über den ein- und ausgehenden Datenverkehr gespeichert und von der Systemadministration ausgewertet. So gut wie alle Vereinbarungen und Richtlinien, welche die Internetnutzung zum Thema haben, lassen sie die Speicherung dieser Daten zu.
Die Sicherheitsprobleme, die mit der Internetnutzung verbunden sind, lassen sich nicht allein über eine zentrale EDV-Abteilung oder über technische Sicherheitsstandards lösen – so wichtig sie auch sein mögen. Ohne die aktive Mithilfe der Beschäftigten würden erhebliche Sicherheitslücken bestehen bleiben.
In einigen wenigen Regelungen ist festgelegt, wie der Zugriff auf das Unternehmensnetzwerk von außen zu erfolgen hat. Die Vereinbarungen beziehen sich im Wesentlichen auf sicherheitsrelevantes Verhalten innerhalb des Firmennetzwerks: Mehr oder weniger ausführliche Hinweise zu Downloads oder wie man sich verhalten soll, wenn Virenbefall zu vermuten ist, sind Beispiele dafür. Auch hier wird die Nutzung eigener Geräte teilweise untersagt.
Einige Regelungen zur Sicherheit beziehen sich auf Daten, die das Unternehmensnetzwerk nicht verlassen dürfen.

»Dem Mitarbeiter ist es nicht erlaubt, vertrauliche und betriebsinterne Informationen, die in Verbindung mit [der Firma] stehen, sowie fremde personenbezogene Daten nach dem Bundesdatenschutzgesetz (BDSG) ohne Berechtigung über Internetseiten zu übertragen bzw. darauf zu veröffentlichen. Die Übertragung bzw. Veröffentli-

chung derartiger Daten muss im Einzelfall vom Vorgesetzten oder, soweit fremde personenbezogene Daten betroffen sind, vom Datenschutzbeauftragten genehmigt werden.«

Ernährungsgewerbe, 090300/277/2009

2.2.6 Personenbezogene Daten, Auswertungen, Protokollierungen

In Kapitel 2.1.7 wurde das Thema Protokollierungen bereits ausführlich behandelt, soweit es allgemeine Regelungen zu den Internetdiensten gibt.
Wie bereits in Kapitel 2.2.5 ausgeführt, wird aus Sicherheitsgründen in fast jeder Vereinbarung bzw. Richtlinie zugelassen, dass die Internetnutzung im Firewallsystem automatisch protokolliert wird. Zusätzliche Protokollierungen finden durch die Proxyserver statt, die aufgerufene Internetseiten speichern, um sie dem Benutzer bei erneutem Aufruf schneller anzeigen zu können. In der Regel fallen im Arbeitsplatzrechner weitere Protokolldaten an, die – ebenfalls zur Erhöhung des Benutzungskomforts – die aufgerufenen Internetseiten in begrenztem Umfang speichern. In allen Protokollen werden Internetadressen und Namen der Seiten, Benutzerkennung, Datum und Uhrzeit des (letzten) Aufrufs sowie die Zugriffsdauer gespeichert, so dass prinzipiell eine lückenlose Verhaltenskontrolle des Benutzers an mehreren Stellen durchführbar wäre.
In vielen Vereinbarungen ist die private Nutzung der IKT-Systeme daran gebunden, dass die Nutzer der Protokollierung zustimmen (ausführlicher dazu vgl. Kap. 2.1.13).

2.3 Spezielle Regelungen zum Intranet

In der aktuellen Auswertung finden sich Vereinbarungen und Regelungen, die das Intranet als Informationsbasis für Mitarbeiterinnen und Mitarbeiter betreffen. Neu sind Vereinbarungen, die interne Netze mit so genannten Social-Business-Tools (→ Glossar) regeln: Hier wechselt

der Fokus von den Beschäftigten als Empfängern von Informationen hin zu Mitgestaltern der unternehmensinternen Information und Kommunikation.
Die technische Sicherheitsproblematik ist von geringerer Bedeutung als beim Internetzugriff, da es sich um ein nichtöffentliches Netzwerk handelt. In den vorliegenden Vereinbarungen ist daher wenig zum Thema Sicherheit in internen Firmennetzen zu finden (vgl. Kap. 2.3.3).

2.3.1 Aufgaben und Inhalte der Intranetnutzung

Einige Unternehmen handhaben das Einstellen von Inhalten in das interne Netz eher restriktiv. Sie definieren es als vom Arbeitgeber bereitgestellte Sammlung wichtiger Informationen und Arbeitsanweisungen für die Beschäftigten. Aus einer bereits etwas älteren Vereinbarung stammt folgende Formulierung.

> »Welche Dokumente und Inhalte in das Intranet gestellt werden, bestimmt die Geschäftsführung.«
>
> Grundstücks- und Wohnungswesen, 090201/292/2006

Andere Vereinbarungen – durchaus auch solche älteren Datums – sehen das Intranet als Ort eines offenen innerbetrieblichen Informations- und Gedankenaustausches.

> »Das Intranet unterstützt eine offene und geschäftsbezogene Informations- und Kommunikationskultur. Welche Dokumente und welche Inhalte in das Intranet gestellt werden, bestimmt jede Abteilung selbst.«
>
> Tankstellen, Kfz.-Reparatur und -Handel, 090300/162/2009

Auch wenn soziale Medien eingesetzt werden, ist es die Hauptaufgabe des betrieblichen Netzes, interne Abläufe und die Zusammenarbeit zu optimieren.

»Die sozialen Netzwerkfunktionen im Intranet haben den Zweck, die Zusammenarbeit der Mitarbeiter bei [der Firma] zu unterstützen und zu erleichtern.«

Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/291/2012

Die erwähnte Aufweichung zwischen Sendern und Empfängern von Informationen wird in diesem Beispiel deutlich.

»Ziel ist es, den Mitarbeitern eine leistungsfähige und zeitgemäße Technik zum Informationsaustausch zur Verfügung zu stellen. Dazu wird den Mitarbeitern im Intranet eine [persönliche Seite] zur Verfügung gestellt, die die Kommunikation und Vernetzung zwischen den Mitarbeitern erleichtern und fördern soll.«

Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/291/2012

2.3.2 Zugangs- und Nutzungsberechtigungen, Verantwortlichkeiten

Zugang zum internen Netz haben in den meisten Betrieben zumindest alle, die über einen PC am Arbeitsplatz verfügen. Um auch diejenigen nicht vom internen Austausch auszuschließen, für die das nicht gilt, gibt es Regelungen wie die Folgende.

»An jedem Standort ist ein für die Beschäftigten [...] zugänglicher PC mit Bildschirm (Terminal) aufzustellen, damit die im Intranet zur Verfügung gestellten Informationen eingesehen werden können.«

Metallerzeugung und -bearbeitung, 90300/142/2006

Für das Nutzungsverhalten im Intranet gelten häufig ähnliche Regelungen wie für das Internet, pauschal gesagt: Es soll nichts Verbotenes oder Anstößiges ins Intranet gestellt werden. Einige Regelungen verbieten die private Nutzung des internen Netzes oder definieren Bereiche, wo diese erlaubt ist.

»Die Nutzung des Intranets zu privaten Zwecken ist grundsätzlich nicht gestattet.«

Fahrzeughersteller sonstiger Fahrzeuge, 090300/179/2010

»Für private Beiträge wird den Beschäftigten ein schwarzes Brett zur Verfügung gestellt, wobei diese Beiträge den Unternehmensinteressen nicht entgegenstehen dürfen.«

Grundstücks- und Wohnungswesen, 090300/205/2009

Aus der gleichen Vereinbarung stammt eine Formulierung, die nicht dazu führen dürfte, dass das Intranet als Ort des innerbetrieblichen Austausches genutzt wird und Beschäftigte dort die Informationen finden, die sie tatsächlich brauchen.

»Das Intranet der [Firma] wird ausschließlich für geschäftsbezogene Informationen genutzt. Die Geschäftsführung entscheidet, wer welche Dokumente mit welchem Inhalt einstellen darf.«

Grundstücks- und Wohnungswesen, 090300/205/2009

Die folgende Vereinbarung formuliert explizit die Rechte der Gewerkschaften im verwaltungsinternen Netz.

»Den im Geltungsbereich dieser Dienstvereinbarung vertretenen Gewerkschaften wird die Möglichkeit eröffnet, im Intranet eigene Inhalte zu präsentieren und sich direkt per E-Mail an die Beschäftigten zu wenden.«

Öffentliche Verwaltung, 090300/293/2012

2.3.3 Sicherheit der Intranetnutzung

Ziel der unter diesem Aspekt aufgeführten Regeln ist es, die Funktionsfähigkeit des Intranets und die darin gespeicherten personenbezogenen Daten sowie die Firmendaten zu schützen. Hier werden im Wesentlichen die Maßnahmen umgesetzt, die das BDSG in § 9 (Technische und organisatorische Maßnahmen) festlegt. Der Schutz muss sowohl von außen (vgl. Kap. 2.1.4) als auch aus dem eigenen Netz heraus sicher-

gestellt werden. Zu den allgemeinen Sicherungsmaßnahmen wie dem Einsatz von Firewalls finden sich Hinweise in Kapitel 2.1.4.
Beispiele für Maßnahmen, die speziell zum Intranet genannt werden, sind: die Server stehen in besonders abgesicherten Räumen (Zutrittskontrolle); die Systeme werden durch Zugriffs- und Passwortschutz vor unbefugtem Zugriff geschützt (Zugangskontrolle); Verschlüsselungsmaßnahmen sollen Daten auf dem Transportweg sichern (Weitergabekontrolle).
Die meisten Vereinbarungen führen konkret aus, wie die einzelnen Maßnahmen umgesetzt werden.

> »Für die Nutzung der IT-Infrastruktur werden den Mitarbeitern sowie den Partnern der [Firma] Berechtigungen erteilt. Ein Zugriffsschutz auf das Netzwerk wird somit durch die Eingabe einer Benutzerkennung (Username) und die Vergabe eines Passwortes geregelt. Die Zugriffsberechtigungen sind ausschließlich von den jeweils berechtigten Anwendern zu nutzen.«
>
> Gummi- und Kunststoffherstellung, 090300/178/2009

Noch deutlicher ist die folgende Formulierung.

> »Die Nutzung einer Kennung durch mehrere Personen ist untersagt.«
>
> Grosshandel (ohne Kfz.), 090300/290/2008

Manchmal wird die gleichzeitige Nutzung des Intranets und des Internets verboten, wie die folgende Regelung zeigt. Über die vermutlich schwierige praktische Umsetzung liegen allerdings keine zusätzlichen Informationen vor.

> »Aus Sicherheitsgründen darf kein Gerät oder IT-Equipment gleichzeitig mit dem Unternehmensnetzwerk und einer anderen externen Verbindung (z. B. WLAN, ISDN, DSL, UMTS) verbunden sein.«
>
> Mess-, Steuer- und Regelungstechnik, 090300/212/2010

2.3.4 Personenbezogene Daten, Auswertungen, Protokollierungen

Ebenso wie in den Regelungen zum Internet wird in einigen Vereinbarungen zum Intranet die Erhebung personenbezogener Daten sowie die Leistungs- und Verhaltenskontrolle ausgeschlossen.

> »Bei der Nutzung des Intranets werden keine personenbezogenen oder -beziehbare Benutzer-Daten erhoben.
> Die mit dem Intranet zusammenhängenden Hardware- und Software-Systeme werden nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Beschäftigten genutzt.«
>
> Fahrzeughersteller von Kraftwagenteilen, 090300/166/2001

Dass die von einigen Unternehmen gewünschte Vernetzung von Beschäftigten nur dann funktioniert, wenn auch personenbezogene Daten preisgegeben werden, deutet diese Vereinbarung an.

> »Ein Mitarbeiterverzeichnis (internes Telefonbuch, Geburtstagsliste ...) ist bereits Bestandteil der Unternehmensdokumentation. Die innerbetriebliche Kommunikation zwischen Beschäftigten verschiedener Abteilungen und Standorte kann durch die Einbindung von Mitarbeiterfotos und Veröffentlichung personenbezogener Daten verbessert werden.«
>
> Kreditgewerbe, 090300/223/2011

Bei zunehmender Vernetzung innerhalb des Betriebs wird schnell deutlich, wer aktiv ist im internen Netz – und wer nicht. Selbst wenn keine aktive Leistungs- und Verhaltenskontrolle seitens des Arbeitgebers erfolgt, liegen bei der Nutzung interner Vernetzungstools Daten vor, die eine solche potenziell ermöglichen. Damit Beschäftigte trotz dieser Umstände die Wahl haben und entscheiden können, was sie von sich preisgeben wollen (und was nicht) und inwieweit sie überhaupt an der Vernetzung teilhaben möchten, ist nachstehend geregelt, dass sie dies sanktionsfrei tun dürfen.

»Die Nutzung [des Intranets] ist freiwillig. Mitarbeitern, die die Funktionalitäten [des Intranets] oder einzelne Felder oder Funktionen nicht nutzen, dürfen daraus keine Nachteile entstehen.«

Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/291/2012

Wenn Beschäftigte die internen Medien nun nutzen, um sich beispielsweise mit Projektmitarbeiterinnen und -mitarbeitern auszutauschen oder schneller an Informationen zu kommen, müssen folgende Aspekte geregelt sein: Wer hat auf die anfallenden Daten Zugriff? Wer darf welche Auswertungen machen?

»Dem Seiteninhaber werden durch [das Intranet] keine Auswertungen oder Reports über [seinen persönlichen Zugang] angezeigt.
Den Community Managern werden ausschließlich folgende anonymisierte Auswertungen über ihre Community, so genannte community reports, angezeigt:
– Tortendiagramm der verwendeten Funktionen (in %)
– Anzahl der Aktivitäten an bestimmten Tagen
[...] Auch für Administratoren ist nicht sichtbar, wer wann wie lange auf einer Seite war.
Auswertungen, welche Mitarbeiter welche Artikel bewertet haben bzw. bewertet wurden, werden nicht durchgeführt.«

Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/291/2012

2.4 Spezielle Regelungen zur E-Mail-Nutzung

In den Regelungen zur E-Mail-Nutzung geht es insbesondere um folgende Fragen: Wie werden E-Mails genutzt? Wie sind mögliche Sicherheitsprobleme in den Griff zu bekommen? Wie ist mit der privaten Nutzung des betrieblichen E-Mail-Systems zu verfahren? Besonders großen Raum nehmen Regelungen ein, die bestimmen, wie in Abwesenheit von Beschäftigten mit eingehenden Mails umgegangen wird.

2.4.1 Rechtliche Hinweise

Viele Vereinbarungen, insbesondere Dienstvereinbarungen aus dem öffentlichen Dienst, legen die eingeschränkte rechtliche Bedeutung von E-Mails klar dar. Die Regelungen zur Rechtswirkung beziehen sich einerseits auf das Außenverhältnis zu Kunden und Bürgern (in öffentlichen Verwaltungen), andererseits auf die interne Kommunikation zwischen Arbeitgeber und Arbeitnehmer.
Zudem gelten E-Mails rechtlich auch ohne digitale Signatur (→ Glossar) als verbindliche Willenserklärung und sind dementsprechend zu behandeln. Beide Punkte greift die folgende Vereinbarung auf.

> »Elektronische Nachrichten können Willenserklärungen darstellen und entsprechende Rechtsfolgen auslösen. Werden sie als Verwaltungsakt oder Rechtsgeschäft erstellt, unterliegen sie entsprechenden Formvorschriften wie z. B. der Schriftform, die derzeit noch eine eigenhändige Unterschrift erfordert. Dieses Erfordernis kann mittels elektronischer Post per E-Mail zurzeit nicht erfüllt werden, ein Formmangel wäre ggf. die Folge. Der Gesetzgeber prüft derzeit die Einführung einer digitalen Signatur. Bis zur rechtlichen Klarstellung können deshalb Erklärungen, die einer besonderen Form bedürfen, nicht per elektronische Post abgegeben werden.«
>
> Öffentliche Verwaltung, 090201/508/2010

Dies bedeutet, dass bis auf Weiteres alle rechtsverbindlichen Daten, die über das E-Mail-System versandt werden, entweder nur oder zusätzlich über den normalen Postweg verschickt werden müssen.
Eine weitere wichtige Vorschrift betrifft die Archivierung. Hier ist zu regeln, unter welchen Umständen ein Zugriff auf das Archiv erfolgen darf.

> »Die Archivierung der E-Mails der Mitarbeiter dient ausschließlich dazu, den gesetzlichen Archivierungsvorschriften aus HGB [Handelsgesetzbuch] und AO [Abgabenordnung] nachzukommen. Ein Zugriff auf das Archiv für sämtliche anderen Zwecke ist ausgeschlossen. Eine Ausnahme gilt nur für Zugriffe von Strafverfolgungsbehörden oder auf Basis eines gerichtlichen Urteils.«
>
> Verlags- und Druckgewerbe, 090300/196/2010

Beschäftigte müssen wissen, für welche Vorgänge welche Vorschriften gelten. Darauf weisen diese Regelungen hin.

> »Gehen rechtserhebliche Erklärungen, die besonderen Formvorschriften unterliegen (z. B. Widerspruch), per elektronische Post ein, ist die zuständige Stelle verpflichtet, den Absender unverzüglich auf den Formmangel und die Folgen hinzuweisen.«
>
> Öffentliche Verwaltung, 090201/508/2010

> »Die Grundsätze einer ordnungsgemäßen Aktenführung gelten sinngemäß auch für ein- und ausgehende elektronische Dokumente. Werden zu einem Vorgang Papierakten geführt, sind die elektronischen Dokumente – soweit diese als geschäftskritisch anzusehen sind – auszudrucken und zu den jeweiligen Akten zu nehmen. Bei digitaler Aktenverwaltung, z. B. DMS [Dokumenten-Management-System], sind die Dokumente digital abzulegen.«
>
> Öffentliche Verwaltung, 090300/274/2012

> »Absender und Empfänger von E-Mails sind allein für deren weitere Verwendung verantwortlich. Sie entscheiden über Speicherung, Löschung und Weiterleitung im Rahmen der gesetzlichen und betrieblichen Regelungen.«
>
> Ernährungsgewerbe, 090300/174/2008

Wie die Kommunikation per Mail zwischen Arbeitnehmer und Arbeitgeber geregelt ist, beschreibt diese Vereinbarung.

> »Über die elektronischen Kommunikationssysteme werden keine individuellen Dienstanweisungen oder disziplinarischen Mitteilungen übermittelt. Vertrauliche Mitteilungen werden hinreichend sicher verschlüsselt.«
>
> Bildungseinrichtung, 090300/154/2006

2.4.2 Vergabe von Postfächern und E-Mail-Adressen

Im Vergleich zur letzten Auswertung zeigen die neueren Vereinbarungen, dass keine Frage mehr darin besteht, ob Beschäftigte einen E-Mail-Zugang bekommen oder nicht. Die Vergabe des Postfachs erfolgt praktisch mit der Einstellung.

> »Um die Teilnahme an der internen und externen Kommunikation sicherzustellen, stellt der Verlag allen Beschäftigten einen dienstlichen E-Mail-Zugang (personalisierte E-Mail-Adresse) und einen Internetzugang zur Verfügung.«
>
> Verlags- und Druckgewerbe, 090300/315/0

Die Postfächer sind häufig nicht nur von bestimmten Arbeitsplätzen aus nutzbar, sondern unabhängig davon erreichbar, wo Beschäftigte gerade arbeiten.

> »Interne Kommunikationsfunktionen wie z. B. elektronische Post werden so eingerichtet, dass sie von allen EDV-unterstützten Arbeitsplätzen aus genutzt werden können.«
>
> Grundstücks- und Wohnungswesen, 090201/292/2006

Ob die Adresse funktionsbezogen oder persönlich ist, wird von den betrieblichen Erfordernissen abhängig gemacht.

> »Es existieren nicht personalisierte E-Mail-Accounts und -adressen, z. B. für den Vertrieb, auf die mehrere Personen Zugriff haben. Externer E-Mail-Versand und Zugriff auf das Internet ist nur personenbezogenen Benutzern gestattet.«
>
> Elektro, 090300/185/2010

Sowohl Unternehmen als auch Verwaltungen haben Interesse an einem einheitlichen Auftritt nach außen. Deswegen folgen E-Mail-Adressen einheitlichen Schemata.

> »Alle Beschäftigten, die über einen an der städtischen Netzinfrastruktur angebundenen PC-Arbeitsplatz verfügen, erhalten eine E-Mail-

Adresse. Diese Adresse ist grundsätzlich nach folgendem Schema aufgebaut: Vorname.Familienname@stadt-[...].de bzw. Organisationseinheit@stadt-[...].de.«

Öffentliche Verwaltung, 090201/508/2010

2.4.3 Private Nutzung der E-Mails

Die Tendenz bezüglich der privaten Nutzung ist in den neueren Vereinbarungen die gleiche wie bereits in Kapitel 2.1.12 beschrieben: Die Spielräume für die Privatnutzung werden kleiner. In einigen Vereinbarungen ist zudem nicht die Rede von einem grundsätzlichen Verbot, das Ausnahmen zuließe, sondern die Formulierungen lassen keinen Zweifel daran, dass die private E-Mail-Nutzung untersagt ist.
Für die Privatnutzung wird häufig auf so genannte Webmailer verwiesen. In einigen Betrieben ist aber auch deren Nutzung verboten. Zudem schreiben viele Regelungen vor, dass den Absendern von privaten Mails an Beschäftigte mitgeteilt werden muss, dies in Zukunft zu unterlassen. Das folgende Beispiel führt alle genannten Punkte auf.

»Das Mailsystem steht ausschließlich für dienstliche Zwecke zur Verfügung. Private Mails dürfen nicht gesendet werden. Da der Empfang privater Mails technisch nicht unterbunden werden kann, sind versehentlich empfangene private Mails sofort zu löschen. Der Absender ist darauf hinzuweisen, den Versand von privaten Mails an die Firmen-Mailadresse künftig zu unterlassen. Für das Senden und Empfangen von privaten Mails kann im Sinne der Absätze 2 und 3 auf Webmaildienste (z. B. gmail.com, web.de, gmx.de) zugegriffen werden.«

Bekleidungsgewerbe, 090300/317/0

Auch die Kontrolle der Bestimmungen ist in einigen Vereinbarungen geregelt.

»Die [Firma] wird in Abstimmung mit dem Personalrat und dem Datenschutzbeauftragten in regelmäßigen Abständen die Einhaltung des Verbots der privaten Nutzung in Stichproben kontrollieren.«

Kreditgewerbe, 090201/385/2009

Wo private Mails über das Firmensystem geschickt oder empfangen werden, gibt es häufig Vorschriften zur besonderen Kennzeichnung oder Speicherung in separaten Ordnern. Dies dient unter anderem dazu, die Einsicht in Postfächer zu regeln oder die Archivierung. Die privaten Mails könnten dann ausgespart werden, um den gesetzlichen Vorschriften aus dem TKG zu entsprechen (ausführlich dazu vgl. Kap. 6.3.).

»Über den Mail-Server der [Firma] versandte oder empfangene private Mails sind als solche durch den Beschäftigten eindeutig zu kennzeichnen (z. B. durch Ablage in gesondertem Mailordner ›privat‹).«

Gesundheit und Soziales, 090201/400/2010

Speziell dieser Arbeitgeber sichert sich trotzdem den Zugriff. In der Einwilligungserklärung zur privaten Nutzung stimmen die Beschäftigten einer möglichen Kontrolle der privaten Mails zu.

»Durch die private Nutzung des Internetzugangs und der freigegebenen Datenschnittstellen erklärt der Beschäftigte seine Einwilligung in die Protokollierung und Kontrolle [...] für den Bereich der privaten Nutzung.«

Gesundheit und Soziales, 090201/400/2010

Einige Regelungen greifen die schwierige Trennbarkeit von privater und geschäftlicher bzw. dienstlicher E-Mail-Nutzung auf. Sie stellen fest, dass es häufig außerhalb des Einflusses von Beschäftigen liegt, wer ihnen Mails welchen Inhalts schickt. Die nachstehende Vereinbarung erlaubt die gelegentliche private E-Mail-Nutzung.

»Beiden Parteien ist bewusst, dass sich eine ausschließlich geschäftliche und persönliche Nutzung nicht scharf trennen lassen. Daher wird gewährleistet, dass eine gelegentliche persönliche Nutzung der E-Mails für die Mitarbeiter/-innen keine arbeitsrechtlichen oder disziplinarischen Maßnahmen zur Folge haben wird, sofern dadurch der betriebliche Ablauf nicht gestört wird und keine zusätzlichen Kosten entstehen.«

Tankstellen, Kfz.-Reparatur und -Handel, 090300/162/2009

Nur wenige Vereinbarungen formulieren eine Zulässigkeit der privaten Nutzung mit definierten Ausnahmen, wie z. B. der Weiterleitung privater Anhänge. Ein weitaus größerer Teil erlaubt die Nutzung außerhalb der Arbeitszeit.

> »Die gelegentliche Nutzung zu privaten Zwecken in den Pausenzeiten wird gestattet, sofern die betrieblichen Interessen nicht gestört werden und keine zusätzlichen Kosten entstehen.«
>
> Metallverarbeitung, 090300/271/2008

2.4.4 (Arbeits-)Organisation bei E-Mail-Nutzung, Ablage/ Löschen von E-Mails, Vertretung

Die Regelungen zum Umgang mit E-Mails nehmen großen Raum in den Vereinbarungen ein. Häufig geht es darum, den rechtskonformen Zugriff auf das Postfach abwesender Mitarbeiterinnen und Mitarbeiter zu regeln, um etwa sicherzustellen, dass die elektronische Post auch dann zeitnah bearbeitet wird, wenn Beschäftigte krank oder im Urlaub sind. Wie diese Regelungen abgefasst sind, steht in Zusammenhang mit den Vorgaben zu privaten Mails (vgl. Kap. 6.3).
Die Ausführlichkeit der Regelungen verdeutlicht den Stellenwert, den E-Mails in der Kommunikation von Behörden und Unternehmen nach außen haben.
Festgelegt werden beispielsweise Formalitäten im Umgang mit E-Mails, unter anderem die Signatur. Diesbezüglich wird häufig bestimmt, dass sie bei dienstlichen Mails Pflicht ist und welche Daten sie enthalten soll. Meist sind die Beschäftigten für ihre Einrichtung selbst verantwortlich, nur ausnahmsweise stellt der Arbeitgeber sie zur Verfügung. Weitere formale Vorschriften betreffen etwa den Betreff (er soll aussagekräftig sein) und die Anrede (die jener im Schriftverkehr gleichen soll). Erstaunlicherweise wird lediglich in einer der vorliegenden Vereinbarungen auf die DIN 5008 verwiesen, die die Gestaltung von E-Mails normiert und beispielsweise Vorgaben zum Umgang mit der Betreffzeile enthält (vgl. Lochmann 2011).
Zu den verwendeten Formaten wird beispielsweise vorgeschrieben, dass Mails im »nur Text«-Format gesendet werden sollen, weil nur so eine

einheitliche, plattformunabhängige Darstellung gewährleistet werden kann. Die fehlenden Standards im Netz sind auch der Grund für die Regelung, dass Sendebestätigungen nicht verwendet werden sollen. Auch das Format von Anhängen wird in diesem Zusammenhang festgelegt: Sie sollen in der Regel eine bestimmte Größe nicht überschreiten und schreibgeschützt versendet werden.
Des Weiteren wird in vielen Vereinbarungen der Umgang mit falsch adressierten Mails festgelegt. Hier wird beispielsweise bestimmt, wer in einem solchen Fall zu benachrichtigen ist.
Ebenso wird die Ablage von Mails geregelt: Was wird in welchem Ordner abgelegt? Wie groß sind die Postfächer? Wann sollen E-Mails gelöscht werden?

> »Nach Kenntnisnahme der E-Mail entscheiden die Benutzer eigenverantwortlich über die Löschung, Weiterleitung oder Archivierung unter Berücksichtigung der betrieblichen Anforderungen. Die Benutzer sind zuständig für die regelmäßige Bereinigung von gespeicherten E-Mails und Anhängen.«
>
> Verlags- und Druckgewerbe, 090300/272/2005

Besonders wichtig für Beschäftigte sind die Vorschriften dazu, wie oft der Posteingang geprüft und wie schnell auf eingehende Post reagiert werden muss. Häufig ist eine tägliche Durchsicht und Bearbeitung vorgesehen. Andere Formulierungen verlangen, dass das Postfach laufend kontrolliert wird und eingehende Mails so schnell wie möglich oder sogar unverzüglich bearbeitet werden.
Wie der E-Mail-Dienst in der internen Arbeitsorganisation eingesetzt wird, legt folgende Vereinbarung fest.

> »Der Empfänger (bei mehreren Empfängern der zuerst aufgeführte Empfänger) einer externen projektbezogenen E-Mail hat diese im hierfür gültigen elektronischen Projektordner nach den gültigen Regeln [...] abzulegen.«
>
> Gummi- und Kunststoffherstellung, 090201/463/2010

Laut nachstehender Vereinbarung sollen elektronische Medien gute Arbeit unterstützen; Abläufe sollten sich nicht nach der Technik richten,

sondern umgekehrt. Diese Forderung stellt durchaus eine Ausnahme in den vorliegenden Regelungen dar.

> »Die Ablauforganisation der Arbeit, insbesondere das damit verbundene Mail-Routing, wird vor Einführung des Systems mit den betroffenen Beschäftigten ausführlich erörtert. Es gilt der Grundsatz, dass die zurzeit bestehenden Arbeitsabläufe im System abgebildet werden. Arbeitsabläufe sollen dabei so gestaltet werden, dass sie den Beschäftigten ein möglichst selbstbestimmtes Arbeiten ermöglichen.«
>
> Anonym, 090300/148/0

Fast alle Vereinbarungen legen das Verfahren im Umgang mit E-Mails fest, wenn Beschäftigte abwesend sind. Die meisten sehen vor, dass ein Abwesenheitsassistent aktiviert werden muss, wenn beispielsweise Urlaub geplant ist. In der Regel sollen eingehende Mails zusätzlich an Vertreterinnen und Vertreter weitergeleitet werden. Diese Details überlassen die folgenden Vereinbarungen den Beschäftigten selbst.

> »Grundsätzlich kann der Mitarbeiter selbst eine so genannte Benutzerfreigabe für seinen Stellvertreter einrichten, einen Abwesenheitsassistenten ausführen oder eine automatische Weiterleitung veranlassen. Die Benutzerfreigabe ist zu bevorzugen.«
>
> Nachrichtentechnik/Unterhaltungs-, Automobilelektronik, 090300/241/2011

> »Im Sinne eines geregelten Betriebsablaufs ist der Beschäftigte verpflichtet, im Falle einer geplanten ganz-/mehrtägigen Abwesenheit den Abwesenheitsassistenten zu aktivieren. Dabei ist unter Berücksichtigung des Postgeheimnisses die Weiterleitung an eine Vertretung nicht zwingend erforderlich. Es muss dann jedoch im Abwesenheitsassistenten auf die Nichtweiterleitung hingewiesen werden.«
>
> Grundstücks- und Wohnungswesen, 090300/205/2009

Komplizierter wird es, wenn die Abwesenheit nicht geplant ist. Die folgende Vereinbarung sieht die Zustimmung des Betriebsrates vor, bevor das Postfach der Abwesenden eingesehen werden darf.

»Zugriffsrechte in besonderen Fällen: Bei Abwesenheit des Mitarbeiters darf ein Zugriff auf dessen Benutzerkonto ohne dessen Zustimmung nur erfolgen, wenn der Betriebsrat sein Einverständnis im Voraus erklärt hat. Der Betriebsrat und der Datenschutzbeauftragte sind bei jeder Überprüfung berechtigt, anwesend zu sein. Ein Zugriff auf dessen E-Mail-Konto darf ohne dessen Zustimmung nur erfolgen, wenn der Betriebsrat sein Einverständnis im Voraus erklärt hat. Die beteiligten Personen sind zur absoluten Verschwiegenheit verpflichtet. Der Betriebsrat und der Datenschutzbeauftragte sind bei jeder Überprüfung berechtigt, anwesend zu sein. Der Mitarbeiter ist verpflichtet, private Mails/Dateien nach Feststellung des Posteingangs getrennt von geschäftlichen zu speichern. Scheidet er aus dem Unternehmen aus, hat er diese Mails/Dateien zu löschen.«

Mess-, Steuer- und Regelungstechnik, 090300/158/2009

2.4.5 Adressbücher und Verteilerlisten

Die Frage, wer berechtigt ist, E-Mails an alle Beschäftigten im Unternehmen zu senden, wird in den neueren Vereinbarungen weniger häufig geregelt. Bestimmungen wie die folgende stellen eher eine Ausnahme im ausgewerteten Material dar.

»So genannte Verteilerlisten, z. B. ›Alle Outlookbenutzer‹, dürfen nur von Abteilungs-/Teamleitern der IT, Vorstand und Geschäftsleitung sowie vom BR verwendet werden.«

Bekleidungsgewerbe, 090300/317/0

Möglicherweise ist die abnehmende Regelung dieser Frage ein Hinweis darauf, dass die E-Mail-Nutzung soweit alltäglich geworden ist und gut funktioniert, dass keine besonderen Vereinbarungen dazu mehr notwendig sind. Oder es wird von Beschäftigten inzwischen erwartet, dass sie eigene Strategien entwickelt haben, um hohes E-Mail-Aufkommen zu bewältigen.
Die Weitergabe und das Zugänglichmachen von Adressbüchern werden durch die nachstehende Formulierung geregelt.

»In elektronischen Adressbüchern werden u. a. personenbezogene Arbeitnehmer-Daten gespeichert, die im Rahmen des Informationsaustauschs auch Dritten, z. B. anderen Konzerngesellschaften, zur Verfügung gestellt werden dürfen.«

Mess-, Steuer- und Regelungstechnik, 090300/212/2010

Solche Regelungen sind bei der Nutzung interner sozialer Medien besonders relevant, etwa wenn die im Outlook-Adressbuch eingegebenen Daten in Mitarbeiterprofile übernommen werden.

2.4.6 Sicherheitsstandards, Umgang mit sensiblen Daten, Datenschutz

Die Sicherheit im E-Mail-Verkehr spielt in den Regelungen in mehrfacher Hinsicht eine bedeutende Rolle: Vertrauliche Daten – seien es personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter, der Kundschaft oder geheim zu haltende betriebliche Daten – dürfen nicht oder nur unter hohen Auflagen per E-Mail versendet werden. Die Verschlüsselung von E-Mails wird einerseits gefordert, um dem »Postkarten-Charakter« der elektronischen Post zu entgehen; andererseits wird sie untersagt, damit die Inhalte der E-Mails überprüfbar bleiben.
Regelungen zu den Anlagen eingehender E-Mails versuchen, das Virenrisiko zu minimieren.
In den neueren Vereinbarungen spielt auch der Umgang mit unerwünschten Werbemails (Spam) eine Rolle, die ähnlich wie virenbehaftete E-Mails häufig bereits aussortiert werden, bevor sie im Postfach des bzw. der Beschäftigten ankommen. Das Aufkommen von Spam-Mails hat offenbar Ausmaße erreicht, die das Funktionieren der E-Mail-Systeme gefährden.
Der Umgang mit als solchen identifizierten Werbemails unterscheidet sich beispielsweise dadurch, ob den Beschäftigten eine Benachrichtigung hierüber zugeht oder nicht. Die Bandbreite liegt zwischen sofortiger Löschung ohne Information der Beschäftigten und dem Zwischenspeichern für einen bestimmten Zeitraum, so dass die Empfänger der Mails noch die Möglichkeit haben, eventuell fälschlich als Spam erkannte Mails zu sichern.
Die Regelungen zur Verringerung des Virenrisikos verlangen Beschäf-

tigten zum Teil eine hohe (Medien-)Kompetenz ab: Sie sollen einschätzen können, von welchen Mails eine konkrete Gefährdung ausgeht.

> »Wenn Sie E-Mails erhalten, deren Inhalt auf Viren schließen lässt, melden Sie dies bitte unverzüglich IS. Öffnen Sie auf keinen Fall Anlagen solcher E-Mails.«
>
> Metallverarbeitung, 010502/67/2000

So und ähnlich wird in vielen Vereinbarungen festgelegt, wie den Anforderungen des Datenschutzes und der Wahrung von Geschäfts- und Betriebsgeheimnissen entsprochen wird.

> »Der Versand von personenbezogenen Daten oder vertraulichen Informationen, die per E-Mail außerhalb des Lotus-Notes-Verbundes über das Internet übertragen werden, ist nur dann gestattet, wenn die Vertraulichkeit der Daten oder Informationen bei der Übertragung durch entsprechende technische Verfahren, z. B. eine geeignete Verschlüsselungsmethode, gewährleistet ist. Dies gilt für den E-Mail-Text und ggf. beigefügte Anlagen.«
>
> Kreditgewerbe, 090201/385/2009

In anderen Betrieben derselben Branche ist die Verschlüsselung ausgeschlossen.

> »Generell sind alle E-Mails unverschlüsselt zu versenden. Eine Verschlüsselung ist nur in Ausnahmefällen an Benutzer innerhalb des E-Mail-Netzwerkes der [Firma] zulässig; hierzu zählen vertrauliche E-Mails, die ausschließlich für den Empfänger, nicht aber durch den Vertreter lesbar sein sollen (E-Mails mit vertraulichen Inhalten, z. B. Personal, Betriebsrat). Externe E-Mails dürfen generell nicht verschlüsselt werden, da sonst eine ordnungsgemäße, automatische Speicherung und spätere Recherche nicht möglich sind.«
>
> Kreditgewerbe, 090300/172/2009

Die folgende Vereinbarung deutet darauf hin, dass zur Gewährleistung eines sicheren und vertrauensvollen Umgangs mit E-Mails eine Sensibilisierung notwendig ist.

»Vertrauliche Daten von Kunden dürfen nicht aktiv unter Einbindung der E-Mail-Kommunikation angefordert werden. Die Adressaten der [...] versandten E-Mails sind darauf hinzuweisen, dass eine Rückmeldung mit personenbezogenen Daten oder vertraulichen Informationen zur Gewährleistung der Datensicherheit nicht mittels E-Mail erfolgen darf.«

Kreditgewerbe, 090201/385/2009

3. Mitbestimmungsrechte, -prozeduren und -instrumente

Dieses Kapitel zeigt auf, welche Regelungen die betrieblichen Verhandlungspartner ergänzend zu den gesetzlichen Informations-, Beratungs- und Mitbestimmungsrechten der Arbeitnehmervertretungen treffen.
Grundsätzlich sind hinsichtlich der institutionellen Mitbestimmung in Bezug auf Internet, Intranet und E-Mail keine wesentlichen Änderungen gegenüber der früheren Auswertung festzustellen. Die Möglichkeiten seitens der Interessenvertretungen, die Internetdienste zu nutzen, wurden in den neueren Vereinbarungen etwas häufiger und differenzierter geregelt.

3.1 Institutionelle Mitbestimmung des Betriebs- oder Personalrates

Grundlage für seine Beratungs- und Mitbestimmungsmöglichkeiten ist für den Betriebs- bzw. Personalrat, dass er rechtzeitig und umfassend durch den Arbeitgeber informiert wird. Die Unschärfe der Begriffe »rechtzeitig« und »umfassend« führt regelmäßig dazu, dass die Vereinbarungen sie genauer definieren; zudem definieren einige Vereinbarungen die Begriffe »verständlich« und »angemessen«. Entsprechende Formulierungen finden sich auf der beigefügten CD-ROM bzw. in der Online-Datenbank im Internet.
Einige betriebliche Partner vereinbaren regelmäßige Sitzungen, in denen der Betriebs- bzw. Personalrat vom Arbeitgeber frühzeitig und umfassend informiert werden soll, z. B. über Planungen und Weiterentwicklungen der technischen Systeme und ihre betriebliche Anwendung. Nur wenige Vereinbarungen berücksichtigen, dass auch der betriebliche Datenschutzbeauftragte diese Informationen bekommen und eventuell

zu den Sitzungen eingeladen werden sollte. Ein Beispiel dazu aus einer Dienstvereinbarung, die die Mitarbeitervertretung einer diakonischen Pflegeeinrichtung abgeschlossen hat.

> »Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden vorab mit der MAV [Mitarbeitervertretung] vereinbart, ebenso werden sie dem betrieblich Beauftragten für den Datenschutz mitgeteilt.«
>
> Gesundheit und Soziales, 090201/400/2010

Erst nach einer Informationsvermittlung ist für die Arbeitnehmervertretung feststellbar, ob Beratungs- oder Mitbestimmungsrechte ableitbar sind. Dies berücksichtigt beispielsweise die folgende Regelung.

> »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.«
>
> Ernährungsgewerbe, 090300/174/2008

Die Vereinbarungen enthalten oft Regelungen zu Informations- oder Beratungsrechten, jedoch keine Regelungen zu weiterreichenden Mitbestimmungsrechten.

> »Der Betriebsrat wird, mindestens einmal jährlich, über geplante Neuerungen bzw. Änderungen der Funktionen hinsichtlich der E-Mail, des Intranets und des Internets informiert.«
>
> Fahrzeughersteller sonstiger Fahrzeuge, 090300/179/2010

> »Dabei werden vor allem die möglichen Auswirkungen auf Arbeitsplätze, Arbeitskräfteeinsatz, Arbeitsbedingungen und Qualifikationsanforderungen beraten.«
>
> Grundstücks- und Wohnungswesen, 090201/292/2006

Die Formulierungen zu den Beratungsrechten wiederholen regelmäßig nur die gesetzlichen Rechte gemäß § 90 Abs. 2 BetrVG.

Mitbestimmungsrechte

Einige Vereinbarungen und Richtlinien heben die Mitbestimmungsrechte des Betriebsrats besonders hervor. Sie werden überwiegend analog zur gesetzlichen Regelung festgeschrieben (vgl. Kap. 6.3). Demnach unterliegt jede Änderung, Ergänzung und Erweiterung von Internetdiensten, Software und Protokollierung der Mitbestimmung.

> »Änderungen der Leistungsmerkmale des Internet-Zugriffs oder der Hard- und Software der Firewall und der Proxyserver sowie der dort gespeicherten Daten bedürfen der vorherigen Zustimmung durch den Gesamtbetriebsrat.«
>
> Baugewerbe, 090300/187/2008

Teilweise wird die Mitbestimmung begrenzt auf Systemerweiterungen, die eine Änderung in den Anlagen zur Betriebs- oder Dienstvereinbarung zur Folge haben. Das folgende Beispiel formuliert, was nicht zustimmungsbedürftig ist.

> »Systemveränderungen oder -erweiterungen, die im Rahmen einer normalen technischen Fortentwicklung erforderlich sind, bedürfen nicht der vorherigen Zustimmung des Betriebsrats.
>
> Anonym, 090300/156/2002

Einzelne neuere Vereinbarungen regeln ein Verfahren, nach dem über die Mitbestimmung der Arbeitnehmervertretung entschieden werden soll. Das folgende Beispiel gibt beiden Vertragspartnern das Recht, Mitbestimmungsverhandlungen einzuleiten.

> »Beide Seiten prüfen dabei, ob durch die geplante Änderung die Bestimmungen dieser Vereinbarung eingehalten bleiben. Ist dies nach Auffassung einer Seite nicht der Fall, so werden Verhandlungen um eine diese Vereinbarung ergänzende Regelung aufgenommen. Gleiches gilt, wenn eine Seite geltend macht, dass durch zwischenzeitlich geänderten Umgang mit den Systemen die Bestimmungen dieser

Vereinbarung verletzt sind oder sich neuer Regelungsbedarf im Sinne des §87 Abs. 1 Nr. 6 BetrVG (Schutz vor Überwachung) ergeben hat.«

Versicherungsgewerbe, 090300/206/2007

Missbrauch

Die meisten Vereinbarungen beziehen den Betriebs- bzw. Personalrat ein, wenn Missbrauchs- oder Verdachtsfälle zu bearbeiten sind. Diese Einbindung beginnt bei der Übermittlung aktueller Informationen über Missbrauchsfälle und geplanten Gegenmaßnahmen. Die folgende Regelung verlangt zudem, dass die Informationen an Geschäftsführung und Betriebsrat gleichzeitig übermittelt werden.

»Bei begründetem Verdacht des Missbrauchs der Nutzung der elektronischen Kommunikationsdienste durch einen Mitarbeiter ist der Betriebsrat umgehend, zu gleicher Zeit, in gleicher Art und ebenso umfänglich wie die Geschäftsleitung zu informieren. Die Missbrauchskontrolle bedarf der vorherigen Zustimmung und Beteiligung des Betriebsrats.«

Gesundheit und Soziales, 090300/157/2005

Regelmäßig wird eine uneingeschränkte Einsichtnahme in die Protokollierungsdateien und deren Auswertung zugestanden. Die Auswertung wird meist mit dem betrieblichen Datenschutzbeauftragten, dem Systemadministrator oder der Geschäftsleitung gemeinsam durchgeführt. Einige Vereinbarungen regeln zusätzlich, dass die Auswertung von Protokollen im Fall des Missbrauchsverdachts der Mitbestimmung unterliegt. Eine wichtige Aufgabe der Arbeitnehmervertretung ist es, die Beschäftigten vor ungerechtfertigten Anschuldigungen und Generalverdacht zu schützen. Dies drückt die folgende Regelung deutlich aus.

»Im Falle des Missbrauchsverdachts ist darauf zu achten, dass der betroffene Mitarbeiter vor Fehlinterpretationen und ungerechtfertigten Konsequenzen geschützt ist. Der Mitarbeiter und ein Vertreter des Betriebsrates sind im Verdachtsfall bei der Sichtung der Daten hinzuzuziehen.«

Kreditgewerbe, 090300/171/2009

Kontrollrechte

Betriebs- und Personalräte können auf Basis der Vereinbarungen in den meisten Fällen jederzeit unangemeldete Kontrollen durchführen. Dazu haben sie Einblick in alle betreffenden Systeme, Daten und Logprotokolle sowie in alle Unterlagen, und sie erhalten Zugang zu allen Räumen. Die sachkundigen Beschäftigten – in der Regel sind dies Netzwerk- und Systemadministratoren – sind zur Auskunft verpflichtet.

> »Der Betriebsrat kann die Einhaltung dieser Betriebsvereinbarung jederzeit überprüfen. Hierzu können System-Protokolle, Konfigurationen und andere Informationsdokumente vom Betriebsrat angefordert werden. IuK-Systeme werden im Betrieb vorgeführt und erläutert.«
>
> Versicherungsgewerbe, 090201/504/2011

Vergleichbare Regelungen finden sich üblicherweise in den IKT-Rahmenvereinbarungen.

Auskunftspersonen und Sachverständige

Einige Vereinbarungen regeln darüber hinaus die Hinzuziehung externer Sachverständiger durch den Betriebs- bzw. Personalrat. Teilweise sind die Formulierungen so unkonkret, dass offen bleibt, ob ein interner oder externer Sachverständiger konsultiert werden soll (»Sachverständige seiner Wahl«). Externe Sachverständige sollen überwiegend zur Kontrolle hinzugezogen oder von der Arbeitnehmervertretung mit der Kontrolle beauftragt werden können.

> »Zur Überprüfung kann der Gesamtbetriebsrat jederzeit vor Ort die Einhaltung der Datenverarbeitung und Speicherung (Archivierung und Protokollierung) personenbezogener Daten kontrollieren. Sollten die Sachkenntnisse des Gesamtbetriebsrates nicht ausreichen, um die Informationen zu verstehen, ist er berechtigt, jederzeit einen Sachverständigen seiner Wahl hinzuzuziehen.«
>
> Grosshandel (ohne Kfz.), 090300/159/2009

Ausführlichere Regelungen zu den Informations-, Beratungs- und Mitbestimmungsrechten der Arbeitnehmervertretungen finden Sie auf der beigefügten CD-ROM bzw. in der Online-Datenbank im Internet.

3.2 Nutzung von Internet, Intranet und E-Mail durch die Interessenvertretung

Zum Internet-, Intranet- und/oder E-Mail-Zugang für Arbeitnehmervertretungen äußert sich rund ein Fünftel der vorliegenden Vereinbarungen. Ausnahmslos erlauben sie den Gremien die Nutzung der E-Mail- und Internetdienste und des betrieblichen Intranets. In einem Fall wird jedoch dem Betriebsrat untersagt, eine eigene Internet-Homepage zu betreiben.

E-Mail und Internet

Es scheint inzwischen selbstverständlich zu sein, dass die Arbeitnehmervertreter die modernen Informations- und Kommunikationsmedien nutzen dürfen. Die juristischen Auseinandersetzungen der letzten Jahre zu diesen Themen dürften damit bald ganz der Vergangenheit angehören. Der folgende Text aus einer aktuellen Betriebsvereinbarung eines Klinik-Konzerns stellt die Rechtslage für alle Gremien und Ebenen exemplarisch dar.

> »Der Konzern- und Gesamtbetriebsrat sowie die örtlichen Betriebsräte haben das Recht, das Internet im Rahmen des üblichen Geschäftsbetriebes zu nutzen.«
>
> Gesundheit und Soziales, 090300/167/2010

Während viele Betriebs- und Personalräte eigene Internetauftritte betreiben, ist dies hier ausdrücklich untersagt.

> »Der Arbeitgeber stellt dem Betriebsrat zur ausschließlichen Erfüllung seiner gesetzlichen Aufgaben eine eigene E-Mail-Adresse zur Verfügung.
> Der Arbeitgeber gewährt dem Betriebsrat ausschließlich zur Erfüllung seiner gesetzlichen Aufgaben die Möglichkeit, das Internet zu nutzen, insbesondere um Informationen abzurufen. Der Betriebsrat ist jedoch nicht berechtigt, eine Homepage im Internet zu installieren.
> Eine weitere Nutzung der Kommunikationsmittel ist vorbehaltlich

der ausdrücklichen schriftlichen Zustimmung des Arbeitgebers ausgeschlossen.«

Wasserversorger, 090300/176/2010

Intranet

In Bezug auf das Intranet, mit dem die Arbeitnehmervertretungen die Beschäftigten informieren können, finden sich teilweise einschränkende Regelungen. Das folgende Zitat aus einer Betriebsvereinbarung formuliert dazu relativ ausführlich.

»Der Betriebsrat hat [...]
- das Recht auf Einrichtung einer eigenen Homepage im Intranet und einer eigenen E-Mail-Adresse,
- das Recht auf einen öffentlichen Ordner und auf Versendung von Rundmails an die Verteiler,
- Anspruch auf Unterstützung für diese Zwecke aus den zuständigen Abteilungen.

Zur Einrichtung einer eigenen Homepage nutzt der Betriebsrat die üblichen, für alle Arbeitsbereiche mit entsprechenden Befugnissen vom Arbeitgeber zur Verfügung gestellten technischen Einrichtungen und Verfahren. Die dazu erforderliche Hard- und Software wird dem Betriebsrat zur Verfügung gestellt.«

Verbände und Gewerkschaften, 090300/168/2007

Sonderschutz

Vereinbarungen, die die Nutzung der E-Mail- und Internetdienste durch die Arbeitnehmervertretungen und/oder deren Präsenz im Intranet regeln, verfügen teilweise einen besonderen Schutz der Daten von den Betriebs- bzw. Personalräten. Die folgende Regelung ist dafür beispielhaft. Sie bezieht zusätzlich alle anderen Personen und Gruppierungen ein, die per Gesetz einem besonderen Schutz unterliegen.

»Werksärzte, Psychologen, Suchtberater, Suchtkrankenhelfer, Sozialberater, Betriebsräte und Jugend- und Auszubildendenvertreter und andere Interessenvertreter der Belegschaft, Schwerbehindertenvertreter, Pressemitarbeiter und Rechtsanwälte sowie die im betrieblichen Datenschutz tätigen Personen und die bDSB [betrieblichen

Datenschutzbeauftragten] genießen einen Sonderschutz. Eine Liste der geschützten Personen wird durch die lokale Personalabteilung dem zuständigen Administrator zur Einrichtung und dem lokalen Betriebsrat zur Überprüfung der Einhaltung dieser Betriebsvereinbarung zur Verfügung gestellt. E-Mails, die an diesen Personenkreis gerichtet sind, unterliegen dem maximalen Schutz.«

Branchenübergreifend, 090300/188/2010

4. Offene Probleme

Einige ungelöste Probleme setzen sich über den gesamten Auswertungszeitraum fort – bei gleichzeitigem Wandel der Regelungen zu diesen Themen im Laufe der letzten zehn Jahre.

Private Nutzung der Internetdienste am Arbeitsplatz

Die früheren Auswertungen ergaben, dass klare Regelungen zur Privatnutzung fehlten. Diese Unklarheiten kommen in neueren Vereinbarungen kaum noch vor: Die Privatnutzung ist zentrales Regelungsthema geworden. Als Reaktion auf die Vorgaben des Telekommunikationsgesetzes und des Telemediengesetzes gehen immer mehr Arbeitgeber dazu über, die Beschäftigten, die die Internetdienste auch privat nutzen wollen, eine Einwilligungserklärung unterzeichnen zu lassen.

Diese Erklärungen gewähren dem Arbeitgeber jedoch oft weitgehende Rechte, etwa die Einsichtnahme in das Postfach oder die Protokolldaten. Dies stellt eine Einschränkung des Fernmeldegeheimnisses, eines Grundrechts, dar – der die Beschäftigten nicht zustimmen müssten. »Eine ausdrückliche Einwilligung in die Nutzung der betrieblichen Kommunikationsmittel zu privaten Zwecken ist nicht erforderlich: Auch eine konkludente Einwilligung ist ausreichend. Diese kann u. U. auch durch betriebliche Übung erfolgen.« (Simitis 2011, BDSG, Kommentar, § 32 Rn. 86)

Die Einwilligungserklärungen enthalten häufig auch Vorgaben zum Verhalten im Netz. Form und inhaltlicher Umfang der Erklärungen haben oft den Charakter von Dienstanweisungen.

Verantwortung des Einzelnen

Mit der Unterschrift unter die Einwilligungserklärung – oder deren Verweigerung – werden einige regelmäßig kollektiv geregelte Sachverhalte der individuellen Verantwortung übertragen. Das setzt medienkompe-

tente Arbeitnehmerinnen und Arbeitnehmer voraus, die wissen, was sie wollen und was sie tun.
Solche Verfahren unterlaufen den Schutzcharakter von Betriebsvereinbarungen und können allenfalls durch entsprechende Qualifikationsangebote ansatzweise ausgeglichen werden. Dies ist in den vorliegenden Vereinbarungen jedoch nicht oder nur unzureichend geregelt (vgl. Kap. 2.1.14).
Insgesamt vermittelt die Regelungspraxis den Eindruck, dass Arbeitgeber sich vermehrt gegen Fehlverhalten ihrer Beschäftigten absichern wollen (vgl. z. B. Kap. 2.1.3). Das betrifft sowohl Äußerungen im öffentlichen Netz als auch die Gefährdung des Unternehmensnetzes durch Viren oder Ähnliches.

Externe Dienstleister

Werden IT-Dienstleistungen outgesourct, befinden sich die personenbezogenen und -beziehbaren Daten der Beschäftigten, insbesondere sämtliche Protokolle, im Zugriff externer Administratoren. Dieser Zugriff auf Protokolldaten, die bei externen Dienstleistern gespeichert sind, ist nur vereinzelt und unzureichend geregelt. Die Arbeitnehmervertretung eines Unternehmens kann somit nicht kontrollieren, ob die vereinbarten Regeln eingehalten werden.

Geschützte dienstliche Kommunikation

Völlig unzureichend befassen sich die vorliegenden Vereinbarungen mit der dienstlichen Kommunikation aller Betriebsangehörigen, die per Gesetz einem besonderen Schutz unterliegen. Die Technologieberatungsstelle in Nordrhein-Westfalen weist in ihrer Handlungshilfe für Betriebsräte darauf hin: »Auch im dienstlichen E-Mail-Verkehr gibt es persönliche oder vertrauliche Mitteilungen, wie z. B. mit dem Betriebsrat/Personalrat, der Schwerbehindertenvertretung, dem betriebsärztlichen Dienst, dem betrieblichen Datenschutzbeauftragten, der Personalabteilung usw.« (vgl. Dietsch u. a. 2012, S. 21). Nur wenige Vereinbarungen weisen darauf hin und enthalten entsprechende Schutzregelungen.

Stellvertreterregelungen

Häufig wird Wert darauf gelegt, dass ein Zugriff auf die E-Mail-Postfächer bei Abwesenheit der Beschäftigten möglich ist, beispielsweise durch Stellvertreter. Das setzt wiederum konkrete Regelungen zur Privatnutzung und zur Stellvertretung voraus. Hier sind die Betriebspartner gefordert, das Interesse der Arbeitgeber nach Verfügbarkeit der Kundenkorrespondenz mit dem Fernmeldegeheimnis und weiteren Grundrechten der Arbeitnehmerinnen und Arbeitnehmer in Einklang zu bringen.

Gesundheitsschutz

Die aktuelle Nutzung der Internetdienste erzeugt neue Anforderungen an den betrieblichen Gesundheitsschutz, die in den vorliegenden Vereinbarungen nicht oder nur randständig behandelt werden. Der Umgang mit Beschleunigung, Arbeitsverdichtung und dem Aufweichen der Grenzen zwischen Beruflichem und Privatem erzeugt neue Belastungen und kann Beschäftigte überfordern. Neben diesen psychischen Belastungen gibt es körperliche, die mit dem Einsatz der Internetdienste einhergehen können: Mobile Geräte erfüllen in der Regel keine ergonomischen Standards, was auch für das Arbeiten unterwegs gilt. Hier geben Interessenvertretungen möglicherweise Gestaltungspotenzial aus der Hand – es sei denn, diese Aspekte werden in Vereinbarungen zu anderen Themen geregelt (vgl. Vogl/Nies 2013).

Mangelnde Aktualität der Vereinbarungen

Aktuelle Diskussionen in den Medien drehen sich vorrangig um fehlende Abgrenzung von Beruf und Freizeit, die psychischen Belastungen durch ständige Erreichbarkeit, aber auch um die Rechtssicherheit von E-Mails und um die sich ausweitende Nutzung sozialer Medien. Diese Themen behandeln die vorliegenden Vereinbarungen nur selten. Regelungen zur Begrenzung der Erreichbarkeit außerhalb der vertraglichen Arbeitszeiten finden sich nur vereinzelt. Die eng mit der technischen Entwicklung verwobene Problematik von Entgrenzung wird in den vorliegenden Vereinbarungen demnach nicht oder unzureichend bearbeitet.

Die bei Abschluss der vorliegenden Dienstvereinbarungen (immer) noch ungelöste Frage der digitalen Signatur zwingt die Verwaltungen

weiterhin dazu, die E-Mail-Kommunikation für formale Verwaltungsschreiben zu untersagen.
Wie die Regelung von Social Media – intern wie extern – sich in Bezug auf die existierenden Vereinbarungen zu E-Mail und Internet auf Dauer entwickeln wird, ist unklar. Obwohl die sozialen Medien ein Teil des Internets sind, werden sie häufig separat geregelt, was sicher den besonderen Rahmenbedingen der Nutzung – beispielsweise der schwierigen Kontrollierbarkeit – geschuldet ist.
Insgesamt scheinen sich die betrieblichen Partner mit aktuellen Fragen relativ spät zu befassen und die entsprechenden betrieblichen Antworten erst zeitverzögert in den Vereinbarungen festzuschreiben.

5. Zusammenfassende Bewertung

Diese Auswertung ist die dritte zum Thema E-Mail- und Internetnutzung innerhalb der letzten zehn Jahre. Damit wurden Vereinbarungen aus mehr als 15 Jahren betrachtet und deren Entwicklung verfolgt. Der betriebliche Umgang mit den Internetdiensten ist in diesem Zeitraum immer selbstverständlicher geworden und inzwischen wird ihr erfolgreicher Einsatz von den Betriebspartnern nahezu durchgehend als wesentlich für den geschäftlichen Erfolg von Unternehmen gesehen. Die E-Mail hat eine ungebrochen wichtige Bedeutung in der Kommunikation mit Kundinnen und Kunden, die Recherche im Internet ist für viele Beschäftigte Alltag.

Entsprechend weniger Raum nehmen Regelungen ein, die bestimmen, ob Beschäftigte die Internetdienste überhaupt nutzen dürfen; der Zugang zum Netz ist selbstverständlich.

Die in früheren Auswertungen festgestellten Unklarheiten – Wer darf das Netz wie nutzen? – kommen so in neueren Vereinbarungen kaum noch vor. Die Privatnutzung ist zentrales Regelungsthema: Der überwiegende Teil der Beschäftigten darf das Netz auch privat nutzen, der Anteil scheint jedoch leicht rückläufig zu sein. Häufig finden sich Regelungen, die die private Nutzung betrieblicher Internetdienste in der Freizeit und in den Pausenzeiten erlauben, nachdem die Beschäftigten eine Erklärung unterzeichnet haben, mit der datenschutzrechtliche Beschränkungen der Protokollierung und Auswertung für den Arbeitgeber aufgehoben werden.

Der Rahmen für die Netznutzung ist für die Beschäftigten somit klarer, aber auch enger geworden. Sie werden mehr in die Pflicht genommen. Das betrifft sowohl ihre Verantwortung für die sicherheitskritischen Aspekte der Internetnutzung als auch für die Organisation des Arbeitsplatzes, wo beispielsweise E-Mail-Weiterleitungen, automatische Abwesenheitsmeldungen etc. eingerichtet werden müssen.

In den Regelungen zur Protokollierung sowie zur Leistungs- und Ver-

haltenskontrolle gibt es keine wesentlichen Änderungen gegenüber der letzten Auswertung aus dem Jahr 2008. Leistungs- und Verhaltenskontrolle wird regelmäßig ausgeschlossen. Die Formulierungen zum Umgang mit den Protokolldateien lassen den Arbeitgebern allerdings große Spielräume, diese auszuwerten. Das Ziel ist immer, missbräuchlicher Nutzung der Internetdienste auf die Spur zu kommen. Die Rolle, die die Interessenvertretung dabei spielt – Wer darf unter welchen Umständen welche Protokolle einsehen? – ist unterschiedlich bedeutsam. Wie bereits in der letzten Auswertung festgestellt wurde, scheinen hier im Gegensatz zu anderen Vereinbarungen zur IuK-Technik, z. B. zu Personalinformationssystemen oder Arbeitszeiterfassungssystemen, die Grundsätze des Persönlichkeits- und Datenschutzes geringere Wertigkeit zu haben.

Lediglich eines der vorliegenden Dokumente nimmt die Ausspähskandale der jüngeren Vergangenheit zum Anlass, Prozesse zu definieren, die einen besseren Schutz der personenbezogenen Daten der Beschäftigten gewährleisten.

Die Bestimmungen zur Leistungs- und Verhaltenskontrolle werden neu betrachtet werden müssen, wenn interne Vernetzungstools (Social Media) verbreitet zum Einsatz kommen. Hier liegen in der Regel auch ohne direkte Protokollierungen Daten vor, die Aussagen über Leistung und Verhalten zulassen: Beispielsweise werden durch unternehmensöffentlich einsehbare Bewertungen und Empfehlungen – eigene oder die von Kolleginnen und Kollegen – das Verhalten und die Arbeitsweise der Beschäftigten transparent.

Häufig sind Regelungen anzutreffen, die einem Imageschaden für das Unternehmen vorbeugen sollen. Das Netz wird zunehmend als Ort wahrgenommen, in dem »Meinung« zum Unternehmen gemacht wird.

Trotz des Aufkommens anderer Kommunikationskanäle hat die E-Mail nach wie vor eine zentrale Bedeutung in der Behörden- und Unternehmenskommunikation. Darauf deuten sehr ausführliche Regelungen zu diesem Dienst aus der jüngsten Zeit hin.

Die Beschleunigung von Arbeitsprozessen durch die E-Mail-, Intranet- und Internetnutzung und damit die zunehmende Arbeitsverdichtung scheinen in den meisten Vereinbarungen als nicht zu ändernde Folgen der Netznutzung betrachtet zu werden. Nur selten sind Formulierungen

zu finden, die die Technik in den Dienst selbstbestimmter Arbeit stellen oder Fragen der Arbeitszeitgestaltung thematisieren. Neuere Fragestellungen zur betrieblichen Netznutzung werden in den vorliegenden Vereinbarungen nicht oder nur randständig behandelt. Das betrifft beispielsweise konkret die zunehmende mobile Nutzung des Netzes und allgemein die Entgrenzung von Arbeit.

6. Beratungs- und Gestaltungshinweise

Die aktuelle Auswertung von neueren Vereinbarungen und Richtlinien zur betrieblichen Nutzung von Internetdiensten ergab, dass sie – verglichen mit der Auswertung aus dem Jahr 2008 – in der Struktur weitestgehend gleich geblieben sind. Der Stichwortkatalog bietet eine Übersicht über die unterschiedlichen Gesichtspunkte bei der Regelung und Organisation der betrieblichen Nutzung von Internetdiensten. Es handelt sich dabei nicht um einen geschlossenen Gestaltungsvorschlag für eine Vereinbarung, sondern um Anregungen für eigene Überlegungen.

6.1 Gestaltungsraster

Ziele der Vereinbarung

- für das Unternehmen: betriebswirtschaftliche Aspekte, Steigerung der Wettbewerbsfähigkeit, Beschleunigung der Kommunikation (intern/extern), Sicherheitsaspekte, Schutz der betrieblichen Netze und Daten, Schutz des Unternehmens (Image)
- für die Beschäftigten: Schutz der Persönlichkeitsrechte, Gewährleistung des Gesundheits- und Arbeitsschutzes, Einbettung in die Arbeitsorganisation mit dem Ziel »gute Arbeit«, Zugang zum Netz für alle Beschäftigten, Gleichbehandlung
- übergreifend: Grundsätze zur Förderung elektronischer Kommunikation, Transparenz im Umgang mit Beschäftigtendaten, dynamischer Charakter der Internetdienste, verständliche und verbindliche Nutzungs- und Verfahrensregeln, Definition der Verantwortlichkeiten

Ziele der Nutzung von Internetdiensten

- Internet: einfachere Recherchen, schnellere Informationsbeschaffung, Darstellung des Unternehmens im Internet, größere Kunden- bzw. Bürgernähe, bessere strategische Positionierung des Unternehmens im Wettbewerb, eigenständige Beschaffung von Informationen durch die Beschäftigten
- Intranet: größere innerbetriebliche Transparenz, Abflachen von Hierarchien, zentraler Informationspool für Beschäftigte, kostengünstige Bereitstellung und Beschaffung interner Informationen, mehr Arbeitszufriedenheit durch Optimierung der Arbeitsabläufe
- E-Mail: Verbesserung des Informationsaustauschs mit Kunden und Geschäftspartnern, Verbesserung der internen und externen Zusammenarbeit, Rationalisierung

Risiken der Nutzung von Internetdiensten

mangelnde Vertraulichkeit beim Datenaustausch, nicht ausreichender Schutz personenbezogener und betrieblicher Daten, mögliche Angriffe oder Eindringen von außen, unbemerktes Einschleusen von Schadsoftware, Störung betrieblicher Rechnernetze, Verletzung von gesetzlichen Bestimmungen, z. B. von Lizenz-, Wiedergabe-, Eigentums- und Persönlichkeitsrechten

Sicherungsmaßnahmen, Verpflichtung und Verantwortung der Beschäftigten

- konzeptionell: Datenschutz- und Sicherheitskonzeption des Unternehmens
- operationell: konkrete technische Sicherungsmaßnahmen: Zugangsberechtigungen, Firewall, Einsatz von Filtersoftware für Internetseiten und Spam-E-Mail; Zugriffsprotokollierung; organisatorische Sicherungsmaßnahmen: Information, Einweisung, Support und Schulung der Beschäftigten, Verhaltensregelungen zum Umgang mit E-Mail, Internet und Intranet, Festlegen der (nicht) gestatteten Internetnutzung, Melden sicherheitsrelevanter Ereignisse

Systemadministration

allgemeine Rechte und Pflichten der Systemadministratoren, Qualifizierung der Systemadministratoren für die gesetzlichen Grundlagen ihrer

Arbeit, Verpflichtung der Systemadministratoren zur Einhaltung von Datenschutz und Fernmeldegeheimnis, Regelung der Einsicht in Protokolldaten, Protokollierung der Aktivitäten der Systemadministration, Kontrollrechte der Interessenvertretung

Datenschutz(-Beauftragte)

- Datenschutz-, Telekommunikations- und Telemediengesetz
- Einhaltung gesetzlicher Bestimmungen, technische und organisatorische Maßnahmen für Datenschutz, Zertifizierung der Datenschutzmaßnahmen
- betriebliche Datenschutzbeauftragte
- Datenschutzkonzept des Unternehmens, Zwecksetzung der Personaldatenverarbeitung, Datenminimierung und -askese, Dauer der Datenspeicherung, Berechtigungsprofile, Verwendung von Verschlüsselungstechniken und digitaler Signatur, Veröffentlichung von Mitarbeiter- und Kundendaten, Kontrollrechte der Interessenvertretung

Externe/Zugriff von außen

externe Systemadministration durch Fremdfirmen, Fernwartung, Vereinbarung mit Dritt-Unternehmen, Auftragsdatenverarbeitung, Protokollierung der Tätigkeiten und Zugriffe, Zugriffsmöglichkeiten für Beschäftigte aus Drittunternehmen, Kontrollrechte der Interessenvertretung

Protokollierung

Regeln der Protokollierung; Analyse der Protokolle von Benutzeraktivitäten; Festlegung der aktivierten Protokollfunktionen, grundsätzliche Regelungen zum Umgang mit Protokollen; Auswertung und Einsichtnahme, Einbeziehung und Kontrollrechte der Interessenvertretung

Aufbewahrung

Fristen, Ausnahmen, Löschen von (Protokoll-)Daten, Kontrollrechte der Interessenvertretung

Verhaltens- und Leistungskontrolle

Grundsätze gemäß § 87 Abs. 1 Nr. 6 BetrVG; grundsätzlicher Ausschluss von Verhaltens- und Leistungskontrolle der Beschäftigten durch die bei

der Nutzung von Internetdiensten anfallenden personenbezogenen Daten; Beweisverwertungsverbot; möglichst eindeutige Festlegung der Ausnahmen bzw. der Anlässe, die für bestimmte Personen eine Dateneinsicht und damit prinzipiell eine Leistungs- und Verhaltenskontrolle ermöglichen sowie Einbeziehung Datenschutzbeauftragter und der Interessenvertretung in diese Prozesse

Sanktionen

Definition von Missbrauchstatbeständen; Maßnahmen bei Verdacht auf Missbrauch oder nachgewiesenem Missbrauch

Private Nutzung der Internetdienste

grundsätzliches Verbot privater Nutzung oder grundsätzliche Zulässigkeit privater Nutzung; Zulässigkeitsvoraussetzungen und -bedingungen; Zugriffsregelungen für private E-Mails; Anwendung der Telekommunikationsgesetze

Information und Qualifizierung der Beschäftigten

- Schulungskonzepte; Schulungsmaßnahmen; Ziele, Inhalte, Häufigkeit, Zielgruppen; Rahmenbedingungen und Ausstattung; Benutzerbetreuung; Arbeitszeit- und Verdienstregelungen
- betriebsöffentliche Internet- und Intranet-Terminals für Beschäftigte ohne Computerarbeitsplatz

Gesundheitsschutz

ergonomische Gestaltung der Bildschirmarbeitsplätze; Schutz vor psychischen Belastungen; Regeln zur Gesundheitsfürsorge und deren Einhaltung, Kontrollen, Audits, regelmäßige Überprüfungen

Organisation der Nutzung von Internetdiensten

- allgemein: Einbettung der Nutzung von Internetdiensten in die bestehende oder eine weiterentwickelte Arbeitsorganisation, Zugang zu den Internetdiensten für Beschäftigte ohne Bildschirmarbeitsplatz
- Intranet: Nutzung gemeinsamer Informationspools, Terminkalender sowie Kommunikationsanwendungen, Präsenz von Arbeitnehmervertretung und Gewerkschaft
- E-Mail: E-Mail-Postfächer, Vertretungsregelungen, Festlegung von

Form und zulässigen Inhalten von E-Mail-Nachrichten, rechtliche Bedeutung von E-Mail-Nachrichten, Netiquette, Adressbücher, Erreichbarkeit, Souveränität der Anwender

Fortentwicklung der Vereinbarung

- Pilotregelung; begrenzte Laufzeit der Vereinbarung oder regelmäßige Prüfung, um die Dynamik der Entwicklung aufgreifen zu können; Öffnungsklauseln für spätere Veränderungen
- Ziele der Fortentwicklung; Optimierung des Sicherheits- und Schutzniveaus sowie des Anwendungskomforts und der Arbeitszufriedenheit
- Prozessregelung; Anpassung von Regelungen im Prozess; Internet-Projektgruppen; Zusammenarbeit von Arbeitgeber- und Arbeitnehmervertretern, um die Anwendung der Internetdienste sowie der geltenden Vorschriften den aktuellen Verhältnissen laufend anzupassen

Mitbestimmungsrechte und -prozeduren

- institutionalisierte Mitbestimmung des Betriebs- oder Personalrates; Informations-, Konsultations-, Beratungs- und Mitbestimmungsrechte der Interessenvertretung; Einbeziehen der Arbeitnehmervertretung in die Bewertung und Fortentwicklung der Nutzung von Internetdiensten; Beteiligung der Arbeitnehmervertretung an Planungs-, Lenkungs- und Entscheidungsgremien sowie an Projektgruppen; Betriebs- oder Personalrat haben das Recht, die Einhaltung der Vereinbarung zu kontrollieren; Einhaltungskontrolle: Regeln, Kontrollzugänge, regelmäßige Informationen; Qualifizierung der Arbeitnehmervertretung; Recht auf Hinzuziehung externer Sachverständiger
- Nutzungsmöglichkeiten durch die Interessenvertretung: Nutzung der Internetdienste durch Betriebs- bzw. Personalrat, besonderer Schutz (auch für Betriebsärzte, Schwerbehindertenvertreter, Datenschutzbeauftragte etc.)
- Konfliktregelungen; Kündigung und Nachwirkung der Vereinbarung; Salvatorische Klausel

6.2 Ausgangspunkte für die gestaltende Einflussnahme durch die Interessenvertretung

Dieses Kapitel gibt in kompakter Form Anregungen für eine Positionsbestimmung der Belegschaftsvertretung.
Die Nutzung der Internetdienste in Betrieben und Verwaltungen kann Beschäftigten große Vorteile bringen: zum Beispiel die Kommunikation vereinfachen und die Informationsbeschaffung optimieren. Im besten Fall führt sie zu mehr Arbeitszufriedenheit und – durch entsprechende Schulungen – zu gut qualifizierten Arbeitnehmerinnen und Arbeitnehmern. Die betriebliche Interessenvertretung kann entscheidend dazu beitragen, dass diese Potenziale genutzt werden und nicht Aspekte wie Arbeitsverdichtung und -beschleunigung im Vordergrund stehen.
Unternehmen stehen vor der Herausforderung, die Sicherheitsfragen zu lösen, die mit jeder Form von Internetnutzung einhergehen: Der Schutz betrieblicher und personenbezogener Daten ist dabei zentrales Thema. Letzterer ist auch Aufgabe der Interessenvertretung. Eine zu starke Reglementierung oder detaillierte Protokollierungen aber verhindern eine sinnvolle Nutzung der Internetdienste durch die Beschäftigten. Es muss das jeweils »richtige« Verhältnis von Sicherheit und Kontrolle gefunden werden. Eine Betriebs- bzw. Dienstvereinbarung soll auch dazu beitragen, die Sensibilität für Sicherheitsfragen bei den Nutzern sowie den Verantwortlichen zu schärfen, ohne dass die Verantwortung für Sicherheitsfragen hauptsächlich bei den Beschäftigten liegt.
Neben diesen Fragen ist die private Nutzung zu regeln. Sie generell zu untersagen, ist in den meisten Fällen eine wenig praxistaugliche Lösung. Eine sinnvolle Begrenzung der privaten Nutzung zu vereinbaren, kann beispielsweise Ziel der Interessenvertretung sein. Bei diesem Aspekt einer Vereinbarung ist es besonders wichtig, den Dialog mit den Beschäftigten zu suchen. Und: Allen Beteiligten muss klar sein, dass eine eindeutige Grenzziehung zwischen beruflicher und privater Nutzung kaum möglich ist. Dem sollte eine Regelung Rechnung tragen.
Um eine eigene Position entwickeln zu können, brauchen die Mitglieder der Interessenvertretung ein Grundverständnis für die Struktur und Organisation des Internets, zu möglichen Gefahren und zu den technischen Abwehrsystemen. Zudem müssen sie die rechtlichen Rahmen-

bedingungen der betrieblichen Netznutzung kennen. Gegebenenfalls muss sich die Interessenvertretung beraten lassen oder anderweitig sachkundig machen. Aufgabe der Arbeitnehmervertretung ist es auch, die durch eine gute Vereinbarung erzielten Vorteile für die Beschäftigten, die bei Ausweitung oder Veränderung der Nutzung von Internetdiensten immer wieder in Frage gestellt werden, zu sichern.
Das kann darüber gelingen, dass die einzelnen Punkte der Vereinbarung einer regelmäßigen gemeinsamen Überprüfung durch Arbeitgeber- und Arbeitnehmervertreter unterzogen werden. Denn eine Vereinbarung muss dem rasanten Entwicklungsprozess der Internettechnik und deren Nutzungsmöglichkeiten Rechnung tragen.
Durch Beteiligung der Beschäftigten kann die Interessenvertretung auch weitere Punkte kompetent regeln, die sich aus der Internetnutzung ergeben. Dazu gehören Fragen der Qualifikation, der Kommunikation, der Kooperation zwischen verschiedenen Hierarchieebenen und der veränderten Arbeitsabläufe.
Nicht zuletzt ist es wichtig, dass die betriebliche Interessenvertretung die Internetdienste selbst nutzt. Dies fördert die qualifizierte Auseinandersetzung mit den Arbeitgebervertretern und macht den Dialog mit den Beschäftigten einfacher. Für die Arbeit des Gremiums ist der sinnvolle Einsatz von Internet und Intranet ein großer Gewinn. Die betriebliche Interessenvertretung sollte in der Vereinbarung verankern, dass sie sich in das Intranet und in den Internetauftritt des Unternehmens mit einem eigenen Informationsangebot einbringen kann.

6.3 Wesentliche rechtliche Grundlagen

Dieses Kapitel enthält einen Überblick über Rechtsvorschriften im Zusammenhang mit der betrieblichen Nutzung der Internetdienste. Die wichtigsten Gesetze unter Berücksichtigung aktueller Rechtsprechung werden knapp behandelt und in ihrer Bedeutung bewertet.

6.3.1 Betriebsverfassungsgesetz

Betriebsräte können Informations-, Beratungs- und Mitbestimmungsrechte gemäß BetrVG nutzen.

Informationsrechte

Arbeitgeber haben die Betriebsräte gemäß §80 Abs. 2 Satz 1 und 2 BetrVG grundsätzlich und gemäß §90 Abs. 1 BetrVG im Speziellen so zu informieren, dass sie bezüglich der Einrichtung, Nutzung und Änderung betrieblicher Internetdienste und der dazu notwendigen technischen Systeme pflichtgemäß handeln können. Über die damit verbundenen personellen Veränderungen und die Personalplanung des Arbeitgebers ist der Betriebsrat gemäß §92 BetrVG zu informieren; in besonderen Fällen stehen ihm auch Beratungsrechte zu. In Betriebsvereinbarungen sind die Informationsrechte oft näher ausformuliert, um unterschiedliche Interpretationen und Konflikte zu vermeiden. Kommt es trotzdem zu Konflikten, weil z. B. der Arbeitgeber die Informationen nicht in notwendigem Umfang oder nicht rechtzeitig liefert, kann der Betriebsrat auf Grundlage des §23 Abs. 3 BetrVG seine Rechte gerichtlich durchsetzen.

Weitere Informationsrechte des Betriebsrats ergeben sich aus §80 Abs. 2 Satz 3 BetrVG. Demgemäß müssen sachkundige Beschäftigte als Auskunftspersonen zur Verfügung stehen. Auch dies wird in einigen Vereinbarungen konkreter formuliert.

Schließlich hat der Betriebsrat gemäß §80 Abs. 3 BetrVG das Recht, externe Sachverständige hinzuzuziehen, die regelmäßig notwendig sind, um die komplizierten technischen Zusammenhänge und Details der Internetdienste und der dazu eingesetzten technischen Systeme zu erläutern und dies mit den rechtlichen Anforderungen, z. B. aus dem Datenschutzrecht, zu verknüpfen. Bevor externe Sachverständige beauftragt werden können, ist in der Regel das innerbetriebliche Fachwissen von sachkundigen Arbeitnehmerinnen und Arbeitnehmern auszuschöpfen. In Vereinbarungen finden sich gelegentlich Regelungen, die dem Betriebsrat ohne vorherige Abstimmung mit dem Arbeitgeber externen, meist zeitlich und finanziell begrenzten Sachverstand zugestehen, wenn der Betriebsrat die Kontrolle der Einhaltung der Regelungen unterstützen soll (vgl. Kap. 3.1). Die Notwendigkeit von

Kontrollen leitet sich unmittelbar aus § 80 Abs. 1 Nr. 1 BetrVG ab. Regelmäßig kann davon ausgegangen werden, dass in einem Betriebsratsgremium das für die Kontrollaufgaben notwendige technische Fachwissen nicht vorhanden ist und dass die innerbetrieblichen Sachkundigen für Kontrollen – eventuell ihrer eigenen Aufgaben – nicht in Frage kommen.

Beratungsrechte

Aus § 90 Abs. 2 BetrVG leitet sich das Beratungsrecht der Betriebsräte a) hinsichtlich der Einrichtung und Änderung von Internetdiensten und den dazu verwendeten technischen Systemen sowie b) hinsichtlich der sich daraus ergebenden Auswirkungen auf die Arbeitnehmer ab. Ein in diesem Zusammenhang anzuwendendes Beratungsrecht ergibt sich aus § 97 Abs. 1 BetrVG, wenn Fragen zu den Schulungen für die Nutzung von Internetdiensten zu behandeln sind. Details zu Qualifizierungsmaßnahmen regeln viele Betriebsvereinbarungen zu E-Mail- und Internetdiensten oder sie verweisen auf übergreifende Vereinbarungen zur Weiterbildung der Arbeitnehmer (vgl. Kap. 2.1.14). Kommt ein Betriebsrat zu der Ansicht, dass die Einführung und Nutzung von Internetdiensten oder sozialen Medien zur Beschäftigungssicherung beitragen kann, dann sollte er seine Rechte gemäß § 92a BetrVG wahrnehmen und dem Arbeitgeber Vorschläge unterbreiten, die dieser ernsthaft prüfen und mit dem Betriebsrat beraten muss.

Mitbestimmungsrechte

Eine zentrale Vorschrift aus Sicht der betrieblichen Interessenvertretung ist § 87 Abs. 1 Nr. 6 BetrVG zur Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die für die Nutzung der Internetdienste notwendigen technischen Systeme wie z. B. Browser, Firewall, Proxyserver speichern in erheblichem Maße personenbezogene Daten, so dass dieses starke Mitbestimmungsrecht des Betriebsrats unmittelbar Anwendung findet.

Der Betriebsrat sollte seine Einflussnahme auf die Ausgestaltung der Internetdienste und ihre betriebliche Nutzung jedoch nicht auf diesen Aspekt reduzieren. Die Mitbestimmung nach § 87 BetrVG greift auch an einigen weiteren Punkten, zum Beispiel:

- Gemäß § 87 Abs. 1 Nr. 8 BetrVG kann der Betriebsrat bei Form, Ausgestaltung und Verwaltung von Sozialeinrichtungen mitbestimmen, wenn beispielsweise ein für alle Beschäftigten zugänglicher Internetzugang oder ein Internet-Café eingerichtet werden soll.
- Bei der betrieblichen Bereitstellung von Smartphones oder Tablet-PCs und deren Nutzung kann der Betriebsrat mitbestimmen, da hier wichtige Fragen der Ordnung im Betrieb (§ 87 Abs. 1 Nr. 1 BetrVG) und des Verhaltens der Arbeitnehmer im Betrieb geklärt werden müssen. Außerdem kann hier die Mitbestimmung bei Leistungen mit Entgeltcharakter (§ 87 Abs. 1 Nr. 11 BetrVG) greifen. Fragen der Ordnung im Betrieb sind regelmäßig auch betroffen, wenn Social-Media-Guidelines (→ Glossar) in Kraft sind.
- Schließlich ist auch § 87 Abs. 1 Nr. 7 BetrVG relevant, um den Gesundheitsschutz an Bildschirmarbeitsplätzen zu regeln.

Bei der Durchführung von Schulungen der Arbeitnehmer, damit diese die Internetdienste effektiv nutzen können, hat der Betriebsrat gemäß § 98 BetrVG ein starkes Mitbestimmungsrecht, das in der Praxis offenbar recht selten genutzt wird und auch in den Betriebsvereinbarungen leider keine besondere Beachtung findet (vgl. Kap. 2.1.14).

In Einzelfällen kann § 111 BetrVG zur Anwendung kommen, wenn durch die Internetdienste grundlegend neue Arbeitsmethoden eingeführt werden und dies Nachteile für erhebliche Teile der Belegschaft zur Folge haben könnte.

Ausstattung/Nutzungsrechte

Eine Nutzung der Internetdienste für die Arbeit der betrieblichen Interessenvertretung kann nach der Novellierung des BetrVG im Jahr 2001 leichter als zuvor rechtlich durchgesetzt werden. Der Gesetzgeber hat den Arbeitgeber in § 40 Abs. 2 BetrVG verpflichtet, dem Betriebsrat neben Räumen, sachlichen Mitteln und dem Büropersonal ausdrücklich auch die IuK-Technik zur Verfügung zu stellen. Erfasst werden damit die Computer-Ausstattung der Büros, die stationären und mobilen Telefone und auch die E-Mail-, Intranet- und Internetzugänge und -dienste.

6.3.2 Datenschutzrecht

Bei der Ausarbeitung von Betriebs- bzw. Dienstvereinbarungen müssen die jeweils anzuwendenden Bundes- oder Landesdatenschutzgesetze sowie die Datenschutzregeln von Telekommunikations- und Telemediengesetz beachtet werden.
Neben den für alle betrieblichen IKT-Systeme geltenden Bestimmungen aus den Datenschutzgesetzen sind bei der Nutzung von E-Mail und Internetdiensten zusätzlich das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) zu beachten. Diese gehen den Datenschutzgesetzen vor, sofern sie speziellere Regeln enthalten. Sie müssen also zuerst zu Rate gezogen werden, falls sie auf den jeweiligen betrieblichen Fall anwendbar sind.
Die Anwendbarkeit hängt entscheidend davon ab, ob das Unternehmen die private Nutzung verbietet, duldet oder erlaubt: Das Unternehmen ist nach aktueller Rechtsprechung im Sinne von § 3 Punkt 6 TKG »Diensteanbieter«, wenn es die private Nutzung duldet oder erlaubt. Sofern das Unternehmen die Telefonkommunikation über das Internet abwickelt (»Voice over IP«), ist auch dies hierbei zu berücksichtigen.
Für Diensteanbieter gelten die strengen Datenschutzanforderungen des TKG, die in § 88 Abs. 3 TKG (Fernmeldegeheimnis) formuliert sind: »Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden.« Der Abschnitt 2 mit den §§ 91 bis 107 TKG enthält weitere spezifische Regelungen zum Datenschutz bei der Telekommunikation. Zusätzlich sind vom Arbeitgeber die Datenschutzbestimmungen der §§ 11 bis 15a TMG zu beachten, sofern er Diensteanbieter im Sinne des TKG ist.
Diese Gesetzeslage macht eine Überwachung der Internetnutzung nahezu unmöglich, so dass das Unternehmen z. B. nicht nach einem Missbrauch in den Protokolldaten recherchieren darf. Viele betriebliche Vereinbarungen enthalten Regelungen, mit denen diese gesetzlichen Bestimmungen außer Kraft gesetzt werden, indem von den Arbeitneh-

mern eine schriftliche Einwilligung in die Auswertung von Protokollen bei Verdacht auf Missbrauch verlangt wird (vgl. Kap. 2.1.13).
Aus praktischer Sicht ist diesem Verfahren nichts entgegenzusetzen. Es sensibilisiert die Beschäftigten für die Datenschutzproblematik und die entsprechenden Betriebsvereinbarungen. In juristischer Hinsicht ist jedoch nicht eindeutig geklärt, ob dieses Verfahren rechtlich einwandfrei ist, weil zumindest einige Juristen davon ausgehen, dass die Einwilligung eines Arbeitnehmers gegenüber seinem Arbeitgeber, in dessen Abhängigkeitsverhältnis er steht, nicht freiwillig sein kann. In den Erklärungen sollte deswegen die Freiwilligkeit sichergestellt werden, indem den Betroffenen zugesichert wird, dass ihnen keine Nachteile bei verweigerter Unterzeichnung entstehen.

6.3.3 Arbeitsschutzrecht

Das Arbeitsschutzrecht ist bei der Nutzung von E-Mail- und Internetdiensten zu berücksichtigen. Das Arbeitsschutzgesetz (ArbSchG) verpflichtet die Arbeitgeber, »die erforderlichen Maßnahmen des Arbeitsschutzes unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Er hat die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls sich ändernden Gegebenheiten anzupassen. Dabei hat er eine Verbesserung von Sicherheit und Gesundheitsschutz der Beschäftigten anzustreben.« (§ 3 ArbSchG) Gemäß § 5 ArbSchG hat der Arbeitgeber die Arbeitsbedingungen zu beurteilen (Gefährdungsbeurteilung). Dies ist bei der Nutzung von E-Mail- und Internetdiensten an stationären Bildschirmarbeitsplätzen relevant und wird durch die Bildschirmarbeitsverordnung (BildscharbV) näher geregelt. In § 3 BildscharbV werden die Anforderungen an eine Gefährdungsbeurteilung konkretisiert; in den §§ 4 und 5 BildscharbV sind die Anforderungen an die Gestaltung von Arbeitsplätzen und Arbeitsabläufen benannt, die natürlich auch auf die Nutzung von E-Mail- und Internetdiensten anzuwenden sind. Betriebsvereinbarungen zu E-Mail- und Internetdiensten enthalten selten betriebliche Regeln, die das Arbeitsschutzrecht umsetzen (vgl. Kap. 4), was jedoch möglicherweise auf allgemeine und übergreifend geltende Regelungen in IKT-Rahmenvereinbarungen zurückzuführen ist.

7. Bestand der Vereinbarungen

Für die vorliegende Broschüre wurden insgesamt 192 betriebliche Regelungen ausgewertet. Jeweils rund ein Drittel sind Betriebsvereinbarungen und Richtlinien. Bei Letzteren handelt es sich überwiegend um so genannte Social-Media-Guidelines.

Art der Vereinbarung	Anzahl
Betriebsvereinbarung	67
Rahmenbetriebsvereinbarung	12
Gesamtbetriebsvereinbarung	12
Konzernbetriebsvereinbarung	11
Rahmenkonzernbetriebsvereinbarung	1
Dienstvereinbarung	18
Rahmendienstvereinbarung	6
Richtlinie	59
Sonstiges	6
Gesamt	**192**

Tabelle 1: *Art und Anzahl der Vereinbarungen*

Während in den früheren Auswertungen die Vereinbarungen größtenteils aus dem öffentlichen Sektor stammten, sind aktuell die dienstleistenden Bereiche am häufigsten vertreten. Der öffentliche Bereich und das verarbeitende Gewerbe lieferten nur geringfügig weniger Vereinbarungen, so dass im Gegensatz zu früheren Jahren keine wesentlichen Unterschiede im Branchenzuschnitt feststellbar sind.

Branche	Anzahl	
Industrie und verarbeitendes Gewerbe		*60*
Fahrzeughersteller sonstiger Fahrzeuge	1	
Fahrzeughersteller Kraftwagen	5	
Fahrzeughersteller von Kraftwagenteilen	5	
Maschinenbau	2	
Metallerzeugung und -bearbeitung	5	
Metallverarbeitung	4	
Chemische Industrie	6	
Gummi- und Kunststoffherstellung	3	
Baugewerbe	1	
Verlags- und Druckgewerbe	7	
Möbelhersteller	2	
Ledergewerbe	1	
Informationstechnikhersteller	2	
Mess-, Steuer- und Regelungstechnik	4	
Nachrichtentechnik/Unterhaltungs-, Automobilelektronik	5	
Elektro	2	
Ernährungsgewerbe	5	
Privatwirtschaftliche Dienstleistungen		*75*
Energiedienstleister	4	
Wasserversorger	2	
Einzelhandel (ohne Kfz.)	4	
Großhandel (ohne Kfz.)	5	
Kreditgewerbe	22	
Datenverarbeitung u. Softwareentwicklung	9	
Telekommunikationsdienstleister	5	
Postdienstleistungen	1	
Sonstige Verkehrsdienstleister	8	
Grundstücks- und Wohnungswesen	4	

Branche	Anzahl
Unternehmensbezogene Dienstleistungen	9
Leasingunternehmen	1
Tankstellen, Kfz.-Reparatur und -Handel	1
Öffentliche Verwaltung	26
Gesundheit und Soziales	13
Verbände und Gewerkschaften	3
Bildungseinrichtung	2
Forschung und Entwicklung	1
Kultur, Sport und Unterhaltung	3
Branchenübergreifend	3
Anonym	6
Gesamt	**192**

Tabelle 2: *Verteilung der Vereinbarungen nach Branchen*

Der Bestand enthält Regelungen ab 1996. Die meisten Dokumente sind jüngeren Datums. Die Richtlinien zum Thema Soziale Medien stammen ausschließlich aus den Jahren 2010 bis 2012.

Abschlussjahr	Anzahl
1996	1
1997	1
1998	1
1999	1
2000	4
2001	2
2002	5
2003	2
2004	8

Abschlussjahr	Anzahl
2005	11
2006	8
2007	12
2008	12
2009	24
2010	29
2011	37
2012	11
2013	1
unbekannt	22
Gesamt	**192**

Tabelle 3: *Abschlussjahr der Vereinbarungen*

Glossar

Account
Allgemein: Zugangsberechtigung zu einem EDV-System. Hier speziell: Bezeichnung eines eingerichteten E-Mail-Benutzerkontos, das eine oder mehrere E-Mail-Adressen, ein oder mehrere Postfächer und deren Zugriffsberechtigung umfasst.

Bring Your Own Device (BYOD)
Konzepte, die zulassen, dass Beschäftigte ihre eigenen Geräte mit in den Betrieb bringen und damit arbeiten.

Client
Arbeitsstation/Anwendungsprogramm, das von seinem Gegenstück (Server) mit Daten versorgt wird und die Interaktion mit dem Benutzer gewährleistet. Auf dem Server werden hauptsächlich die für alle Clients notwendigen Daten zentral vorgehalten (z. B. Webpages, Datenbanken).

Cloud Computing
Unabhängig vom eigenen Rechner bestehende Rechnerleistung und Speicherplatz im Internet.

Digitale Signatur
Verbindliche Unterschrift in elektronischer Form als Voraussetzung für eine verbindliche elektronische Kommunikation. Die digitale Signatur wird durch mathematische Verknüpfung des Textes mit einem persönlichen, geheimen Signaturschlüssel erzeugt. Empfänger können diese Signatur mit dem öffentlichen Schlüssel prüfen. Rechtsverbindlichkeit erhält das Verfahren durch das Signaturgesetz.

Internet Protocol/Transmission Control Protocol (IP/TCP)
Grundlegendes Verbindungsprotokoll für den Datenaustausch zwischen Internetrechnern. Es kann unterschiedliche Hardware benutzen und wird von nahezu allen Betriebssystemen unterstützt.

Internet-Protokoll-Adresse (IP-Adresse)
Eindeutige Adresse eines Computers.

Logikbombe
Programm, das nach Eintreten bestimmter Bedingungen schädliche Aktionen auslöst. Es hat nicht die Fähigkeit, sich selbst zu vermehren, hier unterscheidet es sich von einem Computer-Virus oder Computer-Wurm.

Netiquette
Zusammensetzung aus Net (dt.: Netz) und Etiquette: In der Netiquette wird gutes bzw. erwünschtes Verhalten in der netzgestützten Kommunikation definiert.

Proxyserver
Engl. »Stellvertreter«. Als Proxyserver bezeichnet man einen Rechner, der Anfragen von den Clients (Browsern) entgegennimmt und diese an das gewünschte Ziel weiterleitet. Der Proxyserver besitzt einen Speicher (Cache), um angefragte Daten zwischenzuspeichern. Damit kann er eventuell nachfolgende Anfragen ohne zusätzliches Anfragen beim www-Server beantworten.

Social-Business-Tools
Auch Social Software oder Social Business Software. Anwendungen zur Kommunikation und Kollaboration im Netz, z. B. Wikis oder Blogs. Die Begriffe bezeichnen in der Regel soziale Medien, die unternehmensintern genutzt werden.

Social Media/Soziale Medien
Gesamtheit der digitalen Medien wie Weblogs, Wikis und soziale Netzwerke (z. B. Facebook), über die Nutzer miteinander kommunizieren, Inhalte austauschen und gemeinsam entwickeln können.

Social-Media-Guidelines
Richtlinien zur betrieblichen Nutzung von Social Media.

Literatur- und Internethinweise

Bitkom (2008): Leitfaden Internet und E-Mail im Unternehmen, Download unter www.bitkom.org/de/publikationen
Bitkom (2013): Leitfaden »Bring your own device«, Download unter www.bitkom.org/de/themen
Böker, Karl-Hermann/Demuth, Ute (2013): IKT-Rahmenvereinbarungen, Reihe Betriebs- und Dienstvereinbarungen, Hans-Böckler-Stiftung (Hrsg.), Frankfurt am Main
Böker Karl-Hermann/Demuth, Ute/Thannheiser, Achim/Werner, Nils (2013): Social Media – Soziale Medien?, Hans-Böckler-Stiftung (Hrsg.), edition 281, Düsseldorf
Buggisch, Christian (2014): Social Media und soziale Netzwerke – Nutzerzahlen in Deutschland 2014, Download unter http://buggisch.wordpress.com
Däubler, Wolfgang (2013): Internet und Arbeitsrecht, 4. Aufl., Frankfurt am Main
Dietsch Gaby/Fickert, Jürgen/Wallbusch, Stefanie (2012): Den Einsatz von Internet und E-Mail regeln – Handlungshilfe für die betriebliche Interessenvertretung, Reihe Arbeit, Gesundheit, Umwelt, Technik, TBS NRW (Hrsg.), Heft 74, November 2012, Dortmund
Greve, Silke/Wedde, Peter (2014): Social-Media-Guidelines, Reihe Betriebs- und Dienstvereinbarungen, Hans-Böckler-Stiftung (Hrsg.), Frankfurt am Main
Hau, Thomas/Göcking, Jens (2013): Datenschutz am Arbeitsplatz, Arbeitskammer des Saarlandes (Hrsg.), Saarbrücken
Hümmerich, Klaus/Lücke, Oliver/Mauer, Reinhold (Hrsg.) (2011): Arbeitsrecht, Nomos-Formulare, 7. Aufl., Baden-Baden
Jenau, Jens (2010): Private Nutzung von Internet und Firmen-E-Mail-Adresse am Arbeitsplatz, in: AiB 2/2010, S. 88–92
Lochmann, Walter (2011): Allen antworten, drucken, speichern und wei-

terleiten? Wie der Einsatz von E-Mails die Arbeit verändert, BTQ (Hrsg.), Kassel
Pangert, Barbara/Schüpbach, Heinz (2013): Die Auswirkungen arbeitsbezogener erweiterter Erreichbarkeit auf Life-Domain-Balance und Gesundheit, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg.), Dortmund/Berlin/Dresden
Polenz, Sven/Thomsen, Sven (2010): Private oder dienstliche Internet- und E-Mail-Nutzung?, Online-Veröffentlichung, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.), Kiel
Ruhland, Robert Malte (2013): Knöllchen wegen offenen E-Mail-Verteilers, in: CuA 11/2013, S. 22ff.
Schwemmle, Michael/Wedde, Peter (2012): Digitale Arbeit in Deutschland. Potenziale und Problemlagen, Bonn, Download unter http://library.fes.de
Simitis, Spiros (Hrsg.) (2011): Bundesdatenschutzgesetz, Kommentar, 7. Aufl., Baden-Baden
Schultz, Stefan (2011): Blackberry-Pause – VW-Betriebsrat setzt E-Mail-Stopp nach Feierabend durch, in: Der Spiegel, Download unter www.spiegel.de/wirtschaft/service
Statistisches Bundesamt (Hrsg.) (2013): Soziale Medien halten Einzug in die Unternehmen, Pressemitteilung Nr. 417 vom 10. 12. 2013, Download unter https://www.destatis.de
Thannheiser, Achim (2014): Mobile Endgeräte – Handy, Smartphone, Blackberry und Tablet, Reihe Betriebs- und Dienstvereinbarungen/Kurzauswertungen, Hans-Böckler-Stiftung (Hrsg.), Download unter www.boeckler.de
Vogl, Gerlinde/Nies, Gerd (2013): Mobile Arbeit, Reihe Betriebs- und Dienstvereinbarungen, Hans-Böckler-Stiftung (Hrsg.), Frankfurt am Main

Das Archiv Betriebliche Vereinbarungen der Hans-Böckler-Stiftung

Die Hans-Böckler-Stiftung verfügt über die bundesweit einzige bedeutsame Sammlung betrieblicher Vereinbarungen, die zwischen Unternehmensleitungen und Belegschaftsvertretungen abgeschlossen werden. Derzeit enthält unser Archiv etwa 16 000 Vereinbarungen zu ausgewählten betrieblichen Gestaltungsfeldern.

Unsere breite Materialgrundlage erlaubt Analysen zu betrieblichen Gestaltungspolitiken und ermöglicht Aussagen zu Trendentwicklungen der Arbeitsbeziehungen in deutschen Betrieben.

Regelmäßig werten wir betriebliche Vereinbarungen in einzelnen Gebieten aus. Leitende Fragen dieser Analysen sind: Wie haben die Akteure die wichtigsten Aspekte geregelt? Welche Anregungen geben die Vereinbarungen für die Praxis? Wie ändern sich Prozeduren und Instrumente der Mitbestimmung? Existieren ungelöste Probleme und offene Fragen? Die Analysen betrieblicher Vereinbarungen zeigen, welche Regelungsweisen und -verfahren in Betrieben bestehen. Die Auswertungen verfolgen dabei nicht das Ziel, Vereinbarungen zu bewerten, denn die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen und Gestaltungshinweise zu geben.

Bei Auswertungen und Zitaten aus Vereinbarungen wird streng auf Anonymität geachtet. Die Kodierung am Ende eines Zitats bezeichnet den Standort der Vereinbarung in unserem Archiv und das Jahr des Abschlusses. Zum Text der Vereinbarungen haben nur Mitarbeiterinnen und Mitarbeiter des Archivs und Autorinnen und Autoren Zugang.

Zusätzlich zu diesen Auswertungen werden vielfältige anonymisierte Auszüge aus den Vereinbarungen auf der beiliegenden CD-ROM und der Online-Datenbank im Internetauftritt der Hans-Böckler-Stiftung zusammengestellt. Damit bieten wir anschauliche Einblicke in die Regelungspraxis, um eigene Vorgehensweisen und Formulierungen anzuregen. Darüber hinaus gehen wir in betrieblichen Fallstudien gezielt Fragen

nach, wie die abgeschlossenen Vereinbarungen umgesetzt werden und wie die getroffenen Regelungen in der Praxis wirken.

Das Internetangebot des Archivs Betriebliche Vereinbarungen ist unmittelbar zu erreichen unter *www.boeckler.de/betriebsvereinbarungen*. Anfragen und Rückmeldungen richten Sie bitte an *betriebsvereinbarung @boeckler.de* oder direkt an

Dr. Manuela Maschke
0211–7778–224, E-Mail: Manuela-Maschke@boeckler.de
Jutta Poesche
0211–7778–288, E-Mail: Jutta-Poesche@boeckler.de
Nils Werner
0211–7778–167, E-Mail: Nils-Werner@boeckler.de

Stichwortverzeichnis

Reihe Betriebs- und Dienstvereinbarungen

Bereits erschienen:

Karl-Hermann Böker · Ute Demuth **E-Mail-Nutzung und Internetdienste**	978-3-7663-6371-8	2014
Achim Thannheiser · Volker Mischewski **Telekommunikation: Anlagen und Anwendungen**	978-3-7663-6370-1	2014
Edgar Rose · Roland Köstler **Mitbestimmung in der Europäischen Aktiengesellschaft (SE)**	978-3-7663-6369-5	2014
Thomas Breisig **Entwicklung von Führungskräften**	978-3-7663-6324-4	2014
Manuela Maschke · Reingard Zimmer **CSR – Gesellschaftliche Verantwortung von Unternehmen**	978-3-7663-6323-7	2013
Hans Riegel · Dietmar Röhricht **Gestaltung des Übergangs in den Ruhestand**	978-3-7663-6297-1	2013
Eberhard Kiesche **Betriebliches Gesundheitsmanagement**	978-3-7663-6274-2	2013
Andrea Jochmann-Döll · Karin Tondorf **Betriebliche Entgeltpolitik für Frauen und Männer**	978-3-7663-6288-9	2013
Ingo Hamm **Flexible Arbeitszeiten – Kontenmodelle**	978-3-7663-6285-8	2013
Regine Rohman **Gefährdungsbeurteilungen**	978-3-7663-6273-5	2013
Gerlinde Vogl · Gerd Nies **Mobile Arbeit**	978-3-7663-6271-1	2013
Manuel Kiper **Gestaltung von Arbeitsstätten durch Mitbestimmung**	978-3-7663-6217-9	2013
Karl-Hermann Böker · Ute Demuth **IKT-Rahmenvereinbarungen**	978-3-7663-6208-7	2012
Manuela Maschke · Gerburg Zurholt **Chancengleich und familienfreundlich**	978-3-7663-6095-3	2012
Gerd Busse · Winfried Heidemann **Betriebliche Weiterbildung**	978-3-7663-6207-0	2012
Karl-Hermann Böker · Christiane Lindecke **Flexible Arbeitszeit – Langzeitkonten**	978-3-7663-6215-5	2012
Detlef Ullenboom **Toleranz, Respekt und Kollegialität**	978-3-7663-6190-5	2012
Rudi Rupp **Restrukturiertungsprozesse in Betrieben und Unternehmen**	978-3-7663-6206-3	2012
Michaela Dälken **Managing Diversity**	978-3-7663-6204-9	2012

Thomas Breisig **Grundsätze und Verfahren der Personalbeurteilung**	978-3-7663-6117-2	2012
Kerstin Hänecke · Hiltraud Grzech-Sukalo **Kontinuierliche Schichtsysteme**	978-3-7663-6174-5	2012
Marianne Giesert · Adelheid Weßling Fallstudien **Betriebliches Eingliederungsmanagement in Großbetrieben**	978-3-7663-6118-9	2012
Sven Hinrichs **Personalauswahl und Auswahlrichtlinien**	978-3-7663-6116-5	2011
Edgar Rose · Roland Köstler **Mitbestimmung in der Europäischen Aktiengesellschaft (SE)**	978-3-7663-6088-5	2011
Hiltraud Grzech-Sukalo · Kerstin Hänecke **Diskontinuierliche Schichtsysteme**	978-3-7663-6061-8	2011
Nikolai Laßmann · Rudi Rupp **Beschäftigungssicherung**	978-3-7663-6076-2	2010
Regine Romahn **Betriebliches Eingliederungsmanagement**	978-3-7663-6071-7	2010
Gerd Busse · Claudia Klein **Duale Berufsausbildung**	978-3-7663-6067-0	2010
Karl-Hermann Böker **Zeitwirtschaftssysteme**	978-3-7663-3942-3	2010
Detlef Ullenboom **Freiwillige betriebliche Sozialleistungen**	978-3-7663-3941-6	2010
Nikolai Laßmann · Dietmar Röhricht **Betriebliche Altersversorgung**	978-3-7663-3943-0	2010
Marianne Giesert Fallstudien **Zukunftsfähige Gesundheitspolitik im Betrieb**	978-3-7663-3798-6	2010
Thomas Breisig **AT-Angestellte**	978-3-7663-3944-7	2010
Reinhard Bechmann **Qualitätsmanagement und kontinuierlicher Verbesserungsprozess**	978-3-7663-6012-0	2010
Berthold Göritz · Detlef Hase · Nikolai Laßmann · Rudi Rupp **Interessenausgleich und Sozialplan**	978-3-7663-6013-7	2010
Thomas Breisig **Leistung und Erfolg als Basis für Entgelte**	978-3-7663-3861-7	2009
Sven Hinrichs **Mitarbeitergespräch und Zielvereinbarung**	978-3-7663-3860-0	2009
Christine Zumbeck **Leiharbeit und befristete Beschäftigung**	978-3-7663-3859-4	2009
Karl-Hermann Böker **Organisation und Arbeit von Betriebs- und Personalräten**	978-3-7663-3884-6	2009
Ronny Heinkel **Neustrukturierung von Betriebsratsgremien nach § 3 BetrVG**	978-3-7663-3885-3	2008
Christiane Lindecke Fallstudien **Flexible Arbeitszeiten im Betrieb**	978-3-7663-3800-6	2008

Svenja Pfahl · Stefan Reuyß **Gelebte Chancengleichheit im Betrieb**	Fallstudien	978-3-7663-3799-3	2008
Karl-Hermann Böker **E-Mail-Nutzung und Internetdienste**		978-3-7663-3858-7	2008
Ingo Hamm **Flexible Arbeitszeit – Kontenmodelle**		978-3-7663-3729-0	2008
Werner Nienhüser · Heiko Hoßfeld **Verbetrieblichung aus der Perspektive betrieblicher Akteure**	Forschung für die Praxis	978-3-7663-3905-8	2008
Martin Renker **Geschäftsordnungen von Betriebs- und Personalräten**		978-3-7663-3732-0	2007
Englische Ausgabe **Integrating Foreign National Employees**		987-3-7663-3753-5	2007
Karl Hermann Böker **Flexible Arbeitszeit – Langzeitkonten**		978-3-7663-3731-3	2007
Hartmut Klein-Schneider **Flexible Arbeitszeit – Vertrauensarbeitszeit**		978-3-7663-3725-2	2007
Regine Romahn **Eingliederung von Leistungsveränderten**		978-3-7663-3752-8	2007
Robert Kecskes **Integration und partnerschaftliches Verhalten**	Fallstudien	978-3-7663-3728-3	2006
Manuela Maschke · Gerburg Zurholt **Chancengleich und familienfreundlich**		978-3-7663-3726-2	2006
Edgar Bergmeier · Andreas Hoppe **Personalinformationssysteme**		978-3-7663-3730-6	2006
Regine Romahn **Gefährdungsbeurteilungen**		978-3-7663-3644-4	2006
Reinhild Reska **Call Center**		978-3-7663-3727-0	2006
Englische Ausgabe **Occupational Health Policy**		978-3-7663-3753-5	2006
Gerd Busse · Winfried Heidemann **Betriebliche Weiterbildung**		978-3-7663-3642-8	2005
Englische Ausgabe **European Works Councils**		978-3-7663-3724-6	2005
Berthold Göritz · Detlef Hase · Anne Krehnker · Rudi Rupp **Interessenausgleich und Sozialplan**		978-3-7663-3686-X	2005
Maria Büntgen **Teilzeitarbeit**		978-3-7663-3641-X	2005
Werner Nienhüser · Heiko Hoßfeld **Bewertung von Betriebsvereinbarungen durch Personalmanager**	Forschung für die Praxis	978-3-7663-3594-4	2004
Hellmut Gohde **Europäische Betriebsräte**		978-3-7663-3598-7	2004
Semiha Akin · Michaela Dälken · Leo Monz **Integration von Beschäftigten ausländischer Herkunft**		978-3-7663-3569-3	2004

Karl-Hermann Böker **Arbeitszeiterfassungssysteme**		978-3-7663-3568-5	2004
Heinz Braun · Christine Eggerdinger **Sucht und Suchtmittelmissbrauch**		978-3-7663-3533-2	2004
Barbara Jentgens · Lothar Kamp **Betriebliches Verbesserungsvorschlagswesen**		978-3-7663-3567-7	2004
Wilfried Kruse · Daniel Tech · Detlef Ullenboom **Betriebliche Kompetenzentwicklung**	Fallstudien	978-3-935145-57-8	2003
Judith Kerschbaumer · Martina Perreng **Betriebliche Altersvorsorge**		978-3-9776-3514-6	2003
Frank Havighorst · Susanne Gesa Umland **Mitarbeiterkapitalbeteiligung**		978-3-7663-3516-2	2003
Barbara Jentgens · Heinzpeter Höller **Telekommunikationsanlagen**		978-3-7663-3515-4	2003
Karl-Hermann Böker **EDV-Rahmenvereinbarungen**		978-3-7663-3519-7	2003
Marianne Giesert · Heinrich Geißler **Betriebliche Gesundheitsförderung**		978-3-7663-3524-3	2003
Ferdinand Gröben **Betriebliche Gesundheitspolitik**		978-3-7663-3523-5	2003
Werner Killian · Karsten Schneider **Umgestaltung des öffentlichen Sektors**		978-3-7663-3520-0	2003
Hartmut Klein-Schneider **Personalplanung**		978-3-935145-19-5	2001
Winfried Heidemann Hrsg. **Weiterentwicklung von Mitbestimmung im Spiegel betrieblicher Vereinbarungen**		978-3-935145-17-9	2000
Hans-Böckler-Stiftung **Beschäftigung – Arbeitsbedingungen – Unternehmensorganisation**		978-3-935145-12-8	2000
Englische Ausgabe **Employment, working conditions and company organisation**		978-3-935145-12-6	2000
Lothar Kamp **Telearbeit**		978-3-935145-01-2	2000
Susanne Gesa Umland · Matthias Müller **Outsourcing**		978-3-935145-08-X	2000
Renate Büttner · Johannes Kirsch Bündnisse für Arbeit im Betrieb	Fallstudien	978-3-928204-77-7	1999
Winfried Heidemann **Beschäftigungssicherung**		978-3-928204-80-7	1999
Hartmut Klein-Schneider **Flexible Arbeitszeit**		978-3-928204-78-5	1999
Siegfried Leittretter **Betrieblicher Umweltschutz**		978-3-928204-77-7	1999
Lothar Kamp **Gruppenarbeit**		978-3-928204-77-7	1999

Hartmut Klein-Schneider
Leistungs- und erfolgsorientiertes Entgelt 978-3-928204-97-4 **1998**

Bücher und Buchreihen der Hans-Böckler-Stiftung

Reihe Betriebs- und Dienstvereinbarungen

Karl-Hermann Böker
Ute Demuth
IKT-Rahmen-vereinbarungen
ISBN 978-3-7663-6208-7
2., aktualisierte Auflage
2013, 158 Seiten
kartoniert, € 12,90
mit CD-ROM

Analyse und Handlungsempfehlungen

Informations- und Kommunikationstechnik ist in Betrieben nicht mehr wegzudenken. Sie stellt Personalverantwortliche und betriebliche Interessenvertreter immer wieder vor neue Herausforderungen. Zentrale Aspekte sind die Wahrung der Rechte von Beschäftigten zum Daten- und Arbeitsschutz, das Abmildern negativer Folgen des Einsatzes neuer Technologien und die Begrenzung der Leistungs- und Verhaltenskontrolle. Angesichts zunehmender Vernetzung und Virtualisierung der Hardware zeigt sich dies als schwierige Gratwanderung.

Diese Auswertung von 140 betrieblichen Vereinbarungen aktualisiert die Analyse »EDV-Rahmenvereinbarungen« aus dem Jahr 2003. Sie zeigt Trends und Entwicklungen und gibt Hinweise für die Gestaltung eigener Vereinbarungen.

BUND VERLAG

Sie finden mehr Informationen, Downloads und unsere Online-Datenbank im Internet unter:
www.boeckler.de/betriebsvereinbarungen

Bücher und Buchreihen der Hans-Böckler-Stiftung

Reihe Betriebs- und Dienstvereinbarungen

Gerlinde Vogl/Gerd Nies
Mobile Arbeit
ISBN 978-3-7663-6271-1
2013, 196 Seiten,
kartoniert, € 12,90
mit CD-ROM

Analyse und Handlungsempfehlungen

Mobilität im Beruf ist für immer mehr Beschäftigte selbstverständlich. Mobile Endgeräte ermöglichen es, außerhalb der räumlichen und zeitlichen Grenzen des Betriebs zu arbeiten. Allerdings nimmt auch die Reisetätigkeit zu, nicht alles lässt sich über schnelle Datenleitungen regeln.

Mobile Arbeit zu gestalten, ist ein relativ junges Thema. Die Auswertung von 96 Betriebs- und Dienstvereinbarungen zeigt wie Betriebs- und Personalräte das Thema aufgreifen. Telearbeit, Dienstreisen, Arbeit beim Kunden und Entsendung sind wichtige Regelungsaspekte. In zehn Unternehmen wurden zudem betriebliche Akteure befragt. Gezeigt wird die Bandbreite möglicher Regelungen. Sie können Anregungen sein, um die zahlreichen noch offenen Probleme anzugehen.

BUND VERLAG

Sie finden mehr Informationen, Downloads und unsere Online-Datenbank im Internet unter:
www.boeckler.de/betriebsvereinbarungen

Bücher und Buchreihen der Hans-Böckler-Stiftung

Reihe Betriebs- und Dienstvereinbarungen

Andrea Jochmann-Döll
Karin Tondorf
Betriebliche Entgeltpolitik für Frauen und Männer
ISBN 978-3-7663-6288-9
2013, 210 Seiten
kartoniert, € 12,90
mit CD-ROM

Analyse und Handlungsempfehlungen

Kollektive Vereinbarungen zu Grundentgelt, Leistungsvergütungen, Erschwerniszuschlägen oder außertariflicher Vergütung dürfen nicht diskriminieren. Um dies zu gewährleisten, müssen die betrieblichen Akteure mögliche Diskriminierung entdecken und wirkungsvoll beseitigen können.

Die Auswertung von 284 betrieblichen Vereinbarungen zeigt, dass Benachteiligungen trotz geschlechtsneutraler Formulierungen entstehen können. Positive Regelungsbeispiele illustrieren, wie Entgeltdiskriminierung vermieden werden kann. Mit rechtlich fundierten Checks können Betriebs- und Personalräte Vereinbarungen auf Diskriminierungspotential untersuchen.

Zwei Fallstudien zur Leistungsvergütung und zur Vergütung von außertariflich Beschäftigten zeigen Möglichkeiten, wie die Entgeltpraxis gestaltet und überwacht werden kann.

BUND VERLAG

Sie finden mehr Informationen, Downloads und unsere Online-Datenbank im Internet unter:
www.boeckler.de/betriebsvereinbarungen

Bücher und Buchreihen der Hans-Böckler-Stiftung

Reihe Betriebs- und Dienstvereinbarungen

Hans Riegel
Dietmar Röhricht
Gestaltung des Übergangs in den Ruhestand
ISBN 978-3-7663-6297-1
2013, 136 Seiten
kartoniert, € 12,90
mit CD-ROM

Analyse und Handlungsempfehlungen

Die Rente mit 67 hat die Debatte um den Übergang in den Ruhestand neu belebt. Wie können Beschäftigte das Rentenalter bei guter Gesundheit erreichen? Wie können individuelle Wünsche berücksichtigt werden? Wer bezahlt? Altersteilzeit stellt ein wichtiges Instrument zur Gestaltung des Übergangs in den Ruhestand dar. Auch nach dem Ende der staatlichen Förderung wird Altersteilzeit genutzt. Sie kann als echte Altersteilzeit zu einer Entlastung noch während des Arbeitslebens führen. Aber der Verzicht auf Einkommen ist nicht für alle Beschäftigten möglich. Tarifvertragliche Regelungen zum demografischen Wandel sehen weitere Wege vor.

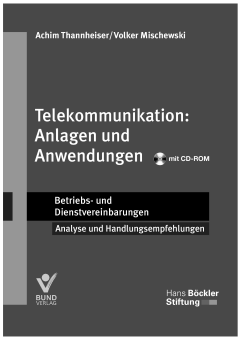
Die Auswertung von 124 Betriebs- und Dienstvereinbarungen der Jahre 1972 bis 2011 zeigt, wie betriebliche Akteure Übergänge in den Ruhestand regeln, welche Trends bestehen und sie gibt Anregungen für die Gestaltung eigener Vereinbarungen.

BUND VERLAG

Sie finden mehr Informationen, Downloads und unsere Online-Datenbank im Internet unter:
www.boeckler.de/betriebsvereinbarungen

Bücher und Buchreihen der Hans-Böckler-Stiftung

Reihe Betriebs- und Dienstvereinbarungen



Achim Thannheiser
Volker Mischewski
Telekommunikation: Anlagen und Anwendungen
ISBN 978-3-7663-6370-1
2014, 143 Seiten
kartoniert, € 12,90
mit CD-ROM

Analyse und Handlungsempfehlungen

Noch vor wenigen Jahren war die ISDN-fähige Anlage die neueste Errungenschaft, die Leistungs- und Verhaltenskontrollen ermöglichte. Heute sind es Internettelefonie und softwarebasierte Telefonsysteme. Der Umfang abbildbarer und erfassbarer personenbezogener Daten ist erheblich gewachsen. Die Kosten der Telefonie treten in den Hintergrund, der Wunsch nach Leistungsmessung rückt in den Vordergrund.

Die Auswertung von 100 Betriebs- und Dienstvereinbarungen zeigt, wie die betrieblichen Akteure das Thema aufgreifen, welche Trends bestehen und sie gibt Hinweise für die Gestaltung eigener Vereinbarungen. Eine Checkliste enthält die wichtigsten Stichworte und gibt einen Überblick über Regelungsmöglichkeiten.

BUND VERLAG

Sie finden mehr Informationen, Downloads und unsere Online-Datenbank im Internet unter:
www.boeckler.de/betriebsvereinbarungen