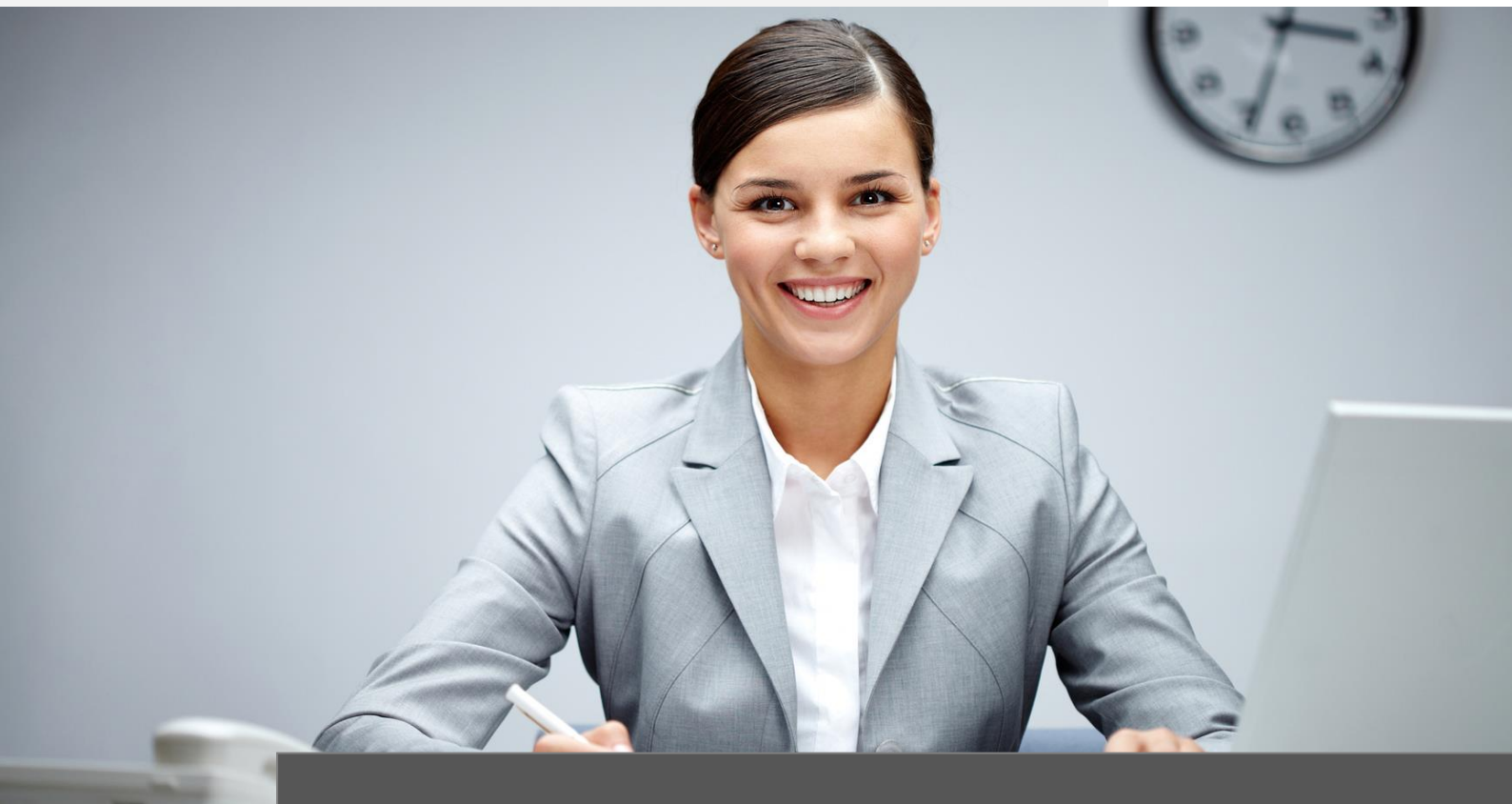


Datenschutz am Arbeitsplatz

März | 2013



Wichtige Datenschutzinformationen für Ihr Unternehmen

DPN

Datenschutz &
Informationssicherheit

Begrüßung Ihr Datenschutzbeauftragter vor Ort _____	3
Datenschutz am Arbeitsplatz Private Internetnutzung _____	4
Datenschutz am Arbeitsplatz Private E-Mail Nutzung _____	6
Datenschutz am Arbeitsplatz Social Media _____	8
Datenschutz am Arbeitsplatz Videoüberwachung _____	10
Datenschutz am Arbeitsplatz Private Telefonnutzung _____	13

Ihr Datenschutzbeauftragter vor Ort

Liebe Leserin, lieber Leser,

das Schlagwort *Beschäftigtendatenschutz* war Anfang dieses Jahres in aller Munde, was uns dazu bewogen hat, den inhaltlichen Fokus dieser Ausgabe auf den „Datenschutz am Arbeitsplatz“ auszurichten.

Interessen von Arbeitnehmern und Arbeitgebern prallen in diesem Bereich häufig aufeinander, vor allem, wenn die Befürchtung einer Überwachung am Arbeitsplatz im Raum steht.

Ob es um Telefon-, E-Mail-, Internetnutzung oder Videoanlagen geht – überall wird eine Überwachung der privaten Daten durch den Arbeitgeber vermutet. Doch was muss bei der Bereitstellung von Telekommunikationsmitteln beachtet werden? Welche Auswirkung hat eine Duldung bzw. Erlaubnis der privaten Nutzung des Beschäftigten?

In dieser Broschüre finden Sie einen kleinen Überblick der Problemfelder und was Sie bzw. wir gemeinsam im Hinblick auf den Datenschutz beachten müssen.

Unser Ziel ist es hierbei, dass Ihr Unternehmen über Datenschutz-Themen am Arbeitsplatz informiert und sensibilisiert wird, sodass Sie bzw. wir sowohl einer Haftung für Tätigkeiten Ihrer Mitarbeiter als auch möglichen Datenschutzverstößen aus dem Weg gehen.

Sowohl für eine ausführliche Beratung rund um das Thema Datenschutz am Arbeitsplatz als auch für allgemeine Fragen zu diesem Thema stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer (02153) 137 87 89 oder per E-Mail f.pastars@dpn-datenschutz.de.

Mit freundlichen Grüßen

Fabio Pastars

Zertifizierter Datenschutzbeauftragter (FH)
DEKRA zertifizierte Fachkraft für Datenschutz



Fabio Pastars



Viele Beschäftigte haben heutzutage die Möglichkeit, das Internet am Arbeitsplatz auch für private Zwecke zu nutzen. Auch wenn dies vielen Unternehmen nicht bewusst ist, ergeben sich hieraus zahlreiche rechtliche Probleme im Hinblick auf Datenschutz, arbeitsrechtliche und persönlichkeitsrechtliche Gesichtspunkte.

Ist beispielsweise keine Regelung der privaten Nutzung von Internet und E-Mail am Arbeitsplatz getroffen und wird die private Nutzung vom Unternehmen geduldet bzw. sogar pauschal erlaubt, so kann dies zu erheblichen Konflikten und Konsequenzen führen.

Rechtslage bei Erlaubnis oder Duldung der privaten Internetnutzung am Arbeitsplatz

Duldet der Arbeitgeber die private Nutzung des Internets stillschweigend, so erhält der Arbeitnehmer Anspruch nach den Grundsätzen betrieblicher Übung (regelmäßige Wiederholung bestimmter Verhaltensweisen). Eine solche betriebliche Übung lässt sich kaum ohne weiteres beseitigen. Daher ist es notwendig, die private Internetnutzung im Betrieb detailliert vorab zu regeln.

Im Falle einer Nutzungsduldung oder -erlaubnis im privaten Zusammenhang hat der Arbeitgeber neben den datenschutzrechtlichen Bestimmungen (Schutz der personenbezogenen Daten) auch das Fernmeldegeheimnis zu beachten. Rein rechtlich betrachtet ist er dann Anbieter von Telemediendiensten bzw. Telekommunikationsdiensten. Dort ist festgelegt, dass Daten mit Personenbezug nur für die Erbringung des Dienstes und dessen Abrechnung verarbeitet werden dürfen. Eine Missachtung des Telemediengesetzes ist strafbar (§206 StGB) und kann mit Bußgeldern von bis zu 300.000 EUR geahndet werden.

Grundsätzlich hat der Arbeitgeber jedoch ein berechtigtes Interesse daran, bei einer privaten Internetnutzung der Mitarbeiter sichergehen zu können, dass Missbrauch oder strafbare Handlungen durch die Mitarbeiter unterbleiben. Um dies in einem begrenzten Rahmen überwachen zu können, müssen jedoch einige Voraussetzungen erfüllt werden.

Hierzu gehören in der Regel eine individuelle Vertragsgestaltung des Beschäftigten, eine Betriebsvereinbarung oder bspw. eine Begrenzung des Zeitrahmens der privaten Internetnutzung (z. B.: Pausenzeiten).

Dennoch zeigt nachfolgendes Beispiel, dass nicht nur das Vorhandensein einer vertraglichen Vereinbarung zur Nutzung des Internets für private Zwecke erforderlich ist, sondern auch auf die genaue Formulierung geachtet werden muss.

In einem Fall vom LAG Rheinland-Pfalz wurde einem Mitarbeiter gekündigt, nachdem dieser während der Arbeitszeit mehrfach das Internet privat und nicht im Zusammenhang mit seiner Tätigkeit genutzt hatte. Dem Mitarbeiter war jedoch in der Vergangenheit mindestens einmal von seinem Vorgesetzten erlaubt worden, sich vom Arbeitsplatz aus in sein privates Bankkonto einzuloggen.

Der Arbeitgeberin lag zwar eine Erklärung zur Internet- und PC-Nutzung vor, die unter anderem folgende Passage enthielt:

„Der Zugang zum Internet und E-Mail ist nur zu dienstlichen Zwecken gestattet. Jeder darüber hinausgehende Gebrauch – insbesondere zu privaten Zwecken – ist ausdrücklich verboten. Verstöße gegen diese Anweisung werden ohne Ausnahme mit arbeitsrechtlichen Mitteln sanktioniert und führen – insbesondere bei Nutzung von kriminellen, pornographischen, rechts- oder linksradikalen Inhalten – zur außerordentlichen Beendigung des Arbeitsverhältnisses.“

Dennoch durfte die Arbeitgeberin dem Mitarbeiter nicht ohne Weiteres kündigen, sondern hätte zunächst eine Abmahnung aussprechen müssen.

Laut dem LAG Rheinland-Pfalz wäre hier zunächst eine Abmahnung rechtens gewesen, da vorliegende Erklärung bereits einige Jahre zurücklag und in ihr lediglich von *arbeitsrechtlicher Sanktionierung* die Rede war.

Was bedeutet das für die Praxis?

Wird das Internet am Arbeitsplatz zur Verfügung gestellt, sollte die private Nutzung unbedingt vertraglich geregelt werden, z. B. durch eine individuelle Vertragsgestaltung oder aber auch durch eine Betriebsvereinbarung. Dabei ist besonders auf die Formulierung der Inhalte und auf die genaue Festlegung der Nutzungsdauer zu achten, sodass diese eindeutig und klar sind und keinen Interpretationsspielraum zulassen.

Die Nutzung von E-Mail am Arbeitsplatz (am PC oder auch mit dem geschäftlichen Smartphone) kann in Bezug auf den Datenschutz viele Fragen aufwerfen. Neben dem jeweiligen Informationsaustausch (Zeitpunkte, Beteiligte) haben bei der E-Mail vor allem die Inhalte selbst eine große Bedeutung. In den meisten Mails ist zudem Personenbezug gegeben – E-Mail-Adressen beinhalten in der Regel einen Namen. Daher gelten auch hier u. a. die grundsätzlichen Vorschriften des BDSG.

Eine Auswertung oder Kontrolle der E-Mail-Nutzung ist dem Arbeitgeber aufgrund des Schutzes der Persönlichkeitsrechte (BDSG), des Post- und Fernmeldegeheimnisses und des Telekommunikationsgesetzes nicht grundsätzlich gestattet.

Ein weiteres Problem kommt in der Archivierungspflicht des Arbeitgebers zum Tragen. Dieser hat unter anderem die gesetzliche Vorgabe, den kompletten geschäftsrelevanten E-Mail-Verkehr zu archivieren, um so gegenüber Vertragspartnern oder auch dem Finanzamt, Vereinbarungen, Ausgaben und viele weitere wichtige Informationen dokumentieren zu können.

Aufgrund dieser Pflichten und der einfachen technischen Umsetzung wird die elektronische Post meist komplett archiviert. Eine automatische Sortierung nach bestimmten Bereichen, wie z.B. geschäftliche oder private Korrespondenz, findet in der Regel nicht statt.

Genau hier steht jedoch die Aufbewahrungspflicht des Unternehmens in einem direkten Spannungsverhältnis zu den datenschutzrechtlichen Vorgaben, da der Arbeitgeber die Privatpost des Arbeitnehmers nicht archivieren darf!

Auch kann er keine manuelle Trennung zwischen privaten und geschäftlichen Inhalten durchführen, da er hierzu die privaten E-Mails lesen müsste, was wiederum gegen das Fernmeldegeheimnis verstößt – ein Konflikt, der ohne eine spezielle Mitarbeiter- oder Betriebsvereinbarung nur schwer zu lösen ist!

Weiterhin ist zu beachten, dass ein E-Mail Account, der auch private E-Mails enthält, bei Ausscheiden des Arbeitnehmers erst dann gelöscht werden darf, wenn sichergestellt ist, dass der Arbeitnehmer kein Interesse mehr an der Nutzung der privaten E-Mails dieses Accounts hat. Die Verletzung dieser Pflicht kann beispielsweise auch einen Schadensersatzanspruch auslösen.

Datenschutz am Arbeitsplatz | Private E-Mail Nutzung

Erst kürzlich hatte das Oberlandesgericht (OLG) Dresden einen konkreten Fall zum Thema private E-Mails im geschäftlichen Account vorliegen.

Worum ging es?

In dem Verfahren war der Antragsteller für einige Monate als Fahrradkurier angestellt. Der Arbeitgeber hatte ihm für die Zeit ein Smartphone inkl. geschäftlichem E-Mail-Account zur Verfügung gestellt, der auch privat genutzt werden durfte.

Nach Beendigung des Arbeitsverhältnisses forderte der Antragsteller u. a. die Herausgabe der auf dem Account gespeicherten Daten.

In diesem Fall sagte das OLG Dresden einerseits, dass der Anspruch des ehemaligen Mitarbeiters auf Herausgabe der gespeicherten Mails entweder aus dem Vertrag zwischen Arbeitgeber und Arbeitnehmer direkt oder dann aus dem Herausgabeanspruch §§ 812, 985 BGB hergeleitet werden kann.

Andererseits teilte das Gericht mit, dass der einstige Mitarbeiter einen Anspruch auf Schadensersatz haben kann, wenn seine Daten unbefugt gelöscht werden.

Eine unbefugte Löschung oder das Unbrauchbarmachen von diesen Daten könnte sogar eine Straftat zur Folge haben. Zwar unterliegt der Mitarbeiter der Beweispflicht, d. h. der Kläger muss einen Schaden nicht nur dem Grunde nach, sondern auch der Höhe nach beweisen können. Dennoch erfüllt eine unberechtigte Löschung eines privat genutzten E-Mail-Accounts den Tatbestand des § 303a StGB (Datenveränderung) und kann mit einer Freiheitsstrafe oder mit einer Geldstrafe geahndet werden.

Was bedeutet das für die Praxis?

Dieser Fall zeigt deutlich, dass es unabdingbar ist, auch die private Nutzung vom geschäftlichen E-Mail Account ausdrücklich zu regeln. Dadurch könnten oben geschilderte Konsequenzen vermieden werden.





Facebook, Xing, Google+ – Soziale Netzwerke sind mittlerweile ein täglicher Begleiter und nicht mehr wegzudenken. Und viele Nutzer zeigen sich hier teils sehr öffentlich - auch in Äußerungen, die die Arbeitswelt betreffen.

Auch Arbeitgeber und Personalverantwortliche recherchieren inzwischen in sozialen Netzwerken nach Informationen über Bewerber.

Recherchen des Arbeitgebers in sozialen Netzwerken

Grundsätzlich ist die Informationsbeschaffung über einen Bewerber durch Recherchen in sozialen Netzwerken nicht erlaubt.

Eine Datenerhebung, -nutzung oder -verarbeitung ist generell nur erlaubt, wenn sie unmittelbar beim Betroffenen und mit dessen Wissen erfolgt.

Dies bedeutet im konkreten Bewerber-Fall, dass eine Recherche nur erlaubt ist, wenn der Bewerber auf bestimmte Netzwerke wie z. B. Xing verwiesen oder wenn er selbst Daten zum Zweck der Arbeitssuche, z. B. bei experteer.de eingestellt hat.

Nutzung sozialer Netzwerke durch den Arbeitnehmer

Grundsätzlich stellt sich die Nutzung sozialer Netzwerke am Arbeitsplatz nicht anderes dar als die Internetnutzung.

Jedoch wurden schon Arbeitnehmer aufgrund negativer Bekundungen in sozialen Netzwerken gekündigt. Beispielsweise bei beleidigenden oder vertragswidrigen Postings (z. B. Betriebs- und Geschäftsgeheimnisse). Besonders kritisch hierbei sind auch Äußerungen - vor allem negative - gegenüber Vorgesetzten und Kollegen.

Was bedeutet das für die Praxis?

Eine Betriebs- oder Dienstvereinbarung bzw. eine „Social Media Guideline“, in der Regeln und Empfehlungen für die Nutzung der sozialen Medien aufgestellt werden, ist für Mitarbeiter bindend und Konflikte in der Anwendung und deren Auswirkung können vermieden werden.

Aber auch hier gilt: Das Grundrecht der freien Meinungsäußerung darf nicht in Frage gestellt werden.

Sogenannte „Social Media Guidelines“ könnten beispielsweise zum Inhalt haben:

- Erlaubnis oder Verbot zur Nutzung sozialer Netzwerke während der Arbeitszeit
- Verhältnis zwischen dienstlicher und privater Nutzung
- Wahrung der Vertraulichkeit und Verschwiegenheit von Betriebsgeheimnissen
- Zulässige und unzulässige Inhalte
- Eigenwerbung bzw. Kritik an Wettbewerbern
- Umgang mit betriebsinterner Kritik
- Umgang mit rechtswidrigen Postings
- u.v.m.

Hierbei ist zu beachten, dass der Betriebsrat bei der Erstellung solcher Guidelines ein Mitbestimmungsrecht hat, da die Inhalte auch Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer betreffen.

Gerne informieren wir Sie ausführlich, was bei einer Betriebsvereinbarung oder bei „Social Media Guidelines“ zu beachten ist und unterstützen Sie bei der Erstellung.

Die zunehmende Videoüberwachung sowohl öffentlich als auch in Firmen soll eigentlich dem Schutz vor Vandalismus, Diebstahl oder anderer Eigentumsdelikten oder aber dem Schutz von Personen dienen. In der Regel ist es nicht Absicht der Videoüberwachung, die Beschäftigten zu beobachten und zu kontrollieren.

So werden in öffentlichen Stellen, in Kreditinstituten oder auch in Kassenbereichen sozusagen nebenbei auch Mitarbeiter überwacht. Ob beiläufig oder zielgerichtet - grundsätzlich gilt, dass die Videoaufzeichnung des Arbeitnehmerverhaltens nur in engen Grenzen zulässig ist.

In vielen Fällen der Videoüberwachung entstehen Interessenkonflikte zwischen Arbeitnehmer und Arbeitgeber.

Eine Videoüberwachung stellt generell einen Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers dar und ist daher grundsätzlich gesetzlich zu rechtfertigen.

Das Bundesdatenschutzgesetz gibt klare Richtlinien für die Videoüberwachung in öffentlichen und nicht-öffentlichen Räumen vor.

Die rechtliche Situation kurz gefasst:

- Auf einfachgesetzlicher Ebene regeln die Vorgaben der Datenschutzgesetze (§ 6b BDSG und §§ 32, 38 BDSG) die Videoüberwachung. Das heißt, Kameraüberwachung gilt grundsätzlich als verboten, eine Erlaubnis muss herbeigeführt bzw. die Überwachung muss mitgeteilt werden.
- Heimliches Filmen am Arbeitsplatz ist verboten. Für Strafverfolgungsbehörden ist dies jedoch im Rahmen von Ermittlungsverfahren mit richterlichem Beschluss möglich.
- Eine Überwachung von Sozialräumen, Umkleidekäben und sanitären Anlagen ist grundsätzlich nicht gestattet.
- Eine begrenzte Kameraüberwachung kann zu festgelegten Zwecken und unter Einhaltung gesetzlicher Vorgaben zulässig sein. Hierzu ist eine Verhältnismäßigkeitsprüfung erforderlich und falls eine Interessenvertretung existiert, eine Betriebs- oder Dienstvereinbarung.

Bei der Videoüberwachung lässt sich abschließend folgendes zusammenfassen:

Auf die Videoüberwachung muss hingewiesen werden

Erfolgt eine Videoüberwachung, sind die Mitarbeiter unbedingt darauf hinzuweisen. Die Überwachungsdaten können nur eingeschränkt verarbeitet und genutzt werden. Nicht mehr benötigte Daten sind unverzüglich zu löschen.

Mitbestimmung des Betriebsrats erforderlich

Der Betriebsrat hat die Videoüberwachung mitzubestimmen – auch im nicht öffentlichen Bereich. Dabei haben beide Seiten das Persönlichkeitsrecht der Arbeitnehmer zu beachten (§ 75 Absatz 2 BetrVG).

Arbeitgeber und Betriebsrat sind grundsätzlich befugt, eine Videoüberwachung im Betrieb einzuführen. Die Zulässigkeit des damit verbundenen Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer richtet sich nach dem Grundsatz der Verhältnismäßigkeit.

Eine Betriebsvereinbarung zur Videoüberwachung sollte es im Unternehmen unbedingt geben.

Folgen einer unerlaubten Video-Überwachung

Eine rechtswidrige Videoüberwachung kann eine strafbare Handlung nach § 201a StGB darstellen. Zudem können Unterlassungs-, Schadensersatz- und Schmerzensgeldansprüche von Arbeitnehmern geltend gemacht werden.

Folgendes Beispiel zeigt, dass die Folgen für den Arbeitgeber nicht unerheblich sind:

Vom Hessischen Landesarbeitsgericht wurde ein Arbeitgeber zur Zahlung einer Entschädigung von 7.000 EUR verurteilt, weil er eine Mitarbeiterin an ihrem Arbeitsplatz permanent mit einer Videokamera überwachte. Die Klägerin war Angestellte einer Niederlassung eines bundesweit aktiven Unternehmens. Eine Videokamera, die gegenüber der Eingangstür des Büros angebracht war, hatte auch den Arbeitsplatz der Mitarbeiterin im Fokus.



Datenschutz am Arbeitsplatz | Videoüberwachung



Die Mitarbeiterin machte mit ihrer Klage Schadensersatzansprüchen wegen Persönlichkeitsverletzung geltend. Der Arbeitgeber wurde zunächst vom Arbeitsgericht zur Zahlung einer Entschädigung von 15.000 EUR verurteilt.

Gegen dieses Urteil legte der Arbeitgeber Berufung ein, welche nur zum Teil Wirkung hatte. Der Arbeitgeber rechtfertigte sich damit, dass die Kamera nicht ständig in Funktion gewesen und nur zur Sicherheit der Mitarbeiter angebracht worden sei. Laut dem Arbeitgeber ist es wohl in der Vergangenheit schon zu Übergriffen auf Mitarbeiter gekommen.

Dennoch, so das Hessische Landesarbeitsgericht, sei der Eingriff in das allgemeine Persönlichkeitsrecht der Mitarbeiterin unverhältnismäßig.

Nach Meinung des Gerichts handle es sich um eine schwerwiegende Verletzung des informationellen Selbstbestimmungsrechts, die nach Abwägung aller Umstände die Verurteilung zu einer Entschädigung von 7.000 EUR rechtfertige. (Hess. LAG, Urteil vom 25. Oktober 2010 - 7 Sa 1586/09)

Was bedeutet das für die Praxis?

Eine Videoüberwachung im Betrieb ist nicht gänzlich ausgeschlossen, unterliegt aber gewissen Voraussetzungen und Bestimmungen. Der Betriebsrat darf auf keinen Fall übergangen werden und eine professionelle bzw. juristische Beratung ist von Anfang an zwingend erforderlich.

Die Videoüberwachung ist sehr brisant und sollte auf jeden Fall durch eine Betriebsvereinbarung, die die gesetzlichen Vorgaben einhält, abgesichert sein.

Fragen Sie uns um Rat - wir unterstützen Sie gerne!

Privatgespräche am Arbeitsplatz - auch außerhalb der Pausenzeiten - sind weit verbreitet und viele Mitarbeiter sind sich nicht im Klaren darüber, dass dies eigentlich verboten ist, denn der Mitarbeiter hat generell keinen Anspruch darauf, das geschäftliche Telefon auch privat zu nutzen.

Viele Arbeitnehmer dulden jedoch Privatgespräche über den geschäftlichen Telefonanschluss ihrer Mitarbeiter - auch über einen längeren Zeitraum (Konkludentes Handeln).

Dies hat jedoch nicht unerhebliche Auswirkung auf den Umgang und die Verwendung der personenbezogenen Daten.

Erlaubt der Arbeitgeber private Gespräche in einem gewissen Umfang und ist keine weitere Vereinbarung getroffen, so wird er juristisch betrachtet zum Telekommunikationsanbieter und darf diese Gespräche nicht speichern, verarbeiten oder überwachen.

Worauf sollte man achten?

Wenn einige Bedingungen beachtet werden, können bestimmte Daten über die Telefonnutzung des Mitarbeiters erfasst werden, ohne dass der Arbeitnehmer eine Persönlichkeitsverletzung geltend machen kann, die Schadensersatzansprüche oder Strafanzeige zur Folge haben kann.

Für den Arbeitgeber ist es deshalb auch hier unerlässlich, klar und deutlich zu regeln, was erlaubt ist und was nicht.

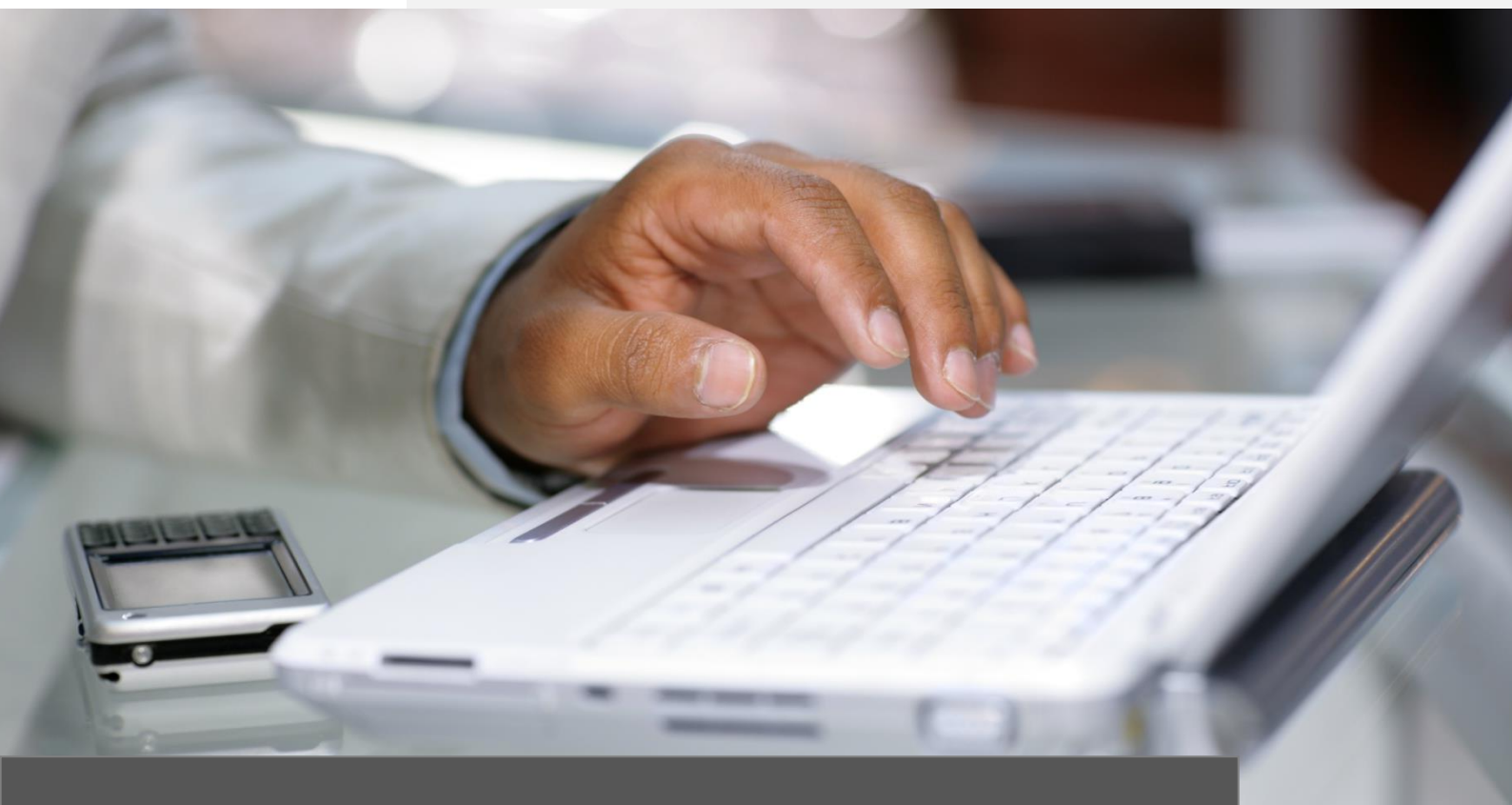
Im Arbeitsvertrag oder in einer Betriebsvereinbarung sollte festgehalten sein, in welchem Umfang eine private Telefonnutzung erlaubt ist, wie die Kontrollen der Nutzung erfolgen und welche personenbezogenen Daten hierfür verwendet werden. So können Ansprüche durch den Arbeitnehmer vermieden werden.

Fazit

Egal über welches Medium – ob Internet, E-Mail, soziale Netzwerke oder Telefon: Über kurz oder lang sollte in jedem Unternehmen verbindlich geklärt und vereinbart werden, in welcher Art und Weise die Mitarbeiter zur Nutzung betriebsinterner Kommunikationseinrichtungen befugt sind.

Wir beraten Sie gerne ausführlich, um rechtssichere Regelungen der Nutzung betriebsinterner Kommunikationseinrichtungen zu erstellen.

März | 2013



Impressum

DPN Datenschutz GmbH & Co. KG

Boisheimer Str. 65

41334 Nettetal

Tel.: (02153) 137 87 89

Fax: (02153) 137 87 84

Web: www.dpn-datenschutz.de

E-Mail: info@dpn-datenschutz.de

Amtsgericht Krefeld, HRA 6213

Ust-IdNr.: DE275528415

p.h.G.: DPN Verwaltung GmbH

Geschäftsführer: Fabio Pastars

Amtsgericht Krefeld, HRB 14208

Redaktion:

Fabio Pastars

Bildnachweise:

Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizenziert.

DPN

Datenschutz &
Informationssicherheit