

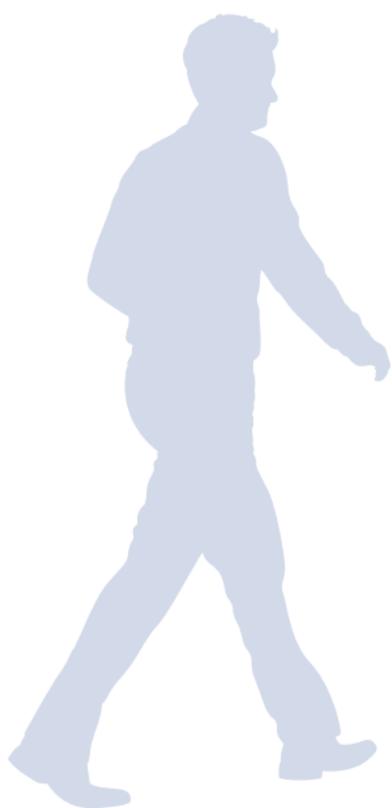


Die Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit



## Surfen am Arbeitsplatz Ein Datenschutz-Wegweiser





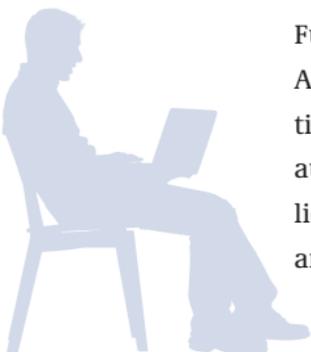
# Inhalt

Allgemeine Fragen zur Wahrung der Privatsphäre	4
Grundsätzliche Anforderungen	6
Allgemeines	6
Dienstliche Nutzung	7
Private Nutzung	8
Protokollierung des Internetzugangs	9

# Allgemeine Fragen zur Wahrung der Privatsphäre

Viele Beschäftigte haben heute Zugang zum Internet am Arbeitsplatz. Um diesen Dienst technisch zu ermöglichen, darf der Arbeitgeber die hierfür erforderlichen **personenbezogenen Daten** verarbeiten. Daten, die nur zur Gewährleistung der Datensicherheit benötigt werden, dürfen nur zu diesem Zweck vorübergehend protokolliert und ausgewertet werden. Arbeitgeber begründen ein darüber hinausgehendes Interesse an einer Kenntnisnahme und Auswertung dieser Daten oftmals damit, dass sich nur so Betriebsgeheimnisse wirksam schützen ließen. Schließlich habe der Arbeitgeber ein berechtigtes Interesse daran zu kontrollieren, ob ein Verbot der privaten Nutzung befolgt werde bzw. eine erlaubte private Nutzung sich in dem vorgesehenen Rahmen bewege. Damit ergeben sich vielfältige Fragen zur Wahrung der Privatsphäre der betroffenen Mitarbeiter. Die hier dargestellten Grundsätze sind sowohl für den privatwirtschaftlichen als auch für den behördlichen Bereich anwendbar.

Für die Beurteilung, ob und inwieweit der Arbeitgeber das Surfverhalten der Beschäftigten kontrollieren und überwachen darf, ist ausschlaggebend, ob ihnen neben der dienstlichen auch die private Nutzung des Internets am Arbeitsplatz gestattet ist.



Im Falle der nur **dienstlichen Nutzung** richtet sich die Zulässigkeit der Verarbeitung personenbezogener Daten nach dem Bundesdatenschutzgesetz. Danach sind das Recht des Beschäftigten auf informationelle Selbstbestimmung und die Interessen des Arbeitgebers an der vorgesehenen Datenverarbeitung gegeneinander abzuwägen. Auch wenn der Beschäftigte dem Direktionsrecht seines Arbeitgebers untersteht, kann er sich doch auf seine **Grundrechtspositionen** berufen.

Daraus ergibt sich, dass eine **Totalüberwachung** der Beschäftigten unverhältnismäßig und unzulässig wäre. Der Arbeitgeber darf aber eine stichprobenhafte und zeitnahe Auswertung der Protokolldaten vornehmen, wobei das Verfahren möglichst transparent zu gestalten ist.

Hat der Arbeitgeber die **private Nutzung** des Internets erlaubt, hat er das **Fernmeldegeheimnis** der Beschäftigten zu beachten. Danach dürfen die Daten nur verarbeitet und genutzt werden, soweit dies für die Erbringung des Internetdienstes und dessen Abrechnung erforderlich ist.





Da der Arbeitgeber ein berechtigtes Interesse daran hat, **Missbrauch oder strafbare Handlungen** nicht nur im dienstlichen Bereich, sondern auch bei der privaten Nutzung des dienstlichen Internetzugangs zu unterbinden, kann er die private Nutzung an bestimmte Bedingungen hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführender Kontrollen knüpfen. Entsprechende Regelungen sollten in einer Betriebs- bzw. Dienstvereinbarung unter Beteiligung des betrieblichen Beauftragten für den Datenschutz festgelegt werden. Die Beschäftigten sollten die Kenntnisnahme schriftlich bestätigen. Wenn der Beschäftigte die erforderlichen, in den Regelungen beschriebenen Kontrollmaßnahmen nicht will, muss er die private Nutzung unterlassen. Es gibt keinen Anspruch, das Internet privat am Arbeitsplatz nutzen zu können.

## Grundsätzliche Anforderungen

### Allgemeines

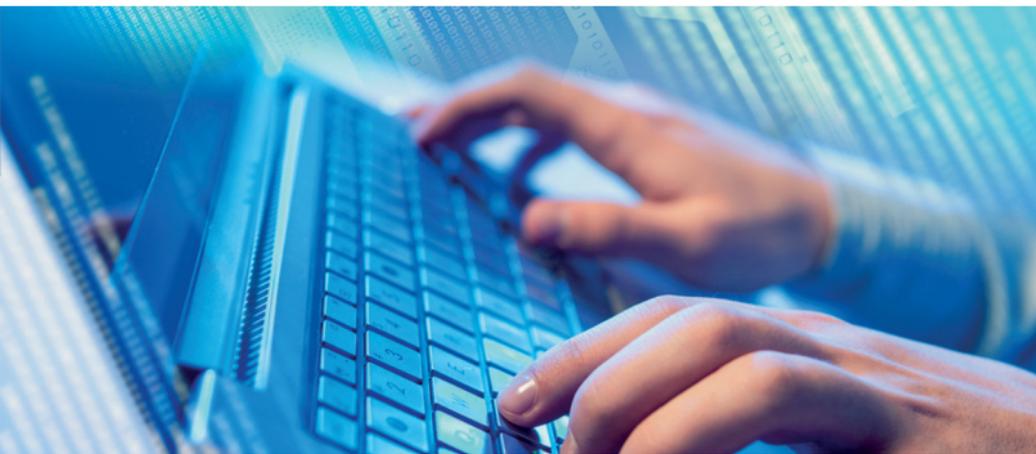
Bei der Nutzung von Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren entsprechend dem Grundsatz von Datenvermeidung und Datensparsamkeit



technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden. Ebenso sollte die Kontrolle der Nutzung so gestaltet werden, dass sie mit so wenigen personenbezogenen Daten wie möglich auskommt.

### Dienstliche Nutzung

Auch wenn der Arbeitgeber die Nutzung von Internetdiensten ausschließlich zu dienstlichen Zwecken gestattet, muss eine automatisierte Vollkontrolle als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten unterbleiben. Kontrollen sind nur stichprobenweise und bei konkretem Missbrauchsverdacht zulässig. Es sollte eine Betriebsvereinbarung abgeschlossen werden, in der die technischen und organisatorischen Fragen der Protokollierung und Auswertung eindeutig geregelt sind.



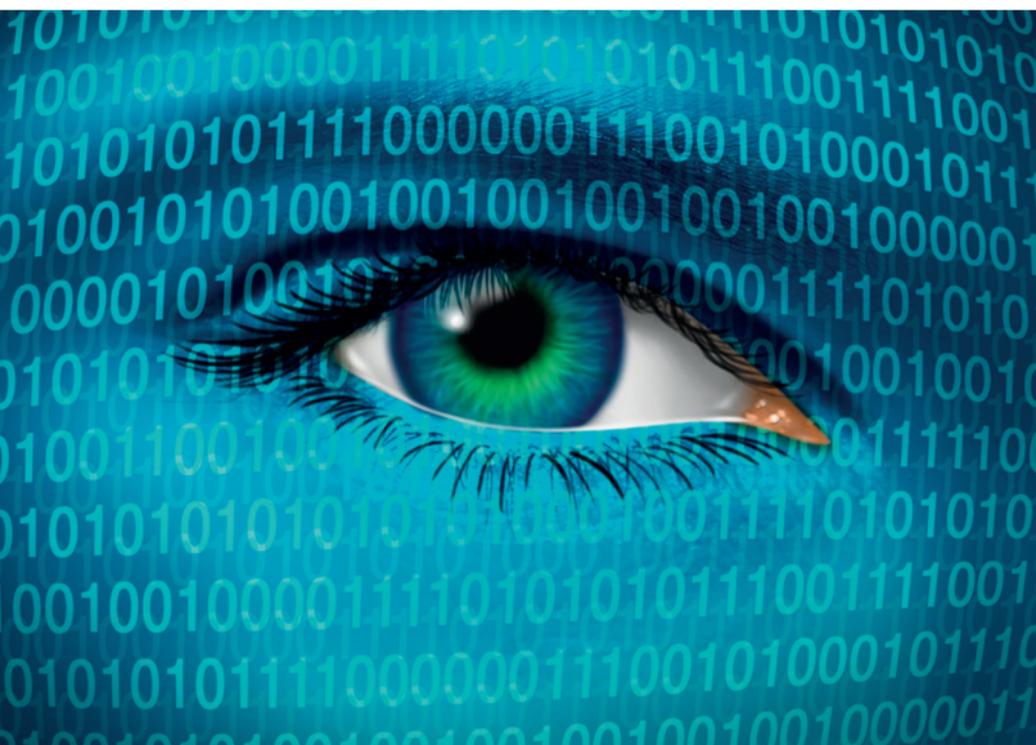
Soweit die Nutzung von E-Mail und Internetdiensten zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherung des ordnungsgemäßen Betriebes der Verfahren protokolliert wird, dürfen diese Daten nur für diese Zwecke genutzt werden. Eine Verwer-

tung zur Verhaltens- und Leistungskontrolle der Beschäftigten ist unzulässig.

### Private Nutzung

Gestattet der Arbeitgeber den Beschäftigten die private Nutzung des Internets, kann er dies an einschränkende Voraussetzungen knüpfen und in angemessener Weise kontrollieren. Dabei ist das Fernmeldegeheimnis zu beachten. Der Umfang der privaten Nutzung, ihre Bedingungen sowie die Kontrolle, ob diese Bedingungen eingehalten werden, müssen – am besten durch eine Betriebsvereinbarung – verbindlich geregelt werden.

Eine Protokollierung darf ohne Einwilligung nur erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherheit, zur Sicherung des ordnungsgemäßen Betriebs oder zu Abrechnungszwecken erforderlich ist. Die Verwendung der Protokolldaten zu anderen Zwecken ist unzulässig.



# Protokollierung des Internetzugangs

Proxy-Server/Web-Server können die Aktivitäten des einzelnen Beschäftigten im Internet umfangreich protokollieren. Diese Protokolle umfassen nicht nur die Benutzeridentifikation (z. B. IP-Adresse), Datum, Uhrzeit und Dauer der Internetnutzung sowie die übertragene Datenmenge. Anhand der Protokolle ist auch genau nachvollziehbar, wer was gelesen hat. Deshalb berühren diese Systemprotokolle das Persönlichkeitsrecht der Beschäftigten. Bei den meisten Servern ist es möglich, im Einzelnen festzulegen, was konkret protokolliert wird. Es ist zu prüfen, welche Angaben für welche Zwecke erforderlich sind. In vielen Fällen wäre es daher unverhältnismäßig, wenn systemseitige Voreinstellungen, die eine Vollprotokollierung vorsehen, einfach übernommen würden. Folgende Grundsätze sind zu beachten:

Der **Umfang der Protokolldaten** muss im Einzelnen festgelegt werden (z. B. Datum, Uhrzeit, Rechner- oder Benutzerkennung, Fehlercode, Anzahl der übertragenen Bytes, Rechner- oder Benutzeridentifikation, eventuell Zieladresse des angeforderten Dokuments, Fehlercode der Übertragung).



Die Verwendung der Protokolldaten muss an genau definierte Zwecke gebunden werden (z. B. Aufrechterhaltung der Systemsicherheit, Analyse und Korrektur technischer Fehler).

Der Zugriff auf die Protokolldaten muss auf das technische Personal begrenzt bleiben, das für den Netzbetrieb und die Bereitstellung der verfügbaren Dienste zuständig ist. Diese Personen sind zu verpflichten, die Zweckbindung und Vertraulichkeit zu beachten.

Die Speicherdauer der Protokolldaten wird so kurz gehalten, wie dies zur Erfüllung der Zwecke erforderlich ist (im Regelfall wenige Tage).

In begründeten Fällen von Missbrauch oder beim Verdacht strafbarer Handlungen kann eine weitergehende Einsicht in die Protokolldaten vorgenommen werden. Dabei sollte ein Verfahren gewählt werden, das die betroffene





Herausgeber:

Die Bundesbeauftragte für den Datenschutz  
und die Informationsfreiheit  
Husarenstraße 30  
53117 Bonn

Tel. +49 (0) 228 99 77 99-0  
Fax +49 (0) 228 99 77 99-550  
E-Mail: [referat24@bfdi.bund.de](mailto:referat24@bfdi.bund.de)  
Internet: [www.datenschutz.bund.de](http://www.datenschutz.bund.de)

Realisation: Appel & Klinger Druck und Medien GmbH, Schneckenlohe  
Bildnachweis: fotolia, shutterstock

Stand: März 2014

Dieser Flyer ist Teil der Öffentlichkeitsarbeit der BfDI. Er wird kostenlos abgegeben und ist nicht für den Verkauf bestimmt.