Workshop
Dienstvereinbarungen zur Internetnutzung / IT-Verträge der öffentlichen Hand

Teilnehmer	Herr Foerster	F+R
	Frau Rattmann	F+R
Ort	Kanzlei F+R	
Zeit	06.03.2007 (09:00 – 16:00 Uhr)	

FOERSTER+RUTOW®
RECHTSANWÄLTE
www.fr-lawfirm.com

Teil 1: Dienstvereinbarungen zur Internetnutzung

09:00 – 09:15	Begrüßung	
09:15 – 10:00	Rechtlicher Rahmen der Internetnutzung am Arbeitsplatz	
10:00 – 10:30	Vorstellung der Richtlinie der zentralen IuK-Leitstelle	
10:30 – 10:45	Pause	
10:45 – 12:00	Kritische Analyse vorgelegter Beispiele der Teilnehmer und Gestaltungsvorschläge anhand der Richtlinie für das Privatunternehmen	
12:00 – 13:00	Mittagessen im Restaurant „Kettensteg“	

Teil 2: IT-Verträge der öffentlichen Hand

13:00 – 13:30	Grundsätze des Vertragsdesigns: Deckblatt, Präambel, Definitionen, Anlagen	
13:30 – 14:00	Typische und atypische Verträge	
14:00 – 14:30	Arten von IT-Verträgen	
14:30 – 14:45	Pause	
14:45 – 15:15	Systementwicklungsvertrag	
15:15 – 15:45	Softwareentwicklungsvertrag	
15:45 – 16:00	Aktuelle Fragen zu Vertragsbeispielen aus dem IT-Service-Bereich	

Workshop
Dienstvereinbarungen zur Internetnutzung (Teil 1)
IT-Verträge der öffentlichen Hand (Teil 2)

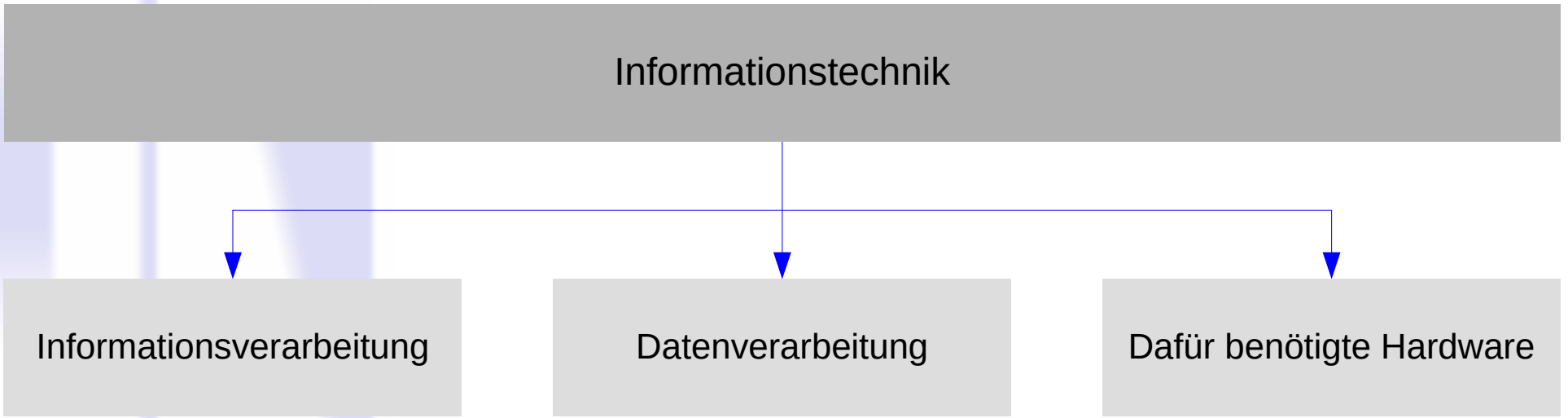
Rechtliche Aspekte in Behörden im Umgang mit E-Mail, Web und IT-Verträgen

Referenten: Viktor Foerster
Lisa Rattmann
www.fr-lawfirm.com

FOERSTER+RUTOW®
RECHTSANWÄLTE
www.fr-lawfirm.com

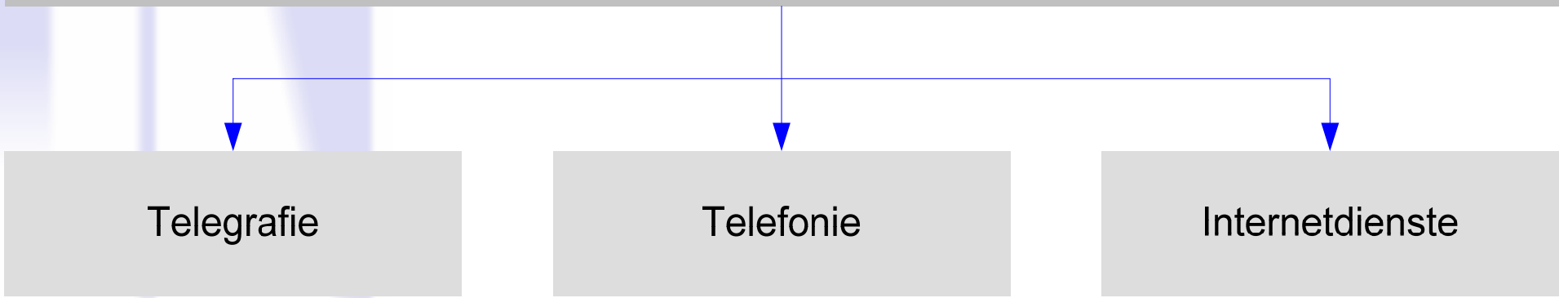
Begriffsklärung

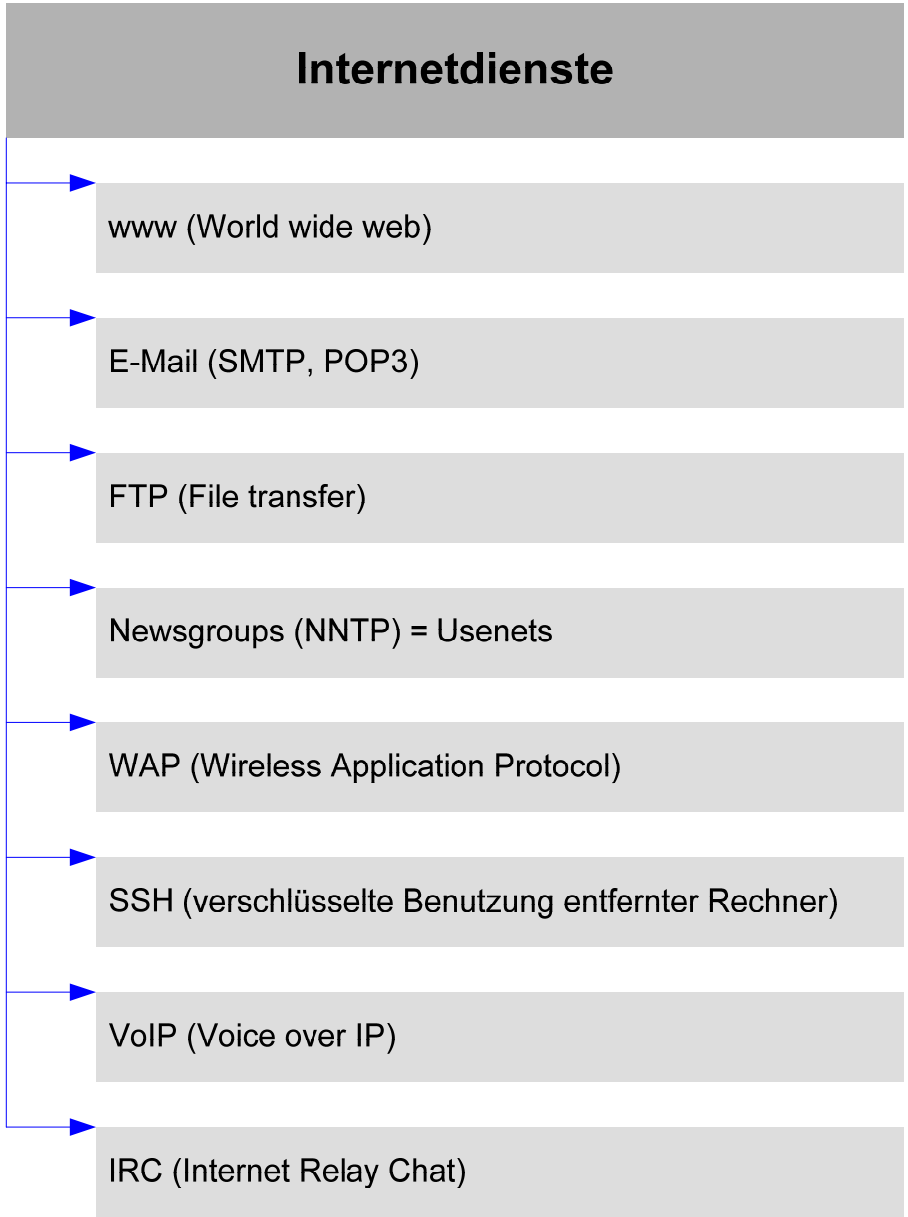
- IT
- Telekommunikation
- Internetdienste
- Betriebliche / betrieblich veranlasste / private Nutzung



Telekommunikation

Jeglicher Austausch von Informationen über eine gewisse Distanz hinweg, ohne sie materiell zu transportieren.





Nutzung von E-Mail & Internet

Betriebliche Nutzung

Internet dient der Erfüllung von Arbeitspflichten,

- z.B. bei Kommunikation mit Kunden oder Partnern
- über berufliche Belange mit Kollegen oder
- bei der Informationsbeschaffung für berufliche Aufgabenerfüllung
- Persönliche Grüße aus Anlass einer beruflichen eMail ändert nichts an der Einstufung als betriebliche Nutzung

Betrieblich veranlasste Nutzung

Internet wird zur Kommunikation im privaten Interesse genutzt, ist aber beruflich veranlasst: z.B.

- da Überstunden anfallen und private Verabredungen mit einer Email verschoben werden müssen,
- eine Terminvereinbarung während der Arbeitszeit aufgrund der Überschneidung der Arbeitszeiten notwendig ist.

Private Nutzung

Internet dient zur

- Kommunikation im privaten Interesse und
- zur Informationsgewinnung aus persönlichem Interesse und
- zum eigenen Abschluss von Verträgen, jeweils
- ohne Beziehung zur beruflichen Tätigkeit.

1. Begriffsklärung
2. Gesetzliche Grundlagen
3. Darstellung der Rechtsprechung bei privater Internetnutzung
4. Kontrolle der Internetnutzung

4.1 bei Verbot privater Nutzung

4.2 bei Erlaubnis privater Nutzung

5. Strafrechtliche Konsequenzen übermäßiger Kontrolle
6. IT-Richtlinie/Dienstanweisung/Dienstvereinbarung
7. Private Nutzung trotz Verbots - Konsequenzen

Internetnutzung

Gesetzliche Grundlagen			
Rechtsgrundlage	Arbeitnehmer (Privatunternehmen)	Angestellte (öffentlicher Dienst)	Beamte
Art. 2 Abs. 1, Art. 1 GG	Recht auf informationelle Selbstbestimmung Wirkt in das Arbeitsverhältnis über arbeitsrechtliche/beamtenrechtliche Generalklauseln, z.B. § 75 Abs. 2 BetrVG		
Individualarbeitsrecht	§§ 611, 242 BGB: Fürsorgepflicht des Arbeitgebers • Schutz der Handlungsfreiheit des Arbeitnehmers • Schutz der persönlichen Integrität (inkl. Privat- und Intimsphäre)		§ 48 BRRG, § 79 BBG, Art. 86 BayBG: beamtenrechtliche Fürsorgepflicht
Kollektives Arbeitsrecht	TVG – (Rahmen-) Tarifverträge	TVG – (Rahmen-) Tarifverträge	
	BetrVG – Betriebsvereinbarung	BPersVG/BayPVG - Dienstvereinbarung	BPersVG/BayPVG - Dienstvereinbarung
Bundesdatenschutzgesetz	Auffanggesetz für personenbezogene Daten (Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person)		
Telekommunikationsgesetz	Datenschutz hinsichtlich der Verbindungsdaten (Inhalt der Telekommunikation und ihre näheren Umstände) • Fernmeldegeheimnis, § 88 TKG • Maßnahmen zum Schutz des Fernmeldegeheimnisses, § 109 TKG		
Telemediengesetz	Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien: §§ 11 – 15 TMG • Grundsätze, § 12 TMG • Bestandsdaten, § 14 TMG • Nutzungsdaten, § 15 TMG		

1. Begriffsklärung
2. Gesetzliche Grundlagen
3. Darstellung der Rechtsprechung bei privater Internetnutzung
4. Kontrolle der Internetnutzung

4.1 bei Verbot privater Nutzung

4.2 bei Erlaubnis privater Nutzung

5. Strafrechtliche Konsequenzen übermäßiger Kontrolle
6. IT-Richtlinie/Dienstanweisung/Dienstvereinbarung
7. Private Nutzung trotz Verbots - Konsequenzen

Darstellung der Rechtsprechung

	Arbeitnehmer (Privatunternehmen)	Angestellter (öffentlicher Dienst)		Beamter
Urteil	BAG vom 07.07.2005	BAG vom 12.01.2006	BAG vom 27.04.2006	VG Düsseldorf vom 26.02.2003
Private Nutzung verboten	**Intranet-Startseite:** "Intranet und Internet nur zum dienstlichen Gebrauch" Hinweis auf Protokollierung und mögliche arbeitsrechtliche Folgen	**Dienstanweisungen:** • Nur dienstliche Software erlaubt • Nutzung des Rechners und des Internets nur zu dienstlichen Zwecken Hinweis auf mögliche arbeitsrechtliche Folgen		**Dienstanweisungen:** • Nutzung des Internets nur zu dienstlichen Zwecken • Einsatz von IT erst nach Freigabe des IT-Dezernats.
Dauer	Unbestimmt während der Arbeitszeit	Unbestimmt	50 Stunden während der Dienstzeit	160 Stunden während der Dienstzeit:
Beanstandetes Verhalten	• Surfen im Internet • Download porno-graphischer Videosequenzen und Bilder	Installation der Software-Programme JAVA und JAP zur Anonymisierung von Internet-Zugriffen auf Dienst-PC	Surfen, vorrangig auf pornografischen Seiten	Download von • Videodateien mit porno-graphischen Darstellungen und Szenen (3474 Videoclips, 3,8 GB) sowie • exe-Dateien, z.B. Moorhuhnjagd, Videoplayer.

Darstellung der Rechtsprechung

	Arbeitnehmer (Privatunternehmen)	Angestellter (öffentlicher Dienst)		Beamter
Urteil	BAG vom 07.07.2005	BAG vom 12.01.2006	BAG vom 27.04.2006	VG Düsseldorf vom 26.02.2003
Konsequenz	§ 626 BGB: außerordentliche Kündigung			Disziplinarmaßnahme
Ziel	Beendigung des Arbeitsverhältnisses			Wahrung von Funktionsfähigkeit und Ansehen des öffentlichen Dienstes
Grund für	an sich wichtiger Grund			disziplinare Relevanz
	Kündigungsrelevante Verletzung arbeitsvertraglicher Pflichten: • **unbefugter Download**, insb. bei Gefahr von Störungen des betrieblichen Betriebssystems sowie von möglichen Rufschädigungen • **private Nutzung an sich**, da möglicherweise zusätzliche Kosten und jedenfalls unberechtigte Inanspruchnahme von Betriebsmitteln • **private Nutzung während der Arbeitszeit** = Verletzung der Hauptleistungspflicht des AN (selbst bei Erlaubnis zur privaten Nutzung).			**Einzelfallentscheidung**, ob in einer privaten Nutzung des dienstlichen Internetzugangs bereits ein disziplinarrechtlich relevantes Fehlverhalten zu sehen ist. **Hier** ist wegen Dauer und Umfang die disziplinare Relevanz überschritten.
	Abmahnung nicht erforderlich, da • Rechtswidrigkeit der Pflichtverletzung (exzessive Nutzung /unbefugter Download) dem AN ohne weiteres erkennbar • Hinnahme des Verhaltens durch den AG offensichtlich ausgeschlossen			**Verweis** genügt, da • Formalverstöße gegen Dienstanweisungen • keine Verletzung des Kernbereichs der Dienstpflichten

Darstellung der Rechtsprechung

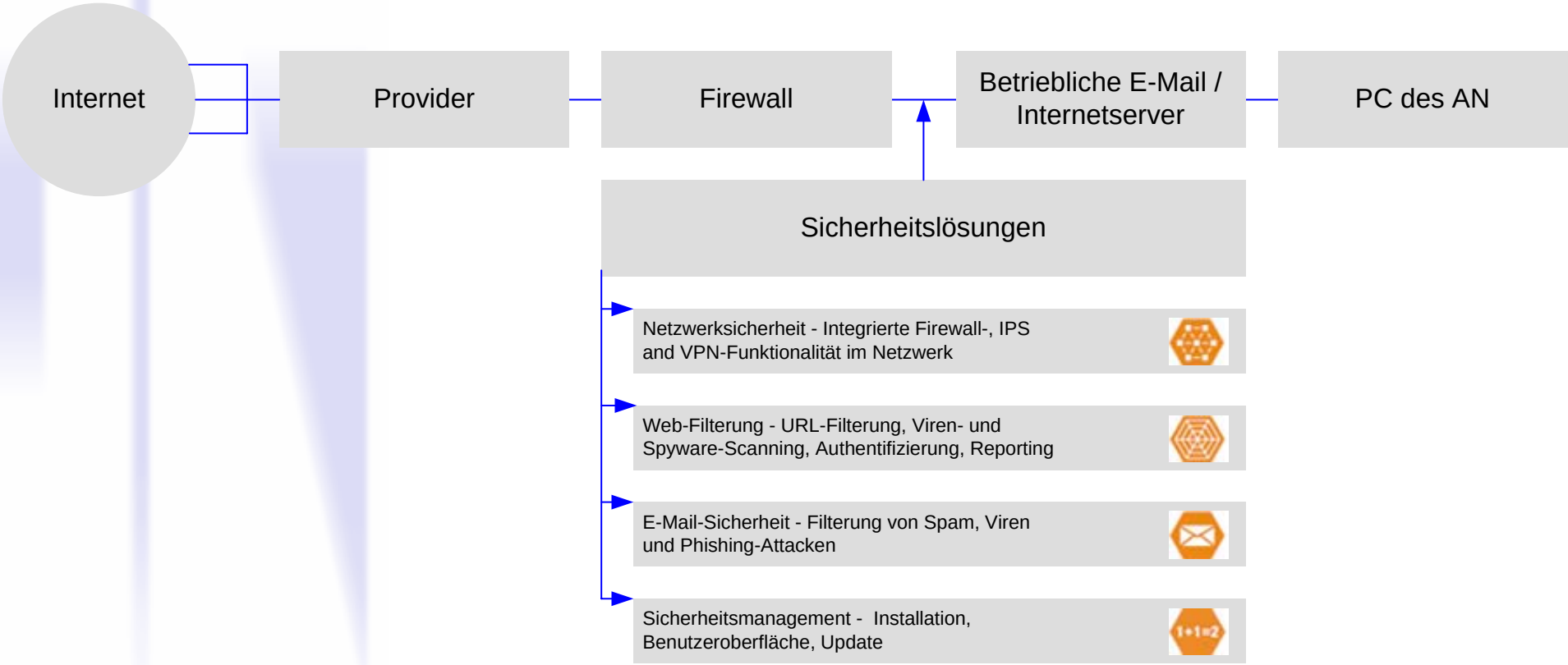
	Arbeitnehmer (Privatunternehmen)	Angestellter (öffentlicher Dienst)		Beamter
Urteil	BAG vom 07.07.2005	BAG vom 12.01.2006	BAG vom 27.04.2006	VG Düsseldorf vom 26.02.2003
Aspekte für die Beurteilung				
Positive Aspekte	• Bisherige beanstandungsfreie Dauer des Beschäftigungsverhältnisses • Regelung zur privaten Internetnutzung für den AN inhaltlich unklar • Tolerierung privater Internetnutzung in geringem Umfang?			Erstmaliger Pflichtenverstoß = einmaliges, persönlichkeits-fremdes Fehlverhalten
	Nicht zu Gunsten des Arbeitnehmers / Angestellten			Zu Gunsten des Beamten
	• keine messbare Verzögerung von Dienstgeschäften • keine zusätzlichen Kosten • keine strafrechtlich relevanten Sachverhalte, kein strafbares Vorgehen			
Negative Aspekte	• Schwere der Pflichtverletzung bei Nutzung während der Arbeitszeit (z.B. Dauer, Verletzung von Aufsichtspflichten) • Zusätzliche Kosten • Verletzung arbeitsvertraglicher Rücksichtnahmepflicht: Gefahr des Virenbefalls/Störungen des Betriebssystems • Bewusste Umgehung der Kontrollmöglichkeit des AG (Anonymisierungssoftware)			Hier nicht vorliegend: • Zusätzliche Kosten • Strafbarkeit des Verhaltens
		§ 8 Abs. 1 S. 1 BAT: gesteigerte Verhaltenspflichten gegenüber einem normalen Angestellten in der Privatwirtschaft		
	Zu Lasten des Arbeitnehmers / Angestellten			Nicht zu Lasten des Beamten
	Gefahr der Rufschädigung (insb. bei pornographischen Internetseiten)			Inhalt der Internetseiten – keine Ungleichbehandlung gleichartiger Pflichtenverstöße

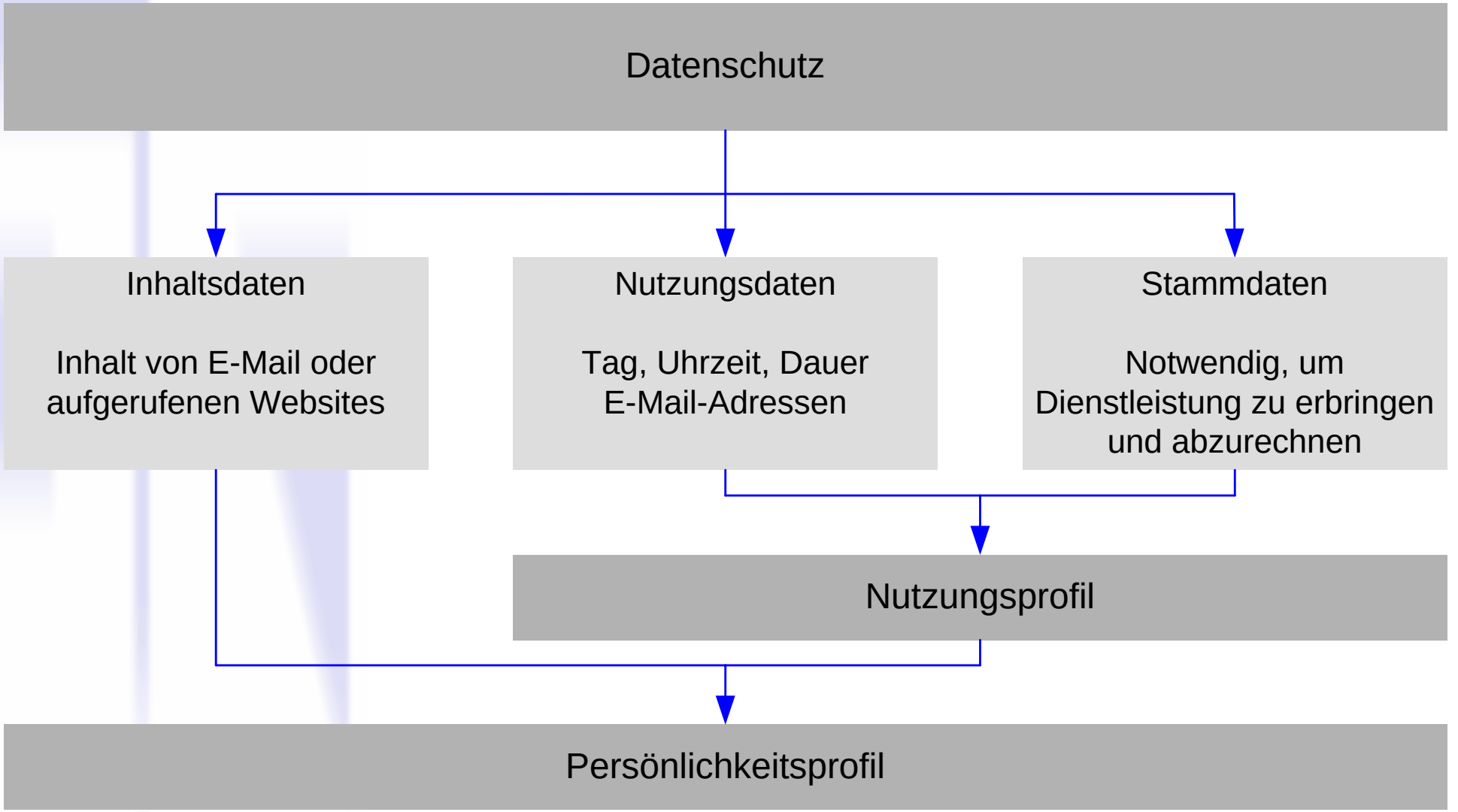
Auszug aus Urteil des VG Düsseldorf vom 26.02.2003

Die Dienstanweisung untersagt jede Art der privaten Nutzung und macht dies nicht etwa davon abhängig, ob es sich um Internetseiten mit pornographischem Inhalt oder anderen Inhalten handelt. Ebenso wenig kommt es für das Gewicht der Pflichtenverstöße darauf an, ob der Dienstvorgesetzte den Inhalt solcher Internetseiten, wie sie der Beamte aufgerufen hat, für anstößig oder unmoralisch hält. Anderenfalls würde dies im Ergebnis zu einer Zensur des Inhalts von Internetseiten und damit auch zu einer Ungleichbehandlung gleichartiger Pflichtenverstöße führen, was mit dem geltenden Dienstrecht nicht vereinbar wäre.

1. Begriffsklärung
2. Gesetzliche Grundlagen
3. Darstellung der Rechtsprechung bei privater Internetnutzung
4. Kontrolle der Internetnutzung
4.1 bei Verbot privater Nutzung
4.2 bei Erlaubnis privater Nutzung
5. Strafrechtliche Konsequenzen übermäßiger Kontrolle
6. IT-Richtlinie/Dienstanweisung/Dienstvereinbarung
7. Private Nutzung trotz Verbots - Konsequenzen

Kontrolle der Internetnutzung der Angestellten/Beamten





Datenschutz bei Verbot privater Nutzung

↓

Bundesdatenschutzgesetz §§ 3a, 4, 27, 28, 31
Bayerisches Datenschutzgesetz

Möglichkeit zu
- stichprobenartigen Kontrollen
- Aufforderung, die dienstlichen Mails zugänglich zu machen, d.h. inhaltliche Kontrolle
- Kontrolle der Verbindungs- und Inhaltsdaten
- Bestellung eines Datenschutzbeauftragten

Konsequenzen einer Erlaubnis privater Nutzung

1. AG = Anbieter von TK-Dienstleistungen
2. Ohne physische Trennung zwischen betrieblicher und privater Kommunikation → alles privat

TKG (Telekommunikationsgesetz)	TMG (Telemediengesetz)	BDSG (Bundesdatenschutzgesetz)
Telekommunikationsgeheimnis gem. § 88 TKG - Keine SPAM- und Viren-Filterung von E-Mails - Keine Content-Control-Maßnahmen - Keine Einsicht in E-Mail-Kommunikation der Beschäftigten - Keine Einsicht und Speicherung der angewählten Adresse → lediglich Protokollierung der äußeren Verbindungsdaten	Protokollierung nur für - Entgeltabrechnung - Gewährleistung störungsfreien Betriebs - Aufklärung strafrechtlichen Verhaltens durch StA	Bestellung eines Datenschutzbeauftragten (§ 4 f. BDSG) regelt die Verbreitung der zulässig erhobenen Daten (z.B. E-Mail-Adresse der Angestellten/Beamten auf der Homepage)
Ausnahme: Einwilligung der Beschäftigten in Protokollierung	Einwilligung der Beschäftigten zur Auswertung erforderlich	
Absicherung der (techn.) Daten gg. den unbefugten Zugriff Dritter, § 109 TKG	Sicherstellung der Anonymität der Verbindungsdaten	

Strafrechtliche Konsequenzen übermäßiger Auswertung / Filterung

§ 44 BDSG vorsätzl. unbefugte Datenerhebung gg. Entgelt / mit Bereicherungsabsicht
§ 202 a StGB Ausspähen von Daten
§ 303 a StGB Datenveränderung

Bei erlaubter privater Nutzung zusätzlich:
§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses bei Filterung und Löschen von EMails (SPAM-Filter) nur bei erlaubter priavter E-Mail-Nutzung (Anw. des TKG)

Schutz vor Strafbarkeit nach §§ 206, 303 a StGB: Einwilligung des Angestellten/Beamten

Beschluss des OLG Karlsruhe vom 10.01.05: Strafbarkeit des Ausfilterns von E-Mail

Sachverhalt:

Sperrung sämtlicher E-Mails, in deren Absenderadresse der Name des ausgeschiedenen Mitarbeiters vorgekommen ist, und zwar auch dann, wenn die E-Mails von anderen Accounts kamen.

Es war nicht schon der Verbindungsaufbau gesperrt. Die E-Mails wurden ordnungsgemäß angenommen, quittiert und in den Verantwortungsbereich der Fakultätssysteme übernommen. Erst einige Minuten später wurden sie fakultätsintern ausgefiltert. Der Antragsteller erhielt verzögert die Meldung "delivery cancelled". Der potentielle Empfänger erhielt von der Nachricht gar nichts.

Sperrung auch solcher E-Mails betroffen, die von Mitarbeitern der Fakultät an den Antragsteller gesendet wurden, d.h. bei denen der Antragsteller Empfänger war, auf dem Verteiler stand oder nur im Betreff erwähnt wurde, d.h. in deren Kopfzeile "C" vorgekommen ist. Hiervon waren sämtliche Mitarbeiter der Fakultät betroffen, ohne vorher befragt oder informiert worden zu sein.

Beschluss des OLG Karlsruhe vom 10.01.05: Strafbarkeit des Ausfilterns von E-Mail

2a. Der Begriff des Unternehmens i.S.v. § 206 StGB ist weit auszulegen. Hierunter ist jede Betätigung im geschäftlichen Verkehr anzusehen, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist.

2b. Stellt eine Hochschule ihre Telekommunikationseinrichtungen zur Versendung und Empfang elektronischer Post (E-Mail) ihren Mitarbeitern und anderen Nutzergruppen auch für private und wirtschaftliche Zwecke zur Verfügung, so wird sie damit außerhalb ihres hoheitlichen Aufgabengebietes tätig und ist als Unternehmen i.S.v. § 206 StGB anzusehen.

3a. Dem Tatbestandsmerkmal "unbefugt" kommt in § 206 StGB eine Doppelfunktion zu. Ein Einverständnis schließt bereits die Tatbestandsmäßigkeit des § 206 StGB aus, im übrigen handelt es sich um ein allgemeines Rechtswidrigkeitsmerkmal.

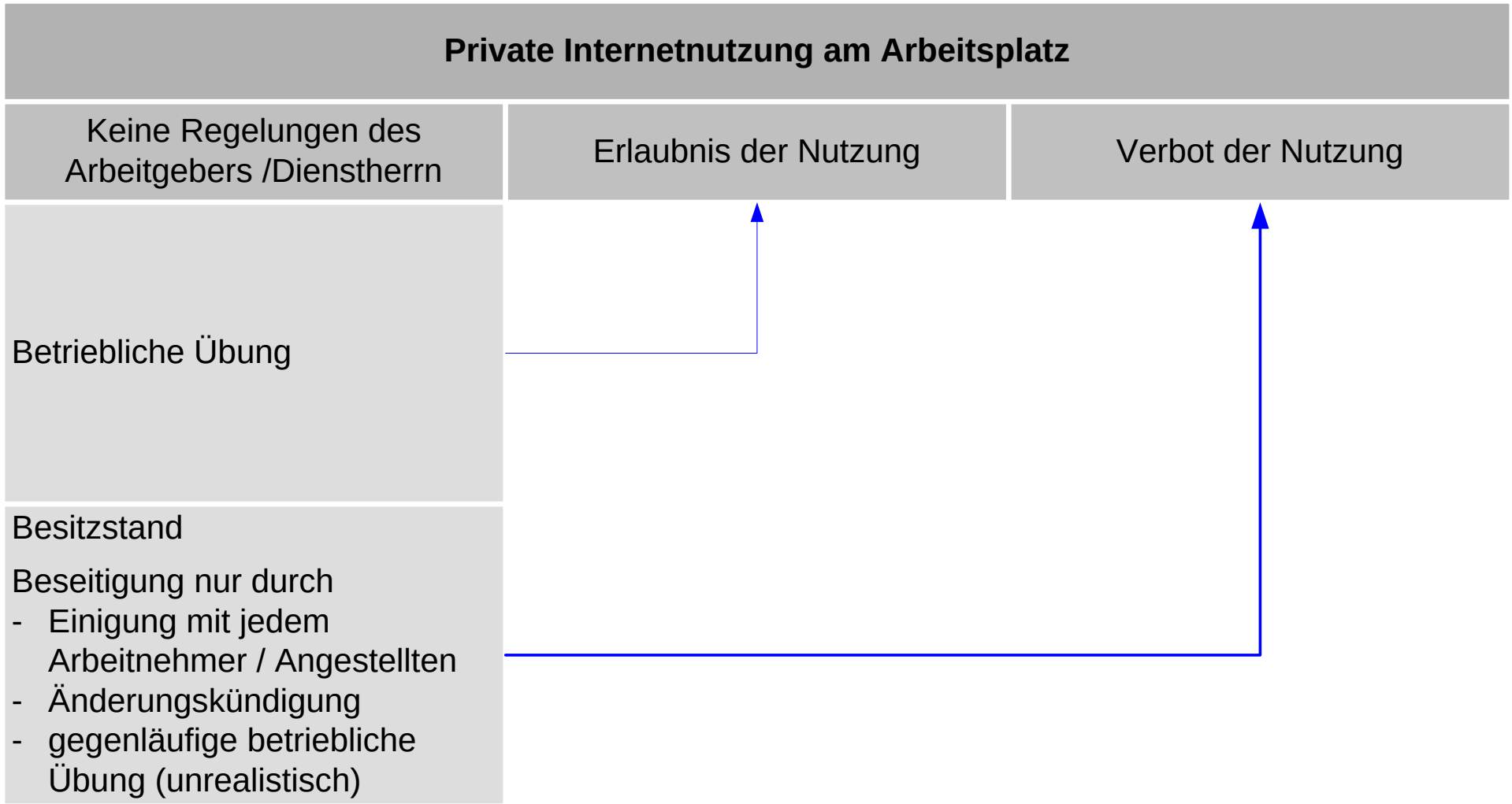
3b. Als Rechtfertigungsgründe für Eingriffe in das Post- und Fernmeldegeheimnis kommen Erlaubnissätze in Betracht, die in einer gesetzlichen Vorschrift, d.h. in einem formellen Gesetz oder einer Rechtsverordnung niedergelegt sind, und die sich ausdrücklich auf Postsendungen, den Postverkehr oder Telekommunikationsvorgänge beziehen. Auch ein Rückgriff auf allgemeine Rechtfertigungsgründe ist möglich, so dass das technische Herausfiltern einer E-Mail gerechtfertigt sein kann, wenn ansonsten Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten können.

1. Begriffsklärung
2. Gesetzliche Grundlagen
3. Darstellung der Rechtsprechung bei privater Internetnutzung
4. Kontrolle der Internetnutzung

4.1 bei Verbot privater Nutzung

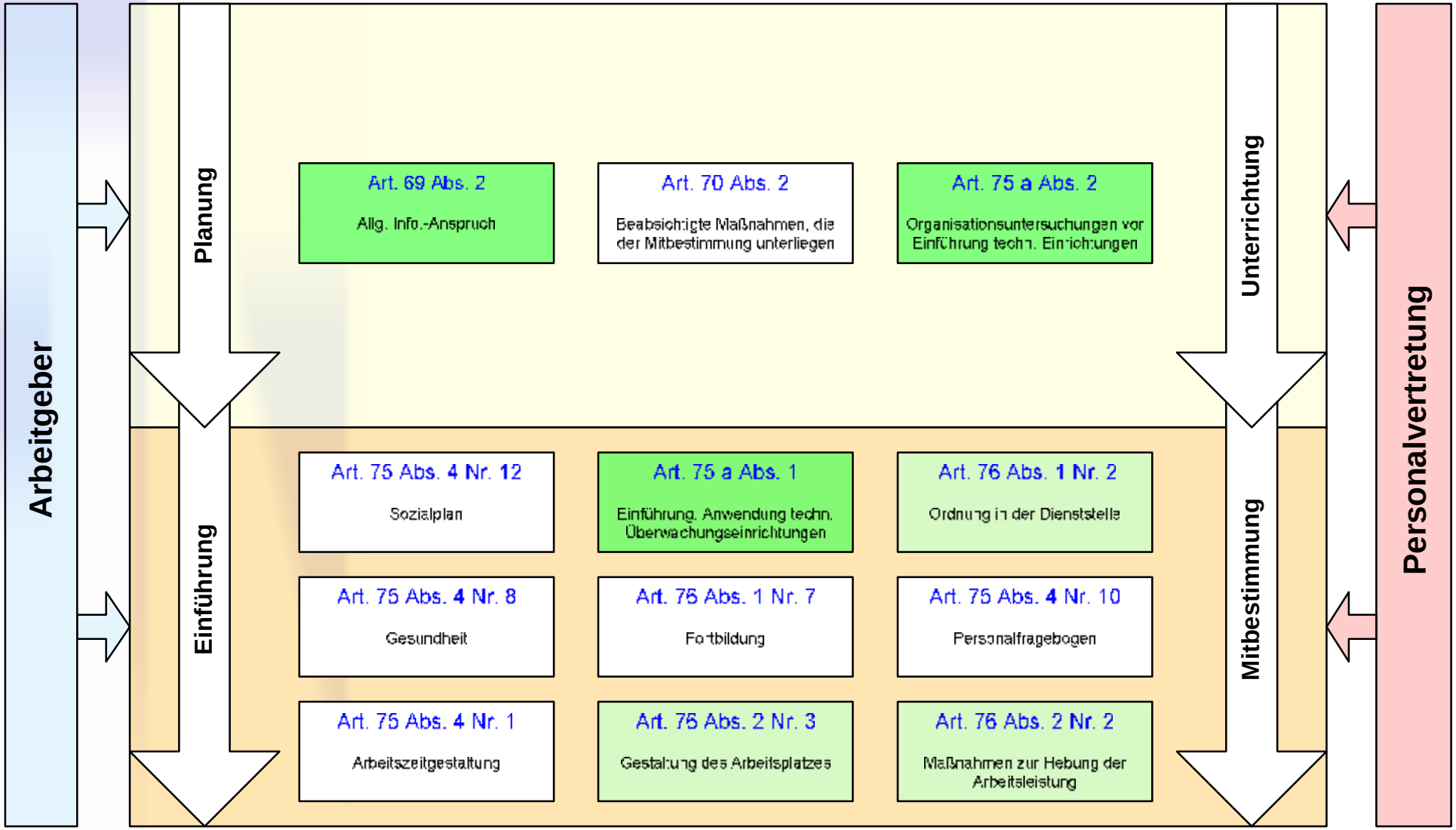
4.2 bei Erlaubnis privater Nutzung

5. Strafrechtliche Konsequenzen übermäßiger Kontrolle
6. IT-Richtlinie/Dienstanweisung/Dienstvereinbarung
7. Private Nutzung trotz Verbots - Konsequenzen



Regelung des Verbots der privaten Nutzung		
Angestellte (Privatunternehmen)	Angestellte (öffentlicher Dienst)	Beamte
Arbeitsvertrag		-
Direktionsrecht	Weisungsrecht	
• Richtlinie (ArbV) • Betriebsvereinbarung	• Dienstanweisung • Dienstvereinbarung	
Mitwirkung		
Betriebsrat	Personalvertretung	
• § 87 I Nr. 1, 6 BetrVG • § 90 I Nr. 2, 4 BetrVG	Art. 75a Abs. 1 BayPVG	

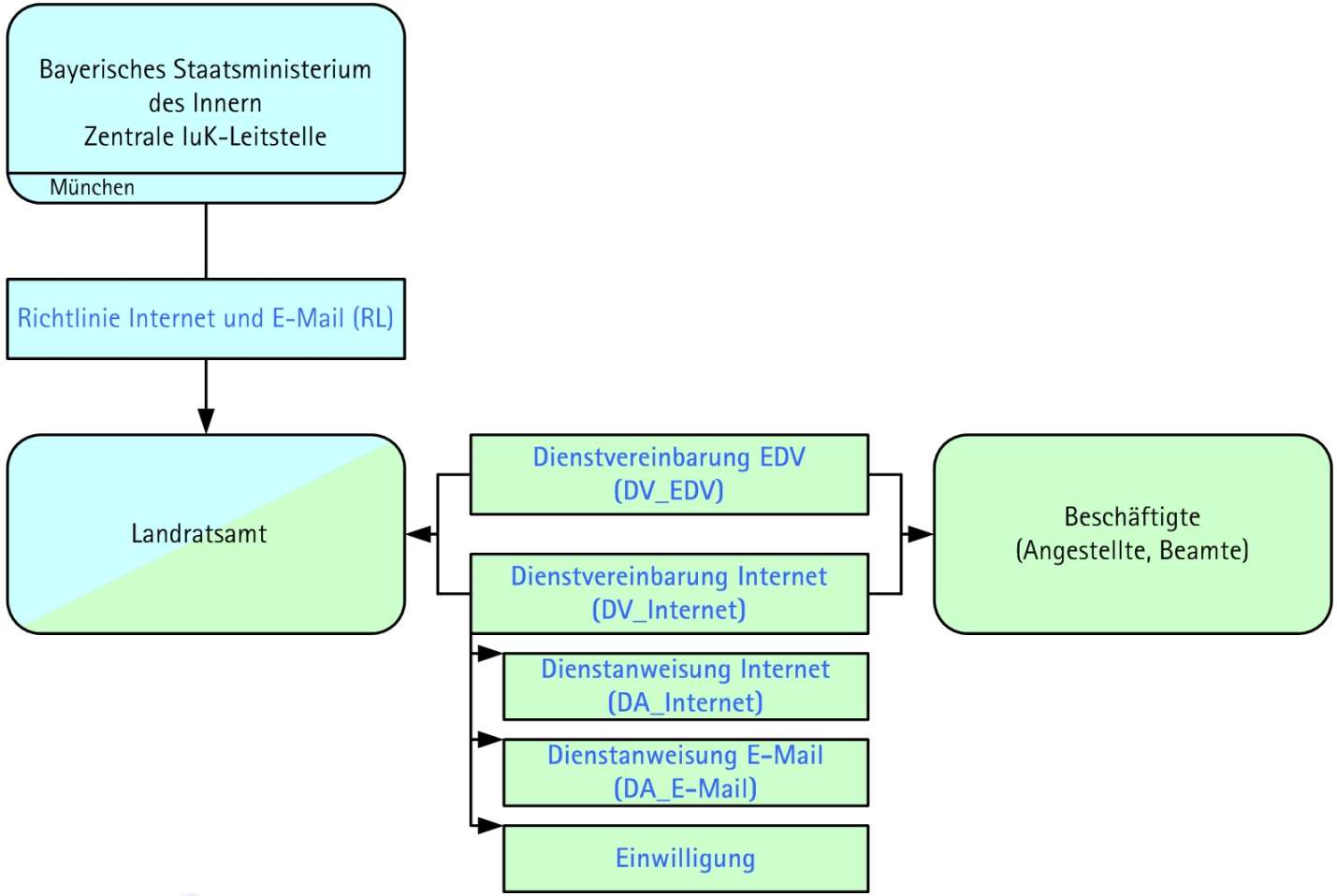
Informations- und Mitbestimmungsrechte



Die Artikelangaben beziehen sich auf das BayPVG in der Fassung vom 11. November 1986, zuletzt geändert am 23.5.2006

- Gültigkeitsbereich: Bayerische Behördennetz Verbindlichkeit für die an das BYBN angeschlossenen Behörden
  - staatlichen Behörden, soweit sie in den Anwendungs-bereich der Richtlinie fallen (Nr. 2)
  - andere Nutzer des Bayerischen Behördennetzes kraft Beitrittserklärung.
- Eine direkte Wirkung ihrer Regelungen gegenüber den Beschäftigten der Dienststelle besteht nicht.
- Als Richtschnur geeignet, da sie sich an den Empfehlungen des von Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutzhandbuchs orientiert.

Richtlinie der zentralen IuK-Leitstelle



Regelung der privaten Nutzung

•Aufbau einer Informationssicherheitsrichtlinie im Privatunternehmen

Kriterien:

- Private Nutzung
- Protokollierung der Internet- und E-Mail-Nutzung
- Verschlüsselung/Schriftform/digitale Signatur
- Passwörter
- Allgemeine Anmerkungen

IT-Sicherheitsrichtlinie (Privatunternehmen)

Verbot privater Nutzung:

LAN, Internet & Email

Umfang und Art der Nutzung

Die Nutzung des LAN, des Internets und der Versand und Empfang von E-Mails ist ausschließlich für dienstliche Zwecke erlaubt. Eine private Nutzung ist nicht zulässig. Die gesetzlichen Bestimmungen insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts sind zu beachten. Es ist insbesondere verboten, pornographische, Gewalt verherrlichende oder rassistische Inhalte aufzurufen oder zu versenden.

Protokollierung

Zugriffe und Datenverkehr im LAN und Internet unterliegen einer automatischen Protokollierung. Die Protokolle dienen primär technischen Zwecken, wie z.B.

- der Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit
- Statistische Feststellung des Nutzungsvolumens.

Die Geschäftsleitung behält sich aber das Recht vor, den Gebrauch des Internets und die Einhaltung dieser IT-Richlinie durch die Mitarbeiter durch Auswertung der Protokolle stichprobenartig oder bei Verdacht einer unerlaubten Nutzung zu überprüfen.

Regelungen in den Dienstanweisungen:

- 2 Landratsämter haben diese komplett verboten.
- 1 Landratsamt hat überhaupt keine Regelung
- 1 Landratsamt (LRA) hat die private Nutzung
  - des Internet verboten
  - von E-Mail / Fax grundsätzlich nur zu dienstlichen Zwecken gestattet. “Ausnahmen sind nur dann erlaubt, wenn dem Amt hierdurch keine Kosten entstehen und der Versand auf ein vernünftiges Maß beschränkt bleibt.“

Rechtliche Konsequenz:

- LRA mit Verbot: nur betriebliche Mails
- LRA ohne Regelung: betriebliche Übung
- LRA mit “Ausnahme“: Es gibt private Mails. Da die Trennung zwischen privaten und dienstlichen Mails nicht möglich ist, sind alle Mails privat.

Kriterien:

- Private Nutzung
- Protokollierung der Internet- und E-Mail-Nutzung
- Verschlüsselung/Schriftform/digitale Signatur
- Passwörter
- Allgemeine Anmerkungen

- **LRA mit Verbot:** Protokollierung unproblematisch; nur nicht zu Leistungskontrolle gestattet.

- **LRA ohne Regelung**: Werden hier Kontrollen durchgeführt und hat sich hier trotz der Annahme, dass “vom Grundsatz her… der Gebrauch des Internets und E-Mail-Systems ausschließlich zu dienstlichen Zwecken erlaubt“ ist, die gegenteilige **betriebliche Übung** herausgebildet, so ist die Protokollierung unzulässig, da keine Einwilligung der Bediensteten erfolgte.

- Das LRA mit der **ausnahmsweise erlaubten E-Mail-Nutzung** führt “Protokolldateien über ein- und auslaufende E-Mails/Faxe“ durch das E-Mail-/Fax-System durch. Eine Einwilligung besteht unseres Wissens auch hier nicht.

  → Protokollierung rechtswidrig

Einwilligung in Protokollierung

- Nur durch Individualvereinbarung
- Vor dem Datenverarbeitungsvorgang
- Erforderliche Angaben:
  - Welche Aufgaben werden protokolliert
  - Für welche Zwecke
  - Wo werden sie gespeichert
  - Wem werden sie zugänglich gemacht
- Schriftform, optisches Abheben von anderen Erklärungen, § 4a I 3, 4 BDSG

Einwilligungserklärung nach IuK-Leitstelle:

Ich möchte von dem Angebot meiner Dienststelle Gebrauch machen, Web-Dienste (WWW-Dienst, E-Mail-Dienst) (ggf. nur WWW-Dienst) in geringfügigem Umfang auch für private Zwecke zu nutzen, z.B. für die Internetrecherche. Mir ist bekannt, dass jede Nutzung unzulässig ist, durch die gewerbliche oder geschäftsmäßige Interessen verfolgt werden oder die den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit schaden oder die Sicherheit des Behördennetzes beeinträchtigen kann. Dies gilt vor allem für das Abrufen oder Verbreiten von Inhalten, die gegen strafrechtliche. Datenschutz-rechtliche, persönlichkeitsrechtliche, lizenz- oder urheberrecht-liche Bestimmungen verstoßen. Dies gilt weiter für das Abrufen oder Verbreiten von verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden, pornographischen, beleidigenden oder verleumderischen Inhalten.

Einwilligungserklärung nach IuK-Leitstelle:

- Ggf. ergänzen um weitere organisatorische Einschränkungen -

Ich willige ein, dass auch meine privaten - also nicht nur die dienstlichen – Internetzugriffe (ggf. ergänzen um "sowie der gesamte dienstliche und private E-Mail-Verkehr") protokolliert werden und dass die Protokolldaten stichprobenartig oder im Einzelfall bei konkretem Verdacht einer missbräuchlichen Nutzung überprüft werden können, um eine missbräuchliche Nutzung feststellen zu können. Ich willige ferner ein, dass meine privaten E-Mails hinsichtlich der Behandlung virenverseuchter E-Mails und unerwünschter Werbung (Spam) wie die dienstlichen E-Mails behandelt werden und gegebenenfalls gelöscht werden. Mir ist bekannt, dass meine Dienststelle die Gestattung der Privatnutzung jederzeit widerrufen kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen mit der Folge, dass ich ab Widerruf die Internetzugriffsmöglichkeit nicht mehr privat nutzen darf.

Diese Einwilligungserklärung wird in den Personalakt aufgenommen.

Bei der Einwilligungserklärung nach Richtlinie der Zentralen IuK-Leitstelle ist nach unserer Auffassung zu ergänzen:

- dass eine inhaltliche Protokollierung der Internetseiten und E-Mails stattfindet und nicht nur die Verbindungsdaten protokolliert werden;
- wo und wie lange die protokollierten Daten gespeichert werden;
- wer die stichprobenartige Kontrolle bzw. die Kontrolle im konkreten Verdachtsfall einer missbräuchlichen Nutzung vornehmen darf (Kontrolle durch berechtigte Mitarbeiter der EDV-Station, Beteiligung der Personalvertretung gem. Art. 75a Abs. 1 Nr. 1 BayPersVG, nachträgliche Information des Benutzers).

Kriterien:

- Private Nutzung
- Protokollierung der Internet- und E-Mail-Nutzung
- Verschlüsselung/Schriftform/digitale Signatur
- Passwörter
- Allgemeine Anmerkungen

Art. 3a BayVwVfG: Elektronische Kommunikation

Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

[1] Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. [2] In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. [3] Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht ermöglicht, ist nicht zulässig.

[1] Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. [2] Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

- Signaturgesetz
- Signaturverordnung

Das LRA ohne Regelung der E-Mail-Nutzung hat keinen Hinweis für seine Bediensteten, dass eine Versendung personenbezogener Daten per E-Mail nur verschlüsselt zulässig ist und sonst nur per Post.

Kriterien:

- Private Nutzung
- Protokollierung der Internet- und E-Mail-Nutzung
- Verschlüsselung/Schriftform/digitale Signatur
- Passwörter
- Allgemeine Anmerkungen

Individuelle Passwörter dürfen von dem Mitarbeiter frei vergeben werden. Jedes Passwort muss den Komplexitätsstandard erfüllen und regelmäßig alle 3 Monate geändert werden. Der Mitarbeiter hat dafür Sorge zu tragen, dass keine weitere Person Kenntnis von seinem individuellen Passwort gelangt. Eine schriftliche Fixierung der individuellen Passwörter ist nur zum Zwecke der sicheren Hinterlegung in einem verschlossenen Umschlag bei der IT-Abteilung gestattet.

Komplexitätsstandard für Passwörter bedeutet, dass diese

- mindestens 8 Zeichen,
- keine erkennbare personenspezifischen Inhalte (z.B. Namen, Kfz-Kennzeichen, Geburtsdatum) und
- mindestens ein Sonderzeichen aufweisen müssen.

Erlangt der Mitarbeiter Kenntnis davon, dass ein Unbefugter Kenntnis von einem individuellen oder gemeinsamen Passwort erlangt hat, hat er das Passwort sofort zu ändern und unverzüglich einen IT-Verantwortlichen zu informieren.

Behandlung von Kennwörtern

Das Kennwort soll die maximal mögliche Länge haben, jedoch mindestens 6 Zeichen. Leicht zu erratende Buchstaben- bzw. Ziffernkombinationen (Kfz.-Kennzeichen, Telefonnummern, usw.), ferner sogenannte triviale Kennwörter (z. B. AAAAAA, 123456) sind nicht zulässig. Nach Möglichkeit sollen willkürliche Kombinationen verwendet werden. Das Kennwort soll aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Es muss drei dieser Klassen“ beinhalten.

Das persönliche Kennwort muss in regelmäßigen Zeitabständen geändert werden. Rechtzeitig vor Ablauf einer vorgegebenen Frist fordert das System den Zugriffsberechtigten bei der Dialogeröffnung zur Änderung des Kennwortes auf. Nach Ablauf der Frist ist eine Anmeldung erst mit einem neuen Kennwort möglich. Hierbei kann das selbe Kennwort nicht noch einmal verwendet werden. Alte Kennwörter können nach einem Kennwortwechsel nicht mehr verwendet werden.

Behandlung von Kennwörtern

Bei einem Personalwechsel ist der IuK-Bereich durch den jeweiligen Sachgebietsleiter unverzüglich zu informieren, um das Kennwort der alten Benutzerkennung zu löschen und für den neuen Benutzer der Kennung ein neues Kennwort zu vergeben. Für die zentralen Dienste sind hierfür die Leiter der jeweiligen Arbeitsbereiche zuständig.

Kennwörter dürfen nur eingegeben werden, wenn sichergestellt ist, dass Dritte keine Gelegenheit zur Kenntnisnahme haben. Kennwörter dürfen nicht aufgezeichnet und nicht weitergegeben werden (auch nicht innerhalb des Sachgebietes).

Ist eine missbräuchliche Verwendung von Kennwörtern bekannt geworden oder ist sie wegen Kenntnisnahme von Kennwörtern durch Unbefugte zu befürchten, so ist das Kennwort sofort zu ändern.

Kriterien:

- Private Nutzung
- Protokollierung der Internet- und E-Mail-Nutzung
- Verschlüsselung/Schriftform/digitale Signatur
- Passwörter
- Allgemeine Anmerkungen

- Definitionskalender / Abkürzungsverzeichnis
- Vermeidung widersprüchlicher Aussagen in verschiedenen Dienstvereinbarungen /-anweisungen

Regelungen in verschiedenen Dienstanweisungen (DA) eines Landratsamtes

- **DA EDV:**

  …Aus diesem Grund müssen die Verwendung nicht dienstlich beschaffter (privater) Software zur Erledigung dienstlicher Aufgaben und der Einsatz privater Hardware im öffentlichen Bereich auf Ausnahmen beschränkt bleiben.

- **DA Internet:**

  Das Einbringen von privater Hard- und / oder Software in das Lokale Netz ist unzulässig, weil dadurch Sicherheitslücken eröffnet werden.

Innerhalb einer Dienstanweisung:

- ## Benutzerkontrolle:

  Das dem Mitarbeiter zugewiesene Passwort ist von diesem in angemessenen Zeitabständen, mindestens zweimal jährlich, durch ein nur ihm bekanntes Passwort zu ersetzen.

- ## Passwortschutz:

  …Darüber hinaus ist das Passwort in unregelmäßigen Zeitabständen – spätestens nach 3 Monaten – zu ändern, sofern das System nicht automatisch dazu auffordert.

§ 110 Abs. 1 S. 1 TKG, § 3 Abs. 1 S. 1 TKÜV:

Pflicht zur Vorhaltung von Einrichtungen zur TK-Überwachung, wenn TK-Leistungen für die Öffentlichkeit erbracht werden

Ausnahme: § 3 Abs. 2 Nr. 5 TKÜV

Weniger als 1000 Nutzungsberechtigte

Stellungnahme

1. Begriffsklärung
2. Gesetzliche Grundlagen
3. Darstellung der Rechtsprechung bei privater Internetnutzung
4. Kontrolle der Internetnutzung

4.1 bei Verbot privater Nutzung

4.2 bei Erlaubnis privater Nutzung

5. Strafrechtliche Konsequenzen übermäßiger Kontrolle
6. IT-Richtlinie/Dienstanweisung/Dienstvereinbarung
7. Private Nutzung trotz Verbots - Konsequenzen

Konsequenzen bei privater Nutzung trotz Verbot		
Angestellte (Privatunternehmen)	Angestellte (öffentlicher Dienst)	Beamte
Arbeitsrechtliche Konsequenz 1. Abmahnung 2. Ordentliche Kündigung 3. Außerordentliche Kündigung		Disziplinarmaßnahmen - Verweis - Geldbuße - Kürzung der Dienstbezüge - Zurückstufung - Entfernung aus dem Beamtenverhältnis
Schadensersatz 1. Vertragliche Ansprüche (§ 280 BGB) 2. Deliktische Ansprüche (§ 823 BGB)		Schadensersatz § 78 BBG
Strafrechtliche Konsequenz § 303 b StGB Computersabotage §§ 184 ff. StGB (pornograph. Inhalte mit Kindern / Tieren)		

Workshop
Dienstvereinbarungen zur Internetnutzung (Teil 1)
IT-Verträge der öffentlichen Hand (Teil 2)

Rechtliche Aspekte in Behörden im Umgang mit E-Mail, Web und IT-Verträgen

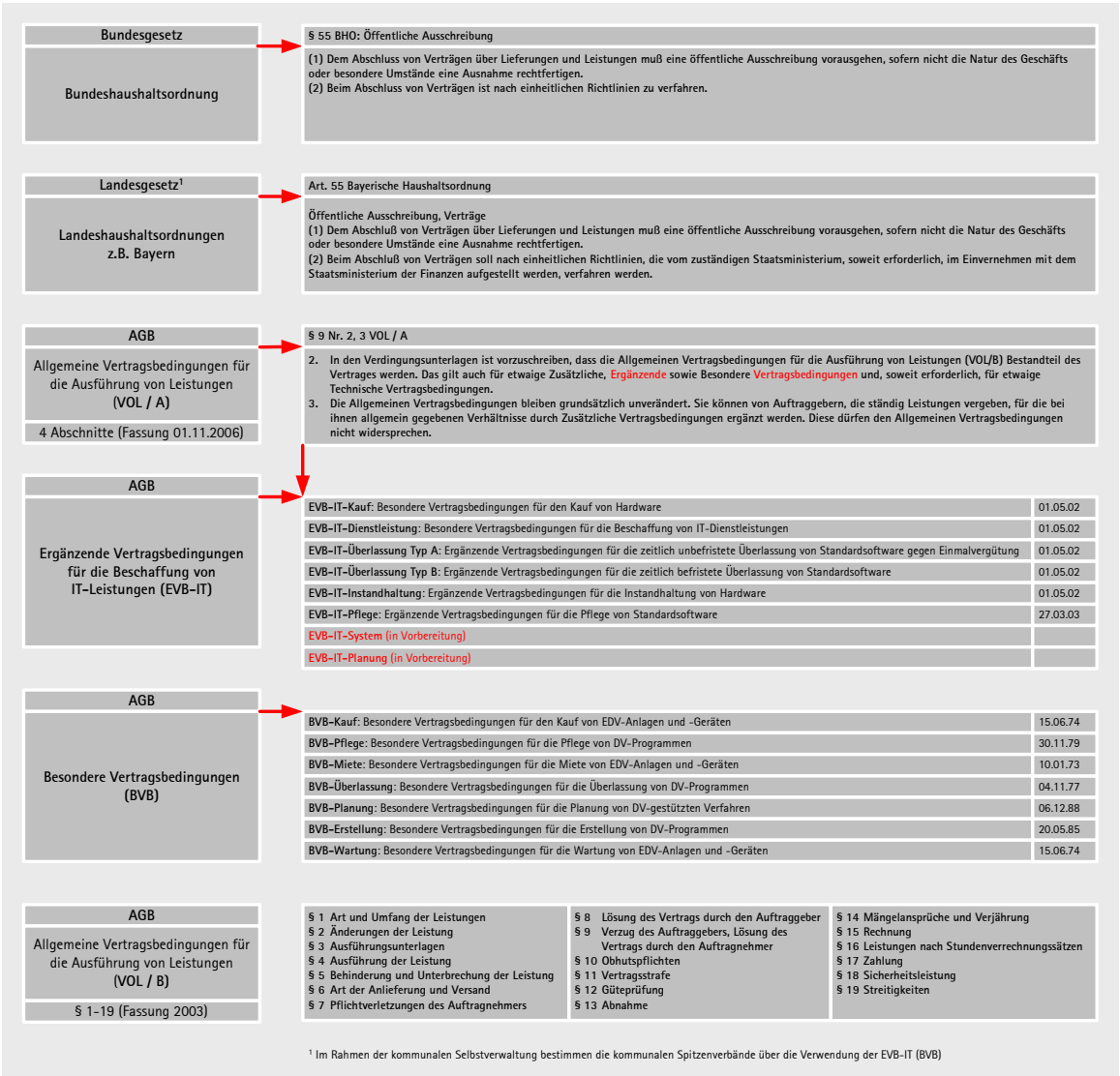
Referenten: Viktor Foerster
Lisa Rattmann
www.fr-lawfirm.com

FOERSTER+RUTOW®
RECHTSANWÄLTE
www.fr-lawfirm.com

1. IT-Verträge nach fr_octogon_typisierung - B2B

1.1 Rechtsgrundlage EVB-IT (BVB)

Die Vertragsgestaltung von IT-Verträgen in der öffentlichen Hand wird durch folgende Rechtsgrundlagen bestimmt:

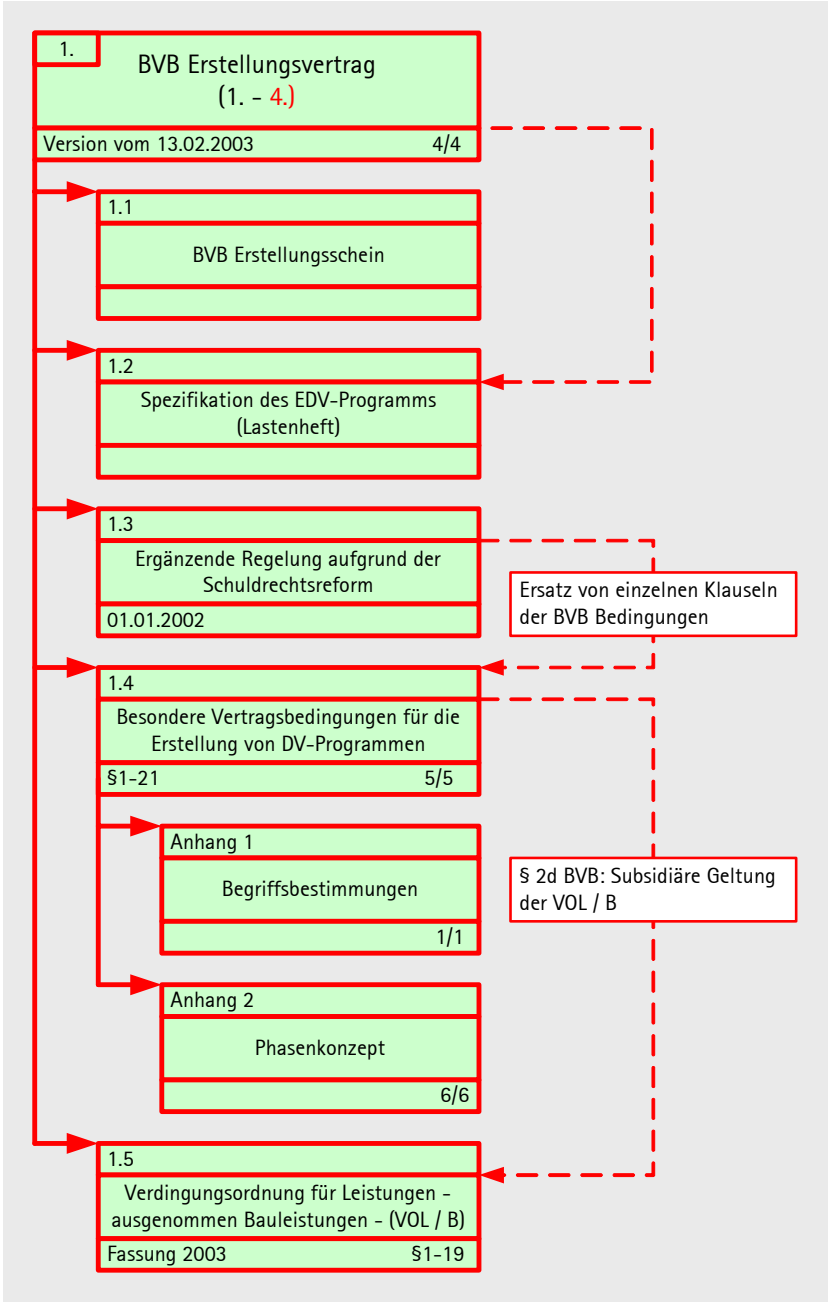


Die EVB-IT (BVB) sind Formularverträge, die im Zusammenwirken zwischen der öffentlichen Hand und Industrievertretern seit etwa 1970 entwickelt wurden. Die Formularverträge unterliegen der Inhaltskontrolle (§§ 305 ff., 310 BGB). Die EVB-IT (BVB) haben die Funktion von Beschaffungsrichtlinien im Sinne der Haushaltsgesetze (z.B. für den Bund, § 55 II BHO). Die EVB-IT (BVB) sind Konkretisierungen der VOL / B bedingt durch die spezielle Regelungsmaterie des IT-Rechts.

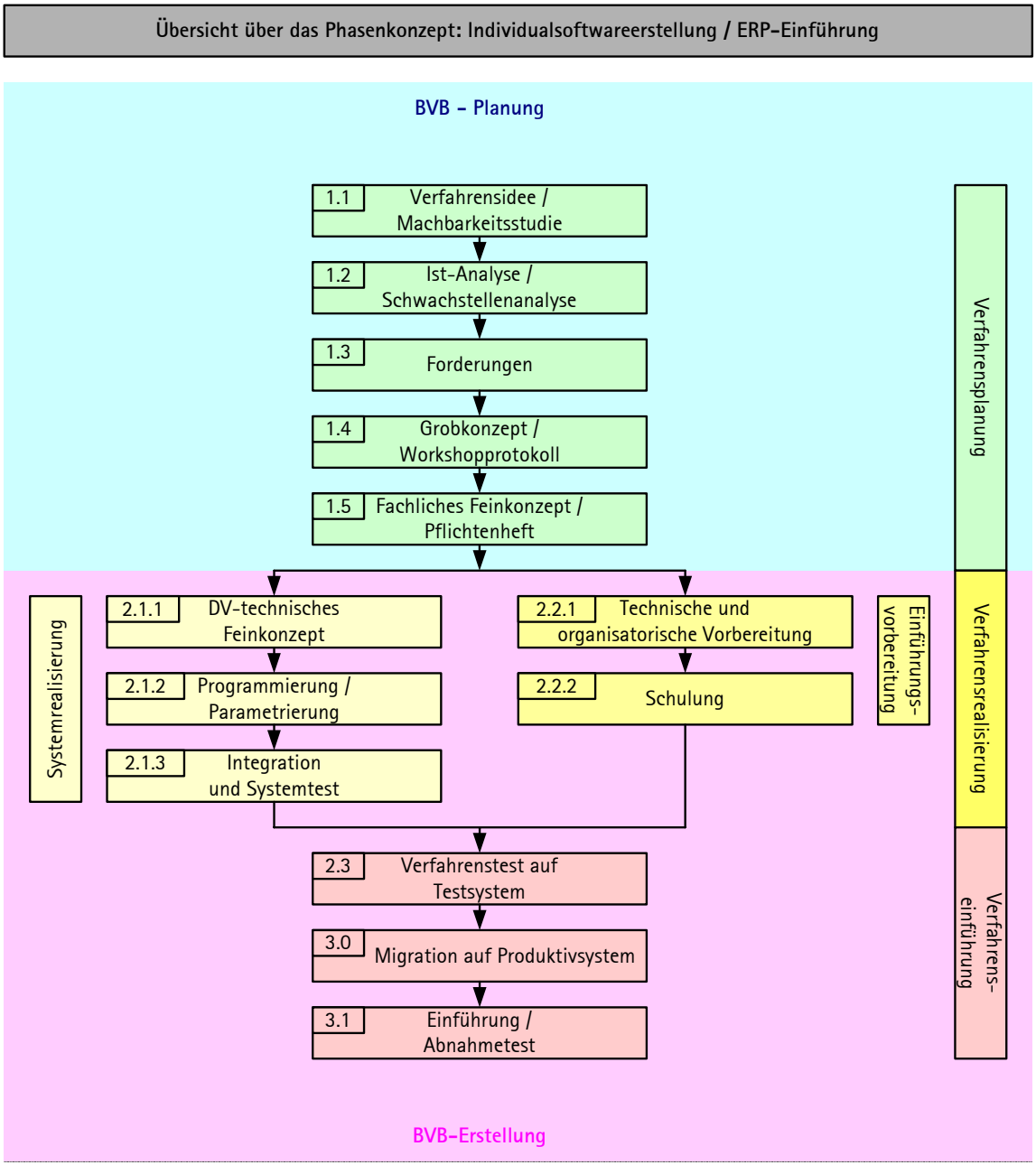
Die EVB-IT (BVB) gelten deshalb nur, wenn sie im Vertrag ausdrücklich einbezogen werden.

1.2 Struktur der Vertragsdokumente

Die Struktur der Vertragsdokumente lässt sich in einer Grafik am Beispiel des Vertrages zur Erstellung von DV-Programmen (BVB-Erstellung) wie folgt verallgemeinern:


1.
BVB Erstellungsvertrag
(1. - 4.)
Version vom 13.02.2003 4/4
1.1
BVB Erstellungsschein
1.2
Spezifikation des EDV-Programms
(Lastenheft)
1.3
Ergänzende Regelung aufgrund der
Schuldrechtsreform
01.01.2002
Ersatz von einzelnen Klauseln
der BVB Bedingungen
1.4
Besondere Vertragsbedingungen für die
Erstellung von DV-Programmen
§1-21 5/5
Anhang 1
Begriffsbestimmungen
1/1
§ 2d BVB: Subsidiäre Geltung
der VOL / B
Anhang 2
Phasenkonzept
6/6
1.5
Verdingungsordnung für Leistungen -
ausgenommen Bauleistungen - (VOL / B)
Fassung 2003 §1-19

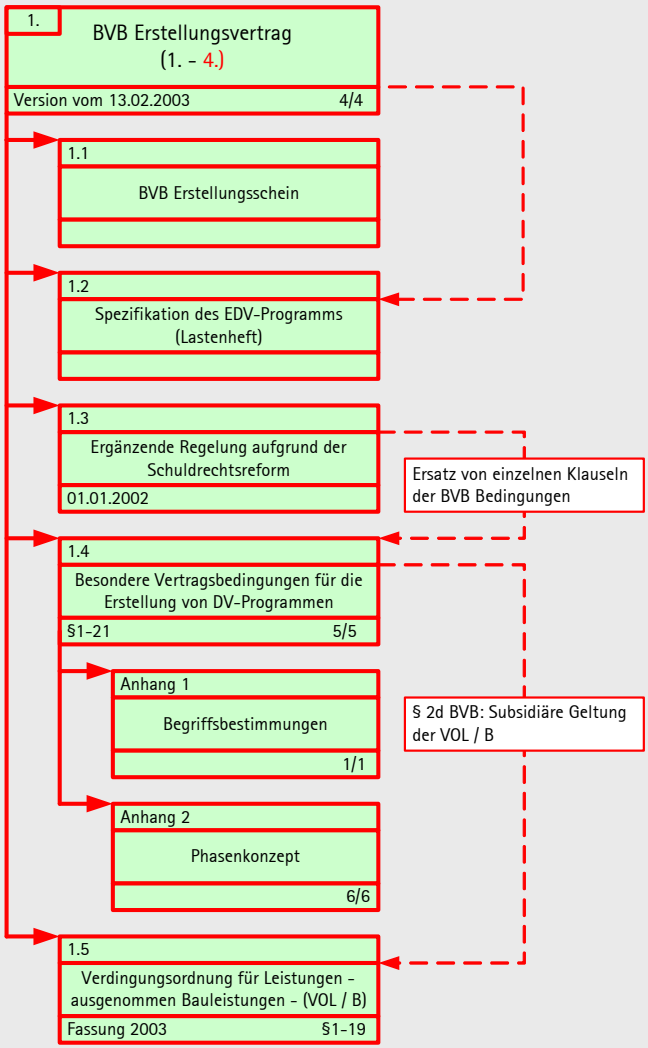
1.3 Phasenkonzept



1.4 Geltungsreihenfolge der Vertragsdokumente

Von den Rechtsgrundlagen (1.1) und der Struktur der Vertragsdokumente (1.2) darf man nicht auf die Geltungsreihenfolge der Vertragsdokumente schließen. Die Geltungsreihenfolge der Vertragsdokumente ist autonom in jedem Vertrag individuell zu gestalten. Die Geltungsreihenfolge der Vertragsdokumente kommt dann zur Anwendung, wenn sich Widersprüche zwischen einzelnen Vertragsdokumenten ergeben. In diesem Fall greift dann die vertragliche Regelung über die Geltungsreihenfolge der Vertragsdokumente ein. In der Praxis der BVB-Verträge ist dies eine höchst komplexe Aufgabenstellung, da mehrere Geltungsreihenfolgen-Regelungen in den Vertragsdokumenten anzutreffen sind. Diese sind nach Möglichkeit inhaltlich in Übereinstimmung zu bringen.

Regelung über Geltungsreihenfolge



2 Vertragsbestandteile
2.1 Es gelten nacheinander als Vertragsbestandteile:
- Dieser Vertrag mit Ausnahme der Nummer 4
- BVB-Erstellungsschein (Seite 1 bis _____) einschließlich der Anlage(n) Nr_____
- Nummer 4 dieses Vertrages einschließlich der Anlagen in der dort festgelegten Rangfolge
- Besondere Vertragsbedingungen für das Erstellen von DV-Programmen (BVB-Erstellung) in der bei Vertragsschluss geltenden Fassung
- Verdingungsordnung für Leistungen - ausgenommen Bauleistungen - Teil B (VOL/B) in der bei Vertragsschluss geltenden Fassung.

BVB-Erstellung und VOL/B liegen beim Auftraggeber zur Einsichtnahme bereit.

Es gelten die Dokumente

- in dieser Reihenfolgen
- in folgender Reihenfolge

§ 2 Art und Umfang der Leistungen
Art und Umfang der beiderseitigen Leistungen werden durch die vertraglichen Abmachungen geregelt. Maßgebend dafür sind:
a) Erstellungsschein,
b) nachstehende Bedingungen einschließlich Begriffsbestimmungen (Anhang 1),
c) Richtlinien und Fachnormen, soweit sie zum Zeitpunkt der Angebotsabgabe allgemein angewandt werden,
d) Allgemeine Bedingungen für die Ausführung von Leistungen - ausgenommen Bauleistungen - (VOL/B).
Bei Unstimmigkeiten gelten die vertraglichen Abmachungen in der vorstehenden Reihenfolge.

2. Bei Widersprüchen im Vertrag gelten nacheinander
a) die Leistungsbeschreibung
b) Besondere Vertragsbedingungen
c) etwaige Ergänzende Vertragsbedingungen
d) etwaige Zusätzliche Vertragsbedingungen
e) etwaige allgemeine Technische Vertragsbedingungen
f) die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B).

Aus diesen generellen Überlick über die unbestimmten Regelungen über den Geltungsbereich in einzelnen Vertragsdokumenten kann man die Aufgabe ermessen, die dem Vertragsdesigner zuwächst, aus dieser differenzierten widersprüchlichen Geltungsreihenfolge eine Eindeutigkeit der Geltungsreihenfolge im Vertrag selbst zu schaffen. Dies wird nur dann erfolgreich sein, wenn es gelingt im Vertragsdokument selbst eine vollständige und abschließende Geltungsreihenfolge unter Aufhebung der übrigen Regelung zu der Geltungsreihenfolge festzulegen.

1.5 Verhältnis BVB zu EVB-IT

Die öffentliche Hand (www.kbst.bund.de) beabsichtigt die weitgehend technisch und rechtlich überholten BVB durch neue BVB-IT Formularverträge abzulösen. Der derzeitige Stand lässt sich wie folgt zusammenfassen:

	BVB	Regelungstatbestände
1.	BVB-Kauf	**Anwendung:** Kauf und zusätzliche **werkvertragliche** Leistungen **Subsidiär:** Gegenüber EVB-IT-Kauf **Vergütung:** Festpreis oder Vergütung mit Preisvorbehalt
2.	BVB-Pflege	**Anwendung:** Funktionsfähigkeit der SW (Mängelbeseitigung und neue SW-Versionen; Dokumentationsanpassung) **Vergütung:** Monatliche Pauschale
3.	BVB-Miete	**Anwendung:** Anwendung von DV-Anlagen und -Geräten, Überlassung von Grundsoftware **Vergütung:** Festpreis oder Vergütung mit Preisvorbehalt
4.	BVB-Überlassung	**Anwendung:** Überlassung von Standard-SW (unbefristete Nutzung): werkvertraglichen Leistungen (z.B. Installation; Parametrierung; Migration; Integration; Softwareanpassungen) **Vergütung:** Einmalvergütung
5.	BVB-Planung	**Anwendung:** Planungsleistungen (Vorbereitende Arbeiten für Grobkonzept; Erarbeitung Grobkonzept und fachliches Feinkonzept) **Vergütung:** Marktpreis; Selbstkostenfestpreis, Selbstkostenerstattungspreis und Selbstkostenrichtpreis
6.	BVB-Erstellung	**Anwendung:** Erstellen von Programmen auf Basis fachlichen Feinkonzeptes: Erstellen DV-technisches Feinkonzept; Programmierung; Systemtest; Dokumentation **Vergütung:** Marktpreis; Selbstkostenfestpreis, Selbstkostenerstattungspreis und Selbstkostenrichtpreis (PR Nr. 30/53[1])
7.	BVB-Wartung	**Anwendung:** (ersetzt durch EVB-IT-Instandhaltung; vgl. unten 5.)
	EVB-IT	**Regelungstatbestände**
1.	EVB-IT-Kauf	**Anwendung:** Kauf von HW und Standard-SW (**keine werkvertraglichen** Leistungen) **Vergütung:** Einzelvergütung zur unbefristeten Nutzung
2.	EVB-IT-Dienstleistung	**Anwendung:** - Schulung - (Organisations-) Beratung - Sonstige Unterstützungsleistungen
3.	EVB-IT-Überlassung Typ A	**Anwendung:** Überlassung von Standard-SW (unbefristete Nutzung): Keine werkvertraglichen Leistungen **Vergütung:** Einmalvergütung
4.	EVB-IT-Überlassung Typ B	**Anwendung:** Überlassung von Standard-SW (befristete Nutzung): Keine werkvertraglichen Leistungen **Vergütung:** Periodische Vergütung
5.	EVB-IT-Instandhaltung	**Anwendung:** Inspektion, Wartung, Instandsetzung (HW) **Ersetzung:** BVB-Wartung **Vergütung:** pauschal oder nach Aufwand
6.	EVB-IT-Pflege S	**Anwendung:** Pflege von Standard-SW **Vergütung:** pauschal oder nach Aufwand
7.	EVB-IT-System	(in Vorbereitung)
8.	EVB-IT-Planung	(in Vorbereitung)

[1] Verordnung PR Nr. 30/53 über die Preise bei öffentlichen Aufträgen In der Fassung vom 21.11.1953, zuletzt geändert durch Achte Zuständigkeitsanpassungsverordnung vom 25.11.2003

Die Ablösungsnotwendigkeit der BVB-Bedingungen durch die EVB-IT-Bedingungen resultiert auch aus der Folge der Schuldrechtsreform. Diese Folgen wurden bisher nur hilfsweise und provisorisch durch die Einfügung von „Ergänzende Regelungen aufgrund der Schuldrechtsreform vom 01.01.2005“ in den einzelnen BVB-Vertragsbedingungen berücksichtigt.

Ein Ersatz der BVB durch die EVB-IT ist überfällig.

Außerdem sind derzeit zwei Formularverträge in Vorbereitung und stehen kurz vor Veröffentlichung durch die beteiligten Fachkremien

- EVB-IT Planung
- EVB-IT System

1.6 Lücken

Auch unter Berücksichtigung der bisher veröffentlichten Formularverträge EVB-IT (BVB) gilt es Regelungslücken für Einkaufsvorgänge der öffentlichen Hand zu identifizieren:

		Lücken in EVB-IT (BVB)
		In den Einkaufsverträgen / -bedingungen der öffentlichen Hand finden sich keine geschlossenen Regelungsmaterien für folgende IT-Leistungsbilder
1.	Installation	Die Installation als werkvertragliches Leistungsbild ist nicht geregelt.
2.	Anpassung etc.	Anpassung, Portierung, Parametrierung von Software sind in den EVB-IT (BVB) nicht erfasst.
3.	System	Ein typischer IT-Systemvertrag ist bisher von EVB-IT (BVB) nicht erfasst. Es liegt ein Entwurf eines EVB-IT-Systemvertrages vor, dessen Veröffentlichung sich aber substantiell verzögert. Angekündigt war die Veröffentlichung bereits für Mitte 2006. Dieser Mangel wurde bisher verwaltet, indem man bestehende EVB-IT (BVB) Vertragsbedingungen miteinander kombiniert hat, z.B. BVB-Planung, Erstellung, Pflege.
4.	ERP	Enterprise Resource Planing (ERP): Diese in der Privatwirtschaft über Standardprodukte eingeführten komplexen IT-Lösungen werden zukünftig auch angepasst auf die Bedürfnisse der öffentlichen Hand Eingang finden, in die öffentliche Verwaltung, insbesondere dort, wo diese privatwirtschaftlich ihre Tätigkeit gestaltet. Typische Module von ERP-Verträgen sind folgende Funktionsbereiche: Materialwirtschaft; Beschaffung; Lagerhaltung; Disposition; Bewertung; Produktion; Finanz- und Rechnungswesen; Controlling; Personalwirtschaft; Forschung und Entwicklung; Verkauf und Marketing; Stammdatenverwaltung; E-Business; Workflow Management; Customer Relationship Management (CRM); Personalinformationssystem (HRES); Produktionsplanungs- und Steuerungssystem (PPS); Wissensmanagement.

1.7 Entscheidungshilfe

Als Entscheidungshilfe für die Auswahl des richtigen Vertragstypus dient die Orientierung am Vertragsgegenstand. Danach lässt sich mit hoher Sicherheit der richtige Vertragstyp bestimmen.

Vertragsgegenstand	empfohlener Vertragstyp
IT-Dienstleistungen	EVB-IT Dienstleistung
Kauf von Hardware (ohne werkvertragliche Leistungsanteile)	EVB-IT Kauf
Kauf von Hardware (mit werkvertraglichen Leistungsanteilen)	BVB-Kauf
Miete von Hardware	BVB-Miete
Instandhaltung (früher: Wartung) von Hardware	EVB-IT Instandhaltung
Kauf von Standardsoftware (ohne werkvertragliche Leistungsanteile)	EVB-IT Überlassung Typ A
Miete von Standardsoftware (ohne werkvertragliche Leistungsanteile)	EVB-IT Überlassung Typ B
Überlassung von Standardsoftware (mit werkvertraglichen Leistungsanteilen	BVB-Überlassung
Pflege von Standardsoftware	EVB-IT Pflege S
Pflege von Individualsoftware	BVB-Pflege
Planung von DV-gestützten Verfahren, insbesondere Planung von Individualsoftware (Planungsphase, Fachliches Feinkonzept)	BVB-Planung
Erstellung von Individualsoftware	BVB-Erstellung
Wartung von HW	BVB-Wartung
Erstellung eines Gesamtsystems zzgl. Systemservice und/oder Weiterentwicklung oder Anpassung des Gesamtsystems nach Abnahme	*EVB-IT-System (in Vorbereitung)*

1.8 Haftungsregelungen im EVB-IT

	EVB-IT	gesetzl. Leitbild	Haftung			
			A Verzug [3]	B Sachmängel[1] [3]	C Rechtsmängel [3]	D Sonstige Haftung[2] [3]

1.	**EVB-IT-Kauf**	KV[4]	- Mahnung
			- pauschalierter Schadenersatz
			  - Höhe: max. 8% des Gesamtpreises
			- Keine Haftungsgrenze
			  - Vorsatz
			  - grobe Fahrlässigkeit
			  - zuges. Eigenschaften
			  - arglistiges Verschweigen
			- Nichtfortsetzungserklärung
			  - Rücktritt
			  - Schadenersatz
			  - Erfüllungsforderung mit Enddatum
				- Mängelanzeige (Muster)
				- Wahlrecht AN
				  - Mängelbeseitigung
				  - Neulieferung
				- Erfolglose Nachfristsetzung
				  - Rücktritt
				  - Minderung
				  - Schadenersatz
				  - Leichte Fahrlässigkeit: max. 8% des Gesamtpreises
				  - Ohne Begrenzung der Höhe:
				  - Vorsatz
				  - Grobe Fahrlässigkeit
				  - zuges. Eigenschaften
				  - arglistiges Verschweigen
				- Verjährungsfrist: 24 Monate ab Lieferung
					- Beseitigung der Rechtsverletzung[3]
					- Freistellung von Ansprüchen Dritter
					- Regeln über gerichtliche und außergerichtliche Zusammen-arbeit
						- Höchstgrenze: 500.000 je Schadensereignis, insg. EUR 1 Mio. pro Vertrag
						  - bei leichter Fahrlässigkeit
						  - für Sach- und Vermögens-schäden
						- Keine Haftung für:
						  - Datenverlust nur Kosten der Wiederherstellung bei ordnungsgemäßer Daten-sicherung
						  - entgangenen Gewinn
						- Keine Haftungsgrenze bei:
						  - Vorsatz
						  - grobe Fahrlässigkeit
						  - zuges. Eigenschaften
						  - arglistiges Verschweigen

2.	**EVB-IT-Dienstleistung**	DV[5]	Keine Verzugsregelung im Vertrag [3]	**„Qualitative Leistungsstörung“** [3]
				- (unverzügliche) Mängelrüge
				- Nacherfüllung
				- (angemessene) Nachfrist
				- fristlose Kündigung
				  - Vergütung, soweit erbrachte Leistung für AG verwertbar
				- außerordentliche Kündigung
				  - Geheimhaltung
				  - Datenschutz
				  - Schutzrechtsverletzung, etc.
					- Beseitigung d. Rechtsverletzung [3]
					- Freistellung von Ansprüchen Dritter
					- Regeln über gerichtliche und außergerichtliche Zusammen-arbeit
						- Höchstgrenze: [3]
						  - bei leichter Fahrlässigkeit
						  - für Sachschäden: EUR 500.000 je Schadensereignis, max. EUR 1 Mio pro Vertrag
						  - für Vermögensschäden: max. 10% der Gesamtvergütung, max. EUR 500.000 je Vertrag
						- Keine Haftung für:
						  - Datenverlust nur Kosten der Wiederherstellung bei ordnungsgemäßer Datensicherung
						  - entgangenen Gewinn
						- Keine Haftungsgrenze bei:
						  - Vorsatz
						  - grobe Fahrlässigkeit
						  - zuges. Eigenschaften
						  - arglistiges Verschweigen
						  - Produkthaftungsgesetz
						  - Körperverletzung / Tod

Gesamthaftungsbegrenzung grundsätzlich nicht vorgegeben
Ausnahme: „sonstige Vereinbarungen“: Individuelle Vereinbarung

[1] „qualitative Leistungsstörung“
[2] Unerlaubte Handlung (§§ 823 ff. BGB); Produkthaftung; Verletzung von Nebenpflichten (pVV; cic)
[3] abschließende Regelung im EVB-IT (Ausnahme: Vorsatz; grobe Fahrlässigkeit)
[4] Kaufvertrag
[5] Dienstvertrag

BVB-Kauf

T

Vertrag über den Kauf von EDV-Anlagen und -Geräten

Inhaltsverzeichnis vom Vertrag

Anhang 1

Kaufschein

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

BVB-Pflege

T

Vertrag über die Pflege von DV-Programmen

Inhaltsverzeichnis vom Vertrag

Anhang 1

Pflegeschein

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

BVB-Miete

T

Vertrag über die Miete von EDV-Anlagen und -Geräten

Inhaltsverzeichnis vom Vertrag

Anhang 1

Mietschein

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

BVB-Überlassung II

T

Vertrag über die Überlassung von Standardsoftware einschließlich der Herbeiführung der Funktionsfähigkeit

Inhaltsverzeichnis vom Vertrag

Inhaltsverzeichnis von AGB

Anhang 1

Überlassungsschein

Anhang 1

Begriffsbestimmungen

BVB-Planung

T

Vertrag über die Planung von DV-gestützten Verfahren

Inhaltsverzeichnis vom Vertrag

Anhang 1

Planungschein

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

Anhang 2

Hinweise zum sachlichen Geltungsbereich

BVB-Erstellung

T

Vertrag über die Erstellung von DV-Programmen

Inhaltsverzeichnis vom Vertrag

Anhang 1

Erstellungsschein

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

Anhang 2

Hinweise zum sachlichen Geltungsbereich

BVB-Wartung

T

Vertrag über die Wartung von EDV-Anlagen und -Geräten

Inhaltsverzeichnis vom Vertrag

Inhaltsverzeichnis von AGB

Anhang 1

Wartungsschein

Anhang 1

Begriffsbestimmungen

EVB-IT-Kauf

T

Vertrag über den Kauf von Hardware und die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung

Inhaltsverzeichnis vom Vertrag

Anhang 1

Störungsmeldeformular

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

EVB-IT-Dienstleistung T

Vertrag über die Beschaffung von IT-Dienstleistungen II

Inhaltsverzeichnis vom Vertrag

Anhang 1

Leistungsnachweis

Anhang 2

Änderungsverfahren

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

EVB-IT-Überlassung Typ A

T

Vertrag über die zeitlich unbefristete Überlassung von Standardsoftware gegen Einmalvergütung

Inhaltsverzeichnis vom Vertrag

Anhang 1

Störungsmeldeformular

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

EVB-IT-Überlassung Typ B

T

Vertrag über die zeitlich befristete Überlassung von Standardsoftware

Inhaltsverzeichnis vom Vertrag

Anhang 1

Störungsmeldeformular

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

EVB-IT-Instandhaltung

T

Vertrag über die Instandhaltung von Hardware

Inhaltsverzeichnis vom Vertrag

Anhang 1

Störungsmeldeformular

Anhang 2

Servicebericht

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

EVB-IT-Pflege S

T

Vertrag über die Pflege von Standardsoftware

Inhaltsverzeichnis vom Vertrag

Anhang 1

Störungsmeldeformular

Anhang 2

Leistungsnachweis

Inhaltsverzeichnis von AGB

Anhang 1

Begriffsbestimmungen

Störungsmeldung Nr. .....

Auftraggeber:		**Auftragnehmer:**	
Org.Einheit/Abteilung:		Org.Einheit/Abteilung:	
Name des Meldenden:		Name des Empfängers:	
Postanschrift:		Postanschrift:	
Telefon für Rückfragen:		Telefon:	
Fax für Rückmeldungen:		Fax:	
e-Mail für Rückmeldungen:		e-Mail:	
Vertragsnummer/Kennung:		Vertragsnummer/Kennung:	
		Web-Adresse:	

Produkt (HW/SW):	
Typ/Modell/Version:	
Seriennummer:	
Tatsächlicher Liefertermin:	
Störung aufgetreten am:	Datum / Uhrzeit
Kurzbeschreibung der Störung:	
Informationen über Ausschluss anderer Störungsursachen:	• ja • nein
Reproduzierbar:	

Systemumgebung/Konfiguration:	
Standort des Produktes:	
Bedeutung der Störung: **(nach Einschätzung des Auftraggebers)**	• Hoch • Mittel • Niedrig
Folgende Dokumente liegen beim Auftraggeber zur Einsicht bereit:	
Bemerkungen:	

_____,	_____	_____,	_____
Ort	Datum	Ort	Datum
Firma		Auftraggeber	
_____		_____	
Unterschrift Auftragnehmer (Name in Druckschrift)		Unterschrift Auftraggeber (Name in Druckschrift)	

Beamtenrechtsrahmengesetz

§ 48 BRRG

Der Dienstherr hat im Rahmen des Dienst- und Treueverhältnisses für das Wohl des Beamten und seiner Familie, auch für die Zeit nach Beendigung des Beamtenverhältnisses, zu sorgen. Er schützt ihn bei seiner amtlichen Tätigkeit und in seiner Stellung als Beamter.

Betriebsverfassungsgesetz

§ 75 BetrVG: Grundsätze für die Behandlung der Betriebsangehörigen

(1) Arbeitgeber und Betriebsrat haben darüber zu wachen, dass alle im Betrieb tätigen Personen nach den Grundsätzen von Recht und Billigkeit behandelt werden, insbesondere, dass jede Benachteiligung von Personen aus Gründen ihrer Rasse oder wegen ihrer ethnischen Herkunft, ihrer Abstammung oder sonstigen Herkunft, ihrer Nationalität, ihrer Religion oder Weltanschauung, ihrer Behinderung, ihres Alters, ihrer politischen oder gewerkschaftlichen Betätigung oder Einstellung oder wegen ihres Geschlechts oder ihrer sexuellen Identität unterbleibt.

(2) Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern.

§ 87 BetrVG: Mitbestimmungsrechte

(1) Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen:

1. ragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb;
2. Beginn und Ende der täglichen Arbeitszeit einschließlich der Pausen sowie Verteilung der Arbeitszeit auf die einzelnen Wochentage;
3. vorübergehende Verkürzung oder Verlängerung der betriebsüblichen Arbeitszeit;
4. Zeit, Ort und Art der Auszahlung der Arbeitsentgelte;
5. Aufstellung allgemeiner Urlaubsgrundsätze und des Urlaubsplans sowie die Festsetzung der zeitlichen Lage des Urlaubs für einzelne Arbeitnehmer, wenn zwischen dem Arbeitgeber und den beteiligten Arbeitnehmern kein Einverständnis erzielt wird;
6. Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen;
7. Regelungen über die Verhütung von Arbeitsunfällen und Berufskrankheiten sowie über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften oder der Unfallverhütungsvorschriften;
8. Form, Ausgestaltung und Verwaltung von Sozialeinrichtungen, deren Wirkungsbereich auf den Betrieb, das Unternehmen oder den Konzern beschränkt ist;
9. Zuweisung und Kündigung von Wohnräumen, die den Arbeitnehmern mit Rücksicht auf das Bestehen eines Arbeitsverhältnisses vermietet werden, sowie die allgemeine Festlegung der Nutzungsbedingungen;
10. Fragen der betrieblichen Lohngestaltung, insbesondere die Aufstellung von Entlohnungsgrundsätzen und die Einführung und Anwendung von neuen Entlohnungsmethoden sowie deren Änderung;

11. Festsetzung der Akkord- und Prämiensätze und vergleichbarer leistungsbezogener Entgelte, einschließlich der Geldfaktoren;
12. Grundsätze über das betriebliche Vorschlagswesen;
13. Grundsätze über die Durchführung von Gruppenarbeit; Gruppenarbeit im Sinne dieser Vorschrift liegt vor, wenn im Rahmen des betrieblichen Arbeitsablaufs eine Gruppe von Arbeitnehmern eine ihr übertragene Gesamtaufgabe im Wesentlichen eigenverantwortlich erledigt.

(2) Kommt eine Einigung über eine Angelegenheit nach Absatz 1 nicht zustande, so entscheidet die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

§ 90 BetrVG: Unterrichtungs- und Beratungsrechte

(1) Der Arbeitgeber hat den Betriebsrat über die Planung

1. von Neu-, Um- und Erweiterungsbauten von Fabrikations-, Verwaltungs- und sonstigen betrieblichen Räumen,
2. von technischen Anlagen,
3. von Arbeitsverfahren und Arbeitsabläufen oder
4. der Arbeitsplätze rechtzeitig unter Vorlage der erforderlichen Unterlagen zu unterrichten.

(2) Der Arbeitgeber hat mit dem Betriebsrat die vorgesehenen Maßnahmen und ihre Auswirkungen auf die Arbeitnehmer, insbesondere auf die Art ihrer Arbeit sowie die sich daraus ergebenden Anforderungen an die Arbeitnehmer so rechtzeitig zu beraten, dass Vorschläge und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können. Arbeitgeber und Betriebsrat sollen dabei auch die gesicherten arbeitswissenschaftlichen Erkenntnisse über die menschengerechte Gestaltung der Arbeit berücksichtigen.

Bundesangestelltentarif

§ 8 (BAT): Allgemeine Pflichten

(1) Der Angestellte hat sich so zu verhalten, wie es von Angehörigen des öffentlichen Dienstes erwartet wird. Es muss sich durch sein gesamtes Verhalten zur freiheitlich demokratischen Grundordnung im Sinne des Grundgesetzes bekennen.

(2) Der Angestellte ist verpflichtet, den dienstlichen Anordnungen nachzukommen. Beim Vollzug einer dienstlichen Anordnung trifft die Verantwortung denjenigen, der die Anordnung gegeben hat. Der Angestellte hat Anordnungen, deren Ausführung - ihm erkennbar - den Strafgesetzen zuwiderlaufen würde, nicht zu befolgen

Bundesbeamtengesetz

§ 78 BBG

(1) Verletzt ein Beamter vorsätzlich oder grob fahrlässig die ihm obliegenden Pflichten, so hat er dem Dienstherrn, dessen Aufgaben er wahrgenommen hat, den daraus entstehenden Schaden zu ersetzen. Haben mehrere Beamte gemeinsam den Schaden verursacht, so haften sie als Gesamtschuldner.

(2) Ansprüche nach Absatz 1 verjähren in drei Jahren von dem Zeitpunkt an, in dem der Dienstherr von dem Schaden und der Person des Ersatzpflichtigen Kenntnis erlangt hat, ohne Rücksicht auf diese Kenntnis in zehn Jahren von der Begehung der Handlung an. Hat der Dienstherr einem Dritten Schadenersatz geleistet, so tritt an die Stelle des Zeitpunktes, in dem der Dienstherr von dem Schaden Kenntnis erlangt, der Zeitpunkt, in dem der Ersatzanspruch des Dritten diesem gegenüber vom Dienstherrn anerkannt oder dem Dienstherrn gegenüber rechtskräftig festgestellt wird.

(3) Leistet der Beamte dem Dienstherrn Ersatz und hat dieser einen Ersatzanspruch gegen einen Dritten, so geht der Ersatzanspruch auf den Beamten über.

§ 79 BBG

Der Dienstherr hat im Rahmen des Dienst- und Treueverhältnisses für das Wohl des Beamten und seiner Familie, auch für die Zeit nach Beendigung des Beamtenverhältnisses, zu sorgen. Er schützt ihn bei seiner amtlichen Tätigkeit und in seiner Stellung als Beamter.

Bundesdatenschutzgesetz

§ 3a BDSG: Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4 BDSG: Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a BDSG: Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4f BDSG: Beauftragter für den Datenschutz

(1) Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nichtöffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nichtöffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 5 BDSG: Datengeheimnis

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.

§ 27 BDSG: Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch

1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
   b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist. Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 BDSG: Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.

(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf

   a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   b) Berufs-, Branchen- oder Geschäftsbezeichnung,
   c) Namen,
   d) Titel,
   e) akademische Grade,
   f) Anschrift und
   g) Geburtsjahr

   beschränken und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder
4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. In den Fällen des Satzes 1 Nr. 3 ist anzunehmen, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

1. auf strafbare Handlungen,
2. auf Ordnungswidrigkeiten sowie
3. bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten nach Absatz 3 übermittelt werden, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

§ 31 BDSG: Besondere Zweckbindung

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.

§ 44 BDSG Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Bürgerliches Gesetzbuch

§ 242 BGB: Leistung nach Treu und Glauben

Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern.

§ 280 BGB: Schadensersatz wegen Pflichtverletzung

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat.

(2) Schadensersatz wegen Verzögerung der Leistung kann der Gläubiger nur unter der zusätzlichen Voraussetzung des § 286 verlangen.

(3) Schadensersatz statt der Leistung kann der Gläubiger nur unter den zusätzlichen Voraussetzungen des § 281, des § 282 oder des § 283 verlangen.

§ 611 BGB: Vertragstypische Pflichten beim Dienstvertrag

(1) Durch den Dienstvertrag wird derjenige, welcher Dienste zusagt, zur Leistung der versprochenen Dienste, der andere Teil zur Gewährung der vereinbarten Vergütung verpflichtet.

(2) Gegenstand des Dienstvertrags können Dienste jeder Art sein.

§ 626 BGB: Fristlose Kündigung aus wichtigem Grund

(1) Das Dienstverhältnis kann von jedem Vertragsteil aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalles und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Dienstverhältnisses bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Dienstverhältnisses nicht zugemutet werden kann.

(2) Die Kündigung kann nur innerhalb von zwei Wochen erfolgen. Die Frist beginnt mit dem Zeitpunkt, in dem der Kündigungsberechtigte von den für die Kündigung maßgebenden Tatsachen Kenntnis erlangt. Der Kündigende muss dem anderen Teil auf Verlangen den Kündigungsgrund unverzüglich schriftlich mitteilen.

§ 823 BGB: Schadensersatzpflicht

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

Grundgesetz

Art 1 GG

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art 2 GG

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Gesetz über Rahmenbedingungen für elektronische Signaturen

Datum: 16. Mai 2001

Fundstelle: BGBl I 2001, 876

Textnachweis ab: 22. 5.2001
Amtlicher Hinweis des Normgebers auf EG-Recht:
Beachtung der
EGRL 34/98 (CELEX Nr: 398L0034)
(+++ Stand: Zuletzt geändert durch Art. 3 Abs. 9 G v. 7. 7.2005 I 1970 +++)

Die Mitteilungspflichten der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 204 S. 37), zuletzt geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18), sind beachtet worden.

SigG 2001 Inhaltsübersicht

Erster Abschnitt Allgemeine Bestimmungen

SigG 2001 § 1 Zweck und Anwendungsbereich

(1) Zweck des Gesetzes ist es, Rahmenbedingungen für elektronische Signaturen zu schaffen.

(2) Soweit nicht bestimmte elektronische Signaturen durch Rechtsvorschrift vorgeschrieben sind, ist ihre Verwendung freigestellt.

(3) Rechtsvorschriften können für die öffentlich-rechtliche Verwaltungstätigkeit bestimmen, dass der Einsatz qualifizierter elektronischer Signaturen zusätzlichen Anforderungen unterworfen wird. Diese Anforderungen müssen objektiv, verhältnismäßig und nichtdiskriminierend sein und dürfen sich nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen.

SigG 2001 § 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. "elektronische Signaturen" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. "fortgeschrittene elektronische Signaturen" elektronische Signaturen nach Nummer 1, die
   a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
   b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
   c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
   d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,
3. "qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die
   a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
   b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,
4. "Signaturschlüssel" einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
5. "Signaturprüfschlüssel" elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,
6. "Zertifikate" elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer Person zugeordnet werden und die Identität dieser Person bestätigt wird,
7. "qualifizierte Zertifikate" elektronische Bescheinigungen nach Nummer 6 für natürliche Personen, die die Voraussetzungen des § 7 erfüllen und von Zertifizierungsdiensteanbietern ausgestellt werden, die mindestens die Anforderungen nach den §§ 4 bis 14 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen,
8. "Zertifizierungsdiensteanbieter" natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen,
9. "Signaturschlüssel-Inhaber" natürliche Personen, die Signaturschlüssel besitzen; bei qualifizierten elektronischen Signaturen müssen ihnen die zugehörigen Signaturprüfschlüssel durch qualifizierte Zertifikate zugeordnet sein,
10. "sichere Signaturerstellungseinheiten" Software- oder Hardwareeinheiten

zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die mindestens die Anforderungen nach § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllen und die für qualifizierte elektronische Signaturen bestimmt sind,

11. "Signaturanwendungskomponenten" Software- und Hardwareprodukte, die dazu bestimmt sind,
    a) Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder
    b) qualifizierte elektronische Signaturen zu prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen,
12. "technische Komponenten für Zertifizierungsdienste" Software- oder Hardwareprodukte, die dazu bestimmt sind,
    a) Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen,
    b) qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar zu halten oder
    c) qualifizierte Zeitstempel zu erzeugen,
13. "Produkte für qualifizierte elektronische Signaturen" sichere Signaturerstellungseinheiten, Signaturanwendungskomponenten und technische Komponenten für Zertifizierungsdienste,
14. "qualifizierte Zeitstempel" elektronische Bescheinigungen eines Zertifizierungsdiensteanbieters, der mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der sich darauf beziehenden Vorschriften der Rechtsverordnung nach § 24 erfüllt, darüber, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben,
15. "freiwillige Akkreditierung" Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.

SigG 2001 § 3 Zuständige Behörde

Die Aufgaben der zuständigen Behörde nach diesem Gesetz und der Rechtsverordnung nach § 24 obliegen der Regulierungsbehörde für Telekommunikation und Post.

Zweiter Abschnitt Zertifizierungsdiensteanbieter

SigG 2001 § 4 Allgemeine Anforderungen

(1) Der Betrieb eines Zertifizierungsdienstes ist im Rahmen der Gesetze genehmigungsfrei.

(2) Einen Zertifizierungsdienst darf nur betreiben, wer die für den Betrieb erforderliche Zuverlässigkeit und Fachkunde sowie eine Deckungsvorsorge nach § 12 nachweist und die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 gewährleistet. Die erforderliche Zuverlässigkeit besitzt, wer die Gewähr dafür bietet, als Zertifizierungsdiensteanbieter die für den Betrieb maßgeblichen Rechtsvorschriften einzuhalten. Die erforderliche Fachkunde liegt vor, wenn die im Betrieb eines Zertifizierungsdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen. Die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes liegen vor, wenn die Maßnahmen zur Erfüllung der Sicherheitsanforderungen nach diesem Gesetz und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 der zuständigen Behörde in einem Sicherheitskonzept aufgezeigt und geeignet und praktisch umgesetzt sind.

(3) Wer den Betrieb eines Zertifizierungsdienstes aufnimmt, hat dies der zuständigen Behörde spätestens mit der Betriebsaufnahme anzuzeigen. Mit der Anzeige ist in geeigneter Form darzulegen, dass die Voraussetzungen nach Absatz 2 vorliegen.

(4) Die Erfüllung der Voraussetzungen nach Absatz 2 ist über die gesamte Zeitdauer der Tätigkeit des Zertifizierungsdienstes sicherzustellen. Umstände, die dies nicht mehr ermöglichen, sind der zuständigen Behörde unverzüglich anzuzeigen.

(5) Der Zertifizierungsdiensteanbieter kann unter Einbeziehung in sein Sicherheitskonzept nach Absatz 2 Satz 4 Aufgaben nach diesem Gesetz und der Rechtsverordnung nach § 24 an Dritte übertragen.

SigG 2001 § 5 Vergabe von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat Personen, die ein qualifiziertes Zertifikat beantragen, zuverlässig zu identifizieren. Er darf dazu mit Einwilligung des Antragstellers personenbezogene Daten nutzen, die der Zertifizierungsdiensteanbieter zu einem früheren Zeitpunkt erhoben hat, sofern diese Daten eine zuverlässige Identifizierung des Antragstellers nach Satz 1 gewährleisten. Er hat die Zuordnung eines Signaturprüfschlüssels zu einer identifizierten Person durch ein qualifiziertes Zertifikat zu bestätigen und dieses jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten. Ein qualifiziertes Zertifikat darf nur mit Zustimmung des Signaturschlüssel-Inhabers abrufbar gehalten werden.

(2) Ein qualifiziertes Zertifikat kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten. Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen. Angaben über die Vertretungsmacht für eine dritte Person dürfen nur bei Nachweis der Einwilligung nach Satz 2, berufsbezogene oder sonstige Angaben des Antragstellers zur Person nur bei Vorlage der Bestätigung nach Satz 2 in ein qualifiziertes Zertifikat aufgenommen werden. Weitere personenbezogene Angaben dürfen in ein qualifiziertes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.

(3) Der Zertifizierungsdiensteanbieter hat auf Verlangen eines Antragstellers in einem qualifizierten Zertifikat an Stelle seines Namens ein Pseudonym aufzuführen. Enthält ein qualifiziertes Zertifikat Angaben über eine Vertretungsmacht für eine dritte Person oder berufsbezogene oder sonstige Angaben zur Person, ist eine Einwilligung der dritten Person oder der für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle zur Verwendung des Pseudonyms erforderlich.

(4) Der Zertifizierungsdiensteanbieter hat Vorkehrungen zu treffen, damit Daten für qualifizierte Zertifikate nicht unbemerkt gefälscht oder verfälscht werden können. Er hat weiter Vorkehrungen zu treffen, um die Geheimhaltung der Signaturschlüssel zu gewährleisten. Eine Speicherung von Signaturschlüsseln außerhalb der sicheren Signaturerstellungseinheit ist unzulässig.

(5) Der Zertifizierungsdiensteanbieter hat für die Ausübung der

Zertifizierungstätigkeit zuverlässiges Personal und Produkte für qualifizierte elektronische Signaturen, die mindestens die Anforderungen nach den §§ 4 bis 14 sowie § 17 oder § 23 dieses Gesetzes und der Rechtsverordnung nach § 24 erfüllen, einzusetzen.

(6) Der Zertifizierungsdiensteanbieter hat sich in geeigneter Weise zu überzeugen, dass der Antragsteller die zugehörige sichere Signaturerstellungseinheit besitzt.

SigG 2001 § 6 Unterrichtungspflicht

(1) Der Zertifizierungsdiensteanbieter hat den Antragsteller nach § 5 Abs. 1 über die Maßnahmen zu unterrichten, die erforderlich sind, um zur Sicherheit von qualifizierten elektronischen Signaturen und zu deren zuverlässiger Prüfung beizutragen. Er hat den Antragsteller darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bei Bedarf neu zu signieren sind, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

(2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschrift, wenn durch Gesetz nicht ein anderes bestimmt ist.

(3) Zur Unterrichtung nach Absatz 1 und 2 ist dem Antragsteller eine Belehrung in Textform zu übermitteln, deren Kenntnisnahme dieser als Voraussetzung für die Ausstellung des qualifizierten Zertifikats in Textform zu bestätigen hat. Soweit ein Antragsteller bereits zu einem früheren Zeitpunkt nach den Absätzen 1 und 2 unterrichtet worden ist, kann eine erneute Unterrichtung unterbleiben.

SigG 2001 § 7 Inhalt von qualifizierten Zertifikaten

(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:

1. den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,
2. den zugeordneten Signaturprüfschlüssel,
3. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
4. die laufende Nummer des Zertifikates,
5. Beginn und Ende der Gültigkeit des Zertifikates,
6. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
7. Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,
8. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
9. nach Bedarf Attribute des Signaturschlüssel-Inhabers.

(2) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Absatz 1 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikates benötigt werden.

SigG 2001 § 8 Sperrung von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde, der Zertifizierungsdiensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen Zertifizierungsdiensteanbieter fortgeführt wird oder die zuständige Behörde gemäß § 19 Abs. 4 eine Sperrung anordnet. Weitere Sperrungsgründe können vertraglich vereinbart werden. Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies zusätzlich kenntlich machen.

(2) Enthält ein qualifiziertes Zertifikat Angaben nach § 5 Abs. 2, so kann auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle, wenn die Voraussetzungen für die berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen, eine Sperrung des betreffenden Zertifikates nach Absatz 1 verlangen.

SigG 2001 § 9 Qualifizierte Zeitstempel

Stellt ein Zertifizierungsdiensteanbieter qualifizierte Zeitstempel aus, so gilt § 5 Abs. 5 entsprechend.

SigG 2001 § 10 Dokumentation

(1) Der Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen zur Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 Nr. 1, 3 und 4 sowie die ausgestellten qualifizierten Zertifikate nach Maßgabe des Satzes 2 so zu dokumentieren, dass die Daten und ihre Unverfälschtheit jederzeit nachprüfbar sind. Die Dokumentation muss unverzüglich so erfolgen, dass sie nachträglich nicht unbemerkt verändert werden kann. Dies gilt insbesondere für die Ausstellung und Sperrung von qualifizierten Zertifikaten.

(2) Dem Signaturschlüssel-Inhaber ist auf Verlangen Einsicht in die ihn betreffenden Daten und Verfahrensschritte zu gewähren.

SigG 2001 § 11 Haftung

(1) Verletzt ein Zertifizierungsdiensteanbieter die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 oder versagen seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen, so hat er einem Dritten den Schaden zu ersetzen, den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft nach § 5 Abs. 1 Satz 2 vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste.

(2) Die Ersatzpflicht tritt nicht ein, wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat.

(3) Wenn ein qualifiziertes Zertifikat die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt, tritt die Ersatzpflicht nur im Rahmen dieser Beschränkungen ein.

(4) Der Zertifizierungsdiensteanbieter haftet für beauftragte Dritte nach § 4 Abs. 5 und beim Einstehen für ausländische Zertifikate nach § 23 Abs. 1 Nr. 2 wie für eigenes Handeln. § 831 Abs. 1 Satz 2 des Bürgerlichen Gesetzbuchs findet keine Anwendung.

SigG 2001 § 12 Deckungsvorsorge

Der Zertifizierungsdiensteanbieter ist verpflichtet, eine geeignete Deckungsvorsorge zu treffen, damit er seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachkommen kann, die dadurch entstehen, dass er die Anforderungen dieses Gesetzes oder der Rechtsverordnung nach § 24 verletzt oder seine Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen. Die Mindestsumme beträgt jeweils 250.000 Euro für einen durch ein haftungsauslösendes Ereignis der in Satz 1 bezeichneten Art verursachten Schaden.

SigG 2001 § 13 Einstellung der Tätigkeit

(1) Der Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der zuständigen Behörde anzuzeigen. Er hat dafür zu sorgen, dass die bei Einstellung der Tätigkeit gültigen qualifizierten Zertifikate von einem anderen Zertifizierungsdiensteanbieter übernommen werden, oder diese zu sperren. Er hat die betroffenen Signaturschlüssel-Inhaber über die Einstellung seiner Tätigkeit und die Übernahme der qualifizierten Zertifikate durch einen anderen Zertifizierungsdiensteanbieter zu benachrichtigen.

(2) Der Zertifizierungsdiensteanbieter hat die Dokumentation nach § 10 an den Zertifizierungsdiensteanbieter, welcher die Zertifikate nach Absatz 1 übernimmt, zu übergeben. Übernimmt kein anderer Zertifizierungsdiensteanbieter die Dokumentation, so hat die zuständige Behörde diese zu übernehmen. Die zuständige Behörde erteilt bei Vorliegen eines berechtigten Interesses Auskunft zur Dokumentation nach Satz 2, soweit dies technisch ohne unverhältnismäßig großen Aufwand möglich ist.

(3) Der Zertifizierungsdiensteanbieter hat einen Antrag auf Eröffnung eines Insolvenzverfahrens der zuständigen Behörde unverzüglich anzuzeigen.

SigG 2001 § 14 Datenschutz

(1) Der Zertifizierungsdiensteanbieter darf personenbezogene Daten nur unmittelbar beim Betroffenen selbst und nur insoweit erheben, als dies für Zwecke eines qualifizierten Zertifikates erforderlich ist. Eine Datenerhebung bei Dritten ist nur mit Einwilligung des Betroffenen zulässig. Für andere als die in Satz 1 genannten Zwecke dürfen die Daten nur verwendet werden, wenn dieses Gesetz es erlaubt oder der Betroffene eingewilligt hat.

(2) Der Zertifizierungsdiensteanbieter hat die Daten über die Identität eines Signaturschlüssel-Inhabers auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen. Die Auskünfte sind zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Übermittelung der Daten zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt.

(3) Soweit andere als die in § 2 Nr. 8 genannten Zertifizierungsdiensteanbieter Zertifikate für elektronische Signaturen ausstellen, gelten die Absätze 1 und 2 entsprechend.

Dritter Abschnitt Freiwillige Akkreditierung

SigG 2001 § 15 Freiwillige Akkreditierung von Zertifizierungsdiensteanbietern

(1) Zertifizierungsdiensteanbieter können sich auf Antrag von der zuständigen Behörde akkreditieren lassen; die zuständige Behörde kann sich bei der Akkreditierung privater Stellen bedienen. Die Akkreditierung ist zu erteilen, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 erfüllt sind. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen der zuständigen Behörde. Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen (qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung) zum Ausdruck gebracht. Sie dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen.

(2) Zur Erfüllung der Voraussetzungen nach Absatz 1 muss das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 durch eine Stelle nach § 18 umfassend auf seine Eignung und praktische Umsetzung geprüft und bestätigt sein. Die Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.

(3) Die Akkreditierung kann mit Nebenbestimmungen versehen werden, soweit dies erforderlich ist, um die Erfüllung der Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 bei Aufnahme und während des Betriebes sicherzustellen.

(4) Die Akkreditierung ist zu versagen, wenn die Voraussetzungen nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt sind; § 19 findet entsprechend Anwendung.

(5) Bei Nichterfüllung der Pflichten aus diesem Gesetz oder der Rechtsverordnung nach § 24 oder bei Vorliegen eines Versagungsgrundes nach Absatz 4 hat die zuständige Behörde die Akkreditierung zu widerrufen oder diese, soweit die Gründe bereits zum Zeitpunkt der Akkreditierung vorlagen, zurückzunehmen, wenn Maßnahmen nach § 19 Abs. 2 keinen Erfolg versprechen.

(6) Im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdiensteanbieters hat die zuständige Behörde eine Übernahme der Tätigkeit durch einen anderen akkreditierten Zertifizierungsdiensteanbieter oder die Abwicklung der Verträge mit den Signaturschlüssel-Inhabern sicherzustellen. Dies gilt auch bei Antrag auf Eröffnung eines Insolvenzverfahrens, wenn die Tätigkeit nicht fortgesetzt wird. Übernimmt kein anderer akkreditierter Zertifizierungsdiensteanbieter die Dokumentation gemäß § 13 Abs. 2, so hat die zuständige Behörde diese zu übernehmen; § 10 Abs. 1 Satz 1 gilt entsprechend.

(7) Bei Produkten für qualifizierte elektronische Signaturen muss die Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 und der Rechtsverordnung nach § 24 nach dem Stand von Wissenschaft und Technik hinreichend geprüft und durch eine Stelle nach § 18 bestätigt worden sein; Absatz 1 Satz 3 findet entsprechende Anwendung. Der akkreditierte Zertifizierungsdiensteanbieter hat

1. für seine Zertifizierungstätigkeit nur nach Satz 1 geprüfte und bestätigte Produkte für qualifizierte elektronische Signaturen einzusetzen,
2. qualifizierte Zertifikate nur für Personen auszustellen, die nachweislich nach Satz 1 geprüfte und bestätigte sichere Signaturerstellungseinheiten besitzen, und
3. die Signaturschlüssel-Inhaber im Rahmen des § 6 Abs. 1 über nach Satz 1 geprüfte und bestätigte Signaturanwendungskomponenten zu unterrichten.

SigG 2001 § 16 Zertifikate der zuständigen Behörde

(1) Die zuständige Behörde stellt den akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus. Die Vorschriften für die Vergabe und Sperrung von qualifizierten Zertifikaten durch akkreditierte Zertifizierungsdiensteanbieter gelten für die zuständige Behörde entsprechend. Sie sperrt von ihr ausgestellte qualifizierte Zertifikate, wenn ein akkreditierter Zertifizierungsdiensteanbieter seine Tätigkeit einstellt oder wenn eine

Akkreditierung zurückgenommen oder widerrufen wird.

(2) Die zuständige Behörde hat

1. die Namen, Anschriften und Kommunikationsverbindungen der akkreditierten Zertifizierungsdiensteanbieter,
2. den Widerruf oder die Rücknahme einer Akkreditierung,
3. die von ihr ausgestellten qualifizierten Zertifikate und deren Sperrung und
4. die Beendigung und die Untersagung des Betriebes eines akkreditierten Zertifizierungsdiensteanbieters

jederzeit für jeden über öffentlich erreichbare Kommunikationsverbindungen nachprüfbar und abrufbar zu halten.

(3) Bei Bedarf stellt die zuständige Behörde auch die von den Zertifizierungsdiensteanbietern oder Herstellern benötigten elektronischen Bescheinigungen für die automatische Authentifizierung von Produkten nach § 15 Abs. 7 aus.

Vierter Abschnitt Technische Sicherheit

SigG 2001 § 17 Produkte für qualifizierte elektronische Signaturen

(1) Für die Speicherung von Signaturschlüsseln sowie für die Erzeugung qualifizierter elektronischer Signaturen sind sichere Signaturerstellungseinheiten einzusetzen, die Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen. Werden die Signaturschlüssel auf einer sicheren Signaturerstellungseinheit selbst erzeugt, so gilt Absatz 3 Nr. 1 entsprechend.

(2) Für die Darstellung zu signierender Daten sind Signaturanwendungskomponenten erforderlich, die die Erzeugung einer qualifizierten elektronischen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten sich die Signatur bezieht. Für die Überprüfung signierter Daten sind Signaturanwendungskomponenten erforderlich, die feststellen lassen,

1. auf welche Daten sich die Signatur bezieht,
2. ob die signierten Daten unverändert sind,
3. welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
4. welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen und
5. zu welchem Ergebnis die Nachprüfung von Zertifikaten nach § 5 Abs. 1 Satz 2 geführt hat.

Signaturanwendungskomponenten müssen nach Bedarf auch den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Die Signaturschlüssel-Inhaber sollen solche Signaturanwendungskomponenten einsetzen oder andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen treffen.

(3) Die technischen Komponenten für Zertifizierungsdienste müssen Vorkehrungen enthalten, um

1. bei Erzeugung und Übertragung von Signaturschlüsseln die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen,
2. qualifizierte Zertifikate, die gemäß § 5 Abs. 1 Satz 2 nachprüfbar oder abrufbar gehalten werden, vor unbefugter Veränderung und unbefugtem Abruf zu schützen sowie
3. bei Erzeugung qualifizierter Zeitstempel Fälschungen und Verfälschungen auszuschließen.

(4) Die Erfüllung der Anforderungen nach den Absätzen 1 und 3 Nr. 1 sowie der Rechtsverordnung nach § 24 ist durch eine Stelle nach § 18 zu bestätigen. Zur Erfüllung der Anforderungen nach den Absätzen 2 und 3 Nr. 2 und 3 genügt eine Erklärung durch den Hersteller des Produkts für qualifizierte elektronische Signaturen. Der Hersteller hat spätestens zum Zeitpunkt des Inverkehrbringens des Produkts eine Ausfertigung seiner Erklärung in schriftlicher Form bei der Regulierungsbehörde für Telekommunikation und Post zu hinterlegen. Herstellererklärungen, die den Anforderungen des Gesetzes und der Rechtsverordnung nach § 24 entsprechen, werden im Amtsblatt der Regulierungsbehörde für Telekommunikation und Post veröffentlicht.

SigG 2001 § 18 Anerkennung von Prüf- und Bestätigungsstellen

(1) Die zuständige Behörde erkennt eine natürliche oder juristische Person auf Antrag als Bestätigungsstelle nach § 17 Abs. 4 oder § 15 Abs. 7 Satz 1 oder als Prüf- und Bestätigungsstelle nach § 15 Abs. 2 an, wenn diese die für die Tätigkeit erforderliche Zuverlässigkeit, Unabhängigkeit und Fachkunde nachweist. Die Anerkennung kann inhaltlich beschränkt, vorläufig oder mit einer Befristung versehen erteilt werden und mit Auflagen verbunden sein.

(2) Die nach Absatz 1 anerkannten Stellen haben ihre Aufgaben unparteiisch, weisungsfrei und gewissenhaft zu erfüllen. Sie haben die Prüfungen und Bestätigungen zu dokumentieren und die Dokumentation im Falle der Einstellung ihrer Tätigkeit an die zuständige Behörde zu übergeben.

Fünfter Abschnitt Aufsicht

SigG 2001 § 19 Aufsichtsmaßnahmen

(1) Die Aufsicht über die Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 obliegt der zuständigen Behörde; diese kann sich bei der Durchführung der Aufsicht privater Stellen bedienen. Mit der Aufnahme des Betriebes unterliegt ein Zertifizierungsdiensteanbieter der Aufsicht der zuständigen Behörde.

(2) Die zuständige Behörde kann gegenüber Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Einhaltung dieses Gesetzes und der Rechtsverordnung nach § 24 treffen.

(3) Die zuständige Behörde hat einem Zertifizierungsdiensteanbieter den Betrieb vorübergehend, teilweise oder ganz zu untersagen, wenn Tatsachen die Annahme rechtfertigen, dass er

1. nicht die für den Betrieb eines Zertifizierungsdienstes erforderliche Zuverlässigkeit besitzt,
2. nicht nachweist, dass die für den Betrieb erforderliche Fachkunde vorliegt,
3. nicht über die erforderliche Deckungsvorsorge verfügt,
4. ungeeignete Produkte für qualifizierte elektronische Signaturen verwendet oder
5. die weiteren Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 nicht erfüllt

und Maßnahmen nach Absatz 2 keinen Erfolg versprechen.

(4) Die zuständige Behörde kann eine Sperrung von qualifizierten Zertifikaten anordnen, wenn Tatsachen die Annahme rechtfertigen, dass qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder dass sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen.

(5) Die Gültigkeit der von einem Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikate bleibt von der Untersagung des Betriebes und der Einstellung der Tätigkeit sowie der Rücknahme und dem Widerruf einer Akkreditierung unberührt.

(6) Die zuständige Behörde hat die Namen der bei ihr angezeigten Zertifizierungsdiensteanbieter sowie der Zertifizierungsdiensteanbieter, die ihre Tätigkeit nach § 13 eingestellt haben oder deren Betrieb nach § 19 Abs. 3 untersagt wurde, für jeden über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten.

SigG 2001 § 20 Mitwirkungspflicht

(1) Die Zertifizierungsdiensteanbieter und die für diese nach § 4 Abs. 5 tätigen Dritten haben der zuständigen Behörde und den in ihrem Auftrag handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten, auf Verlangen die in Betracht kommenden Bücher, Aufzeichnungen, Belege, Schriftstücke und sonstigen Unterlagen in geeigneter Weise zur Einsicht vorzulegen, auch soweit sie in elektronischer Form geführt werden, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren.

(2) Der zur Erteilung einer Auskunft Verpflichtete kann die Auskunft verweigern, wenn er sich damit selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr der Verfolgung wegen einer Straftat oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Er ist auf dieses Recht hinzuweisen.

Sechster Abschnitt Schlussbestimmungen

SigG 2001 § 21 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4 Abs. 2 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, 3 und 4, einen Zertifizierungsdienst betreibt,
2. entgegen § 4 Abs. 3 Satz 1 oder § 13 Abs. 1 Satz 1 eine Anzeige nicht, nicht richtig oder nicht rechtzeitig erstattet,
3. entgegen § 5 Abs. 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 eine Person nicht, nicht richtig oder nicht rechtzeitig identifiziert,
4. entgegen § 5 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, ein qualifiziertes Zertifikat nicht nachprüfbar hält,
5. entgegen § 5 Abs. 1 Satz 3 ein qualifiziertes Zertifikat abrufbar hält,
6. entgegen § 5 Abs. 2 Satz 3 oder 4 eine Angabe in ein qualifiziertes Zertifikat aufnimmt,
7. entgegen § 5 Abs. 4 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Vorkehrung nicht oder nicht richtig trifft,
8. entgegen § 5 Abs. 4 Satz 3 einen Signaturschlüssel speichert,
9. entgegen § 10 Abs. 1 Satz 1, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, eine Sicherheitsmaßnahme oder ein qualifiziertes Zertifikat nicht, nicht richtig oder nicht rechtzeitig dokumentiert,
10. entgegen § 13 Abs. 1 Satz 2, auch in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1, nicht dafür sorgt, dass ein qualifiziertes Zertifikat von einem anderen Zertifizierungsdiensteanbieter übernommen wird und ein qualifiziertes Zertifikat nicht oder nicht rechtzeitig sperrt oder
11. entgegen § 13 Abs. 1 Satz 3 in Verbindung mit einer Rechtsverordnung nach § 24 Nr. 1 einen Signaturschlüssel-Inhaber nicht, nicht richtig oder nicht rechtzeitig benachrichtigt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1, 7 und 8 mit einer Geldbuße bis zu fünfzigtausend Euro, in den übrigen Fällen mit einer Geldbuße bis zu zehntausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.

SigG 2001 § 22 Kosten und Beiträge

(1) Die zuständige Behörde erhebt für ihre folgenden Amtshandlungen Kosten (Gebühren und Auslagen):

1. Maßnahmen im Rahmen der freiwilligen Akkreditierung von Zertifizierungsdiensteanbietern nach § 15 und der Rechtsverordnung nach § 24,
2. Maßnahmen im Rahmen der Ausstellung der qualifizierten Zertifikate nach § 16 Abs. 1 sowie der Ausstellung von Bescheinigungen nach § 16 Abs. 3,
3. Maßnahmen im Rahmen der Anerkennung von Prüf- und Bestätigungsstellen nach § 18 und der Rechtsverordnung nach § 24,
4. Maßnahmen im Rahmen der Aufsicht nach § 19 Abs. 1 bis 4 in Verbindung mit § 4 Abs. 2 bis 4 und der Rechtsverordnung nach § 24.

Kosten werden auch für den Verwaltungsaufwand erhoben, der dadurch entsteht, dass sich die Behörde bei der Durchführung der Aufsicht privater Stellen bedient. Das Verwaltungskostengesetz findet Anwendung.

(2) Zertifizierungsdiensteanbieter, die den Betrieb nach § 4 Abs. 3 angezeigt haben, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der

Voraussetzungen nach § 19 Abs. 6 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird. Zertifizierungsdiensteanbieter, die nach § 15 Abs. 1 akkreditiert sind, haben zur Abgeltung des Verwaltungsaufwands für die ständige Erfüllung der Voraussetzungen nach § 16 Abs. 2 eine Abgabe an die zuständige Behörde zu entrichten, die als Jahresbeitrag erhoben wird.

SigG 2001 § 23 Ausländische elektronische Signaturen und Produkte für elektronische Signaturen

(1) Elektronische Signaturen, für die ein ausländisches qualifiziertes Zertifikat aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie Artikel 5 Abs. 1 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2) in der jeweils geltenden Fassung entsprechen, qualifizierten elektronischen Signaturen gleichgestellt. Elektronische Signaturen aus Drittstaaten sind qualifizierten elektronischen Signaturen gleichgestellt, wenn das Zertifikat von einem dortigen Zertifizierungsdiensteanbieter öffentlich als qualifiziertes Zertifikat ausgestellt und für eine elektronische Signatur im Sinne von Artikel 5 Abs. 1 der Richtlinie 1999/93/EG bestimmt ist und wenn

1. der Zertifizierungsdiensteanbieter die Anforderungen der Richtlinie erfüllt und in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum akkreditiert ist oder
2. ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, welcher die Anforderungen der Richtlinie erfüllt, für das Zertifikat einsteht oder
3. das Zertifikat oder der Zertifizierungsdiensteanbieter im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Union und Drittstaaten oder internationalen Organisationen anerkannt ist.

(2) Elektronische Signaturen nach Absatz 1 sind qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung nach § 15 Abs. 1 gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

(3) Produkte für elektronische Signaturen, bei denen in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie 1999/93/EG in der jeweils geltenden Fassung entsprechen, werden anerkannt. Den nach § 15 Abs. 7 geprüften Produkten für qualifizierte elektronische Signaturen werden Produkte für elektronische Signaturen aus einem in Satz 1 genannten Staat oder aus einem Drittstaat gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.

SigG 2001 § 24 Rechtsverordnung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung die zur Durchführung der §§ 3 bis 23 erforderlichen Rechtsvorschriften zu erlassen über

1. die Ausgestaltung der Pflichten der Zertifizierungsdiensteanbieter in Bezug auf die Betriebsaufnahme und während des Betriebes sowie bei Einstellung des Betriebes nach § 4 Abs. 2 und 3, §§ 5, 6 Abs. 1, §§ 8, 10, 13 und 15,
2. die gebührenpflichtigen Tatbestände und die Gebührensätze sowie die Höhe der Beiträge und das Verfahren der Beitragserhebung durch die zuständige Behörde; bei der Bemessung der Beiträge ist der Verwaltungsaufwand (Personal- und Sachaufwand) sowie Investitionsaufwand zugrunde zu legen soweit er nicht bereits durch eine Gebühr abgegolten wird,
3. die Ausgestaltung des Inhalts und die Gültigkeitsdauer von qualifizierten Zertifikaten nach § 7,
4. die zur Erfüllung der Verpflichtung zur Deckungsvorsorge nach § 12

zulässigen Sicherheitsleistungen sowie deren Umfang, Höhe und inhaltliche Ausgestaltung,

5. die näheren Anforderungen an Produkte für qualifizierte elektronische Signaturen nach § 17 Abs. 1 bis 3 sowie die Prüfung dieser Produkte und die Bestätigung, dass die Anforderungen erfüllt sind, nach § 17 Abs. 4 und § 15 Abs. 7,
6. die Einzelheiten des Verfahrens der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen nach § 18,
7. den Zeitraum sowie das Verfahren, nach dem Daten mit einer qualifizierten elektronischen Signatur nach § 6 Abs. 1 Satz 2 neu signiert werden sollten,
8. das Verfahren zur Feststellung der gleichwertigen Sicherheit von ausländischen elektronischen Signaturen und ausländischen Produkten für elektronische Signaturen nach § 23.

SigG 2001 § 25 Übergangsvorschriften

(1) Die nach dem Signaturgesetz vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), genehmigten Zertifizierungsstellen gelten als akkreditiert im Sinne von § 15. Diese haben der zuständigen Behörde innerhalb von drei Monaten nach Inkrafttreten dieses Gesetzes einen Deckungsnachweis nach § 12 vorzulegen.

(2) Die von den Zertifizierungsstellen nach Absatz 1 bis zum Zeitpunkt des Inkrafttretens dieses Gesetzes nach § 5 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), ausgestellten Zertifikate sind qualifizierten Zertifikaten gleichgestellt. Inhaber von Zertifikaten nach Satz 1 sind innerhalb von sechs Monaten nach Inkrafttreten dieses Gesetzes durch die Zertifizierungsstelle nach § 6 Abs. 2 in geeigneter Weise zu unterrichten.

(3) Die von der zuständigen Behörde erfolgten Anerkennungen von Prüf- und Bestätigungsstellen nach § 4 Abs. 3 Satz 3 und § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872), geändert durch Artikel 5 des Gesetzes vom 19. Dezember 1998 (BGBl. I S. 3836), behalten ihre Gültigkeit, soweit sie in Übereinstimmung mit § 18 dieses Gesetzes stehen.

(4) Technische Komponenten, bei denen die Erfüllung der Anforderungen nach § 14 Abs. 4 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872) geprüft und bestätigt wurde, sind Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 dieses Gesetzes gleichgestellt.

Strafgesetzbuch

§ 184 StGB: Verbreitung pornographischer Schriften

(1) Wer pornographische Schriften (§ 11 Abs. 3)

1. einer Person unter achtzehn Jahren anbietet, überlässt oder zugänglich macht,
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, ausstellt, anschlägt, vorführt oder sonst zugänglich macht,
3. im Einzelhandel außerhalb von Geschäftsräumen, in Kiosken oder anderen Verkaufsstellen, die der Kunde nicht zu betreten pflegt, im Versandhandel oder in gewerblichen Leihbüchereien oder Lesezirkeln einem anderen anbietet oder überlässt,

3a. im Wege gewerblicher Vermietung oder vergleichbarer gewerblicher Gewährung des Gebrauchs, ausgenommen in Ladengeschäften, die Personen unter achtzehn Jahren nicht zugänglich sind und von ihnen nicht eingesehen werden können, einem anderen anbietet oder überlässt,

4. im Wege des Versandhandels einzuführen unternimmt,
5. öffentlich an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, oder durch Verbreiten von Schriften außerhalb des Geschäftsverkehrs mit dem einschlägigen Handel anbietet, ankündigt oder anpreist,
6. an einen anderen gelangen lässt, ohne von diesem hierzu aufgefordert zu sein,
7. in einer öffentlichen Filmvorführung gegen ein Entgelt zeigt, das ganz oder überwiegend für diese Vorführung verlangt wird,
8. herstellt, bezieht, liefert, vorrätig hält oder einzuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 bis 7 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, oder
9. auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Ausland unter Verstoß gegen die dort geltenden Strafvorschriften zu verbreiten oder öffentlich zugänglich zu machen oder eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Absatz 1 Nr. 1 ist nicht anzuwenden, wenn der zur Sorge für die Person Berechtigte handelt; dies gilt nicht, wenn der Sorgeberechtigte durch das Anbieten, Überlassen oder Zugänglichmachen seine Erziehungspflicht gröblich verletzt. Absatz 1 Nr. 3a gilt nicht, wenn die Handlung im Geschäftsverkehr mit gewerblichen Entleihern erfolgt.

§ 184a StGB: Verbreitung gewalt- oder tierpornographischer Schriften

Wer pornographische Schriften (§ 11 Abs. 3), die Gewalttätigkeiten oder sexuelle Handlungen von Menschen mit Tieren zum Gegenstand haben,

1. verbreitet,
2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder
3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 184b StGB: Verbreitung, Erwerb und Besitz kinderpornographischer Schriften

(1) Wer pornographische Schriften (§ 11 Abs. 3), die den sexuellen Missbrauch von Kindern (§§ 176 bis 176b) zum Gegenstand haben (kinderpornographische Schriften),

1. verbreitet,
2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht oder
3. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.

(2) Ebenso wird bestraft, wer es unternimmt, einem anderen den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.

(3) In den Fällen des Absatzes 1 oder des Absatzes 2 ist auf Freiheitsstrafe von sechs Monaten bis zu zehn Jahren zu erkennen, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und die kinderpornographischen Schriften ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben.

(4) Wer es unternimmt, sich den Besitz von kinderpornographischen Schriften zu verschaffen, die ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergeben, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer die in Satz 1 bezeichneten Schriften besitzt.

(5) Die Absätze 2 und 4 gelten nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.

(6) In den Fällen des Absatzes 3 ist § 73d anzuwenden. Gegenstände, auf die sich eine Straftat nach Absatz 2 oder Absatz 4 bezieht, werden eingezogen. § 74a ist anzuwenden.

§ 184c StGB: Verbreitung pornographischer Darbietungen durch Rundfunk, Medien- oder Teledienste

Nach den §§ 184 bis 184b wird auch bestraft, wer eine pornographische Darbietung durch Rundfunk, Medien- oder Teledienste verbreitet. In den Fällen des § 184 Abs. 1 ist Satz 1 bei einer Verbreitung durch Medien- oder Teledienste nicht anzuwenden, wenn durch technische oder sonstige Vorkehrungen sichergestellt ist, dass die pornographische Darbietung Personen unter achtzehn Jahren nicht zugänglich ist.

§ 184f StGB Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. sexuelle Handlungen nur solche, die im Hinblick auf das jeweils geschützte Rechtsgut von einiger Erheblichkeit sind,
2. sexuelle Handlungen vor einem anderen nur solche, die vor einem anderen vorgenommen werden, der den Vorgang wahrnimmt.

§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 206 StGB: Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekannt geworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 303a StGB: Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 303b StGB: Computersabotage

(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Telekommunikationsgesetz

Teil 7 Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit

Abschnitt 1 Fernmeldegeheimnis

§ 88 TKG 2004: Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) 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.

(3) 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. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Fahrzeugs für Seefahrt oder Luftfahrt, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

§ 89 TKG 2004: Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

Mit einer Funkanlage dürfen nur Nachrichten, die für den Betreiber der Funkanlage, Funkamateure im Sinne des Gesetzes über den Amateurfunk vom 23. Juni 1997 (BGBl. I S. 1494), die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, abgehört werden. Der Inhalt anderer als in Satz 1 genannter Nachrichten sowie die Tatsache ihres Empfangs dürfen, auch wenn der Empfang unbeabsichtigt geschieht, auch von Personen, für die eine Pflicht zur Geheimhaltung nicht schon nach § 88 besteht, anderen nicht mitgeteilt werden. § 88 Abs. 4 gilt entsprechend. Das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.

§ 109 TKG 2004: Technische Schutzmaßnahmen

(1) Jeder Diensteanbieter hat angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze

1. des Fernmeldegeheimnisses und personenbezogener Daten und
2. der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen.

(2) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat darüber hinaus bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Dabei sind der Stand der technischen Entwicklung sowie die räumliche Unterbringung eigener Netzelemente oder mitbenutzter Netzteile anderer Netzbetreiber zu berücksichtigen. Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Betreiber der Anlagen die Verpflichtungen nach Absatz 1 und Satz 1 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Betreiber zugeordnet werden können. Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht.

(3) Wer Telekommunikationsanlagen betreibt, die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, hat einen Sicherheitsbeauftragten oder eine Sicherheitsbeauftragte zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

1. welche Telekommunikationsanlagen eingesetzt und welche Telekommunikationsdienste für die Öffentlichkeit erbracht werden,
2. von welchen Gefährdungen auszugehen ist und
3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind.

Das Sicherheitskonzept ist der Regulierungsbehörde unverzüglich nach Aufnahme der Telekommunikationsdienste vom Betreiber vorzulegen, verbunden mit einer Erklärung, dass die darin aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden. Stellt die Regulierungsbehörde im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie vom Betreiber deren unverzügliche Beseitigung verlangen. Sofern sich die dem Sicherheitskonzept zu Grunde liegenden Gegebenheiten ändern, hat der Betreiber das Konzept anzupassen und der Regulierungsbehörde unter Hinweis auf die Änderungen erneut vorzulegen. Die Sätze 1 bis 4 gelten nicht für Betreiber von Telekommunikationsanlagen, die ausschließlich dem Empfang oder der Verteilung von Rundfunksignalen dienen. Für Sicherheitskonzepte, die der Regulierungsbehörde auf der Grundlage des § 87 des Telekommunikationsgesetzes vom 25. Juli 1996 (BGBl. I S. 1120) vorgelegt wurden, gilt die Verpflichtung nach Satz 2 als erfüllt.

Bayerisches Beamtengesetz

Art. 86 BayBG: Fürsorgepflicht

[1] Der Dienstherr hat im Rahmen des Dienst- und Treueverhältnisses für das Wohl des Beamten und seiner Familie, auch für die Zeit nach Beendigung des Beamtenverhältnisses, zu sorgen. [2] Er schützt ihn bei seiner amtlichen Tätigkeit und in seiner Stellung als Beamter.

Bayerisches Personalvertretungsgesetz

Art. 70 BayPVG: Formen und Verfahren der Mitbestimmung und Mitwirkung

(1) [1] Soweit eine Maßnahme der Mitbestimmung des Personalrats unterliegt (Art. 75, 75a Abs. 1), kann sie nur mit seiner Zustimmung getroffen werden. [2] Das gilt, ausgenommen in den Fällen des Art. 75 Abs. 1, auch, soweit eine Maßnahme nur als Versuch oder zur Erprobung durchgeführt werden soll. [3] Die beabsichtigte Maßnahme ist auf Antrag des Personalrats vor der Durchführung mit dem Ziel einer Verständigung eingehend mit ihm zu erörtern. [4] Bei Gemeinden und Gemeindeverbänden, sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts soll die Mitbestimmung des Personalrats erfolgen, bevor das zuständige Organ endgültig entscheidet. [5] Der Beschluss des Personalrats ist dem zuständigen Organ zur Kenntnis zu bringen.

(2) [1] Der Leiter der Dienststelle unterrichtet den Personalrat schriftlich von der beabsichtigten Maßnahme und beantragt seine Zustimmung. [2] Die Gründe für die beabsichtigte Maßnahme sollen angegeben werden. [3] Der Beschluss des Personalrats über die beantragte Zustimmung ist dem Leiter der Dienststelle innerhalb von zwei Wochen mitzuteilen. [4] In dringenden Fällen kann der Leiter der Dienststelle diese Frist auf eine Woche abkürzen. [5] Die Maßnahme gilt als gebilligt, wenn nicht der Personalrat innerhalb der genannten Frist die Zustimmung unter Angabe der Gründe schriftlich verweigert. [6] Soweit der Personalrat dabei Beschwerden oder Behauptungen tatsächlicher Art vorträgt, die für einen Beschäftigten ungünstig sind oder ihm nachteilig werden können, hat der Leiter der Dienststelle dem Beschäftigten Gelegenheit zur Äußerung zu geben; die Äußerung ist aktenkundig zu machen.

Art. 75 BayPVG: Angelegenheiten, in denen der Personalrat zu beteiligen ist

(1) [1] Der Personalrat hat mitzubestimmen in Personalangelegenheiten bei 1. Einstellung - mit Ausnahme der Fälle, in denen das Beamtenverhältnis nach Ablegung der Laufbahnprüfung auf Grund von Rechtsvorschriften endet (Art. 43 Abs. 2 BayBG) und der Vorbereitungsdienst eine allgemeine Ausbildungsstätte im Sinn des Art. 12 Abs. 1 Satz 1 des Grundgesetzes ist

1. Anstellung, Ernennung zum Beamten auf Lebenszeit;
2. Beförderung, Übertragung eines anderen Amts mit höherem Endgrundgehalt ohne Änderung der Amtsbezeichnung, Verleihung eines anderen Amts mit anderer Amtsbezeichnung beim Wechsel der Laufbahngruppe;
3. Übertragung der Dienstaufgaben eines anderen Amtes mit höherem oder niedrigerem Endgrundgehalt für eine Dauer von mehr als sechs Monaten, Zulassung zum Aufstieg in die nächst höhere Laufbahngruppe;
4. Höhergruppierung, Übertragung einer höher zu bewertenden Tätigkeit für eine Dauer von mehr als sechs Monaten;
5. Rückgruppierung, Übertragung einer niedriger zu bewertenden Tätigkeit für eine Dauer von mehr als sechs Monaten;
6. Versetzung, Umsetzung innerhalb der Dienststelle, wenn sie mit einem Wechsel des Dienstorts verbunden ist (das Einzugsgebiet im Sinn des Umzugskostenrechts gehört zum Dienstort), es sei denn, dass der Beschäftigte mit der Versetzung oder Umsetzung einverstanden ist;
7. Abordnung für eine Dauer von mehr als drei Monaten, es sei denn, dass der Beschäftigte mit der Abordnung einverstanden ist;
8. Hinausschiebung des Eintritts in den Ruhestand wegen Erreichens der Altersgrenze;
9. Weiterbeschäftigung von Arbeitnehmern über die Altersgrenze hinaus;
10. Anordnungen, welche die Freiheit in der Wahl der Wohnung beschränken;
11. Versagung oder Widerruf der Genehmigung einer Nebentätigkeit, soweit es sich nicht um Beschäftigte handelt, bei deren Einstellung das Mitbestimmungsrecht des Personalrats nach Nummer 1 ausgeschlossen ist;
12. Ablehnung eines Antrags auf Teilzeitbeschäftigung, Ermäßigung der Arbeitszeit oder Urlaub oder Widerruf einer genehmigten Teilzeitbeschäftigung;
13. Geltendmachung von Ersatzansprüchen gegen einen Beschäftigten;
14. Zuweisung nach § 123a des Beamtenrechtsrahmengesetzes für eine Dauer von mehr als drei Monaten.

[2] Bei der Geltendmachung von Ersatzansprüchen gegen einen Beschäftigten (Satz 1 Nr. 13) wird der Personalrat nur auf Antrag des Beschäftigten beteiligt; dieser ist von der beabsichtigten Maßnahme rechtzeitig vorher in Kenntnis zu setzen.

(2) Der Personalrat kann die Zustimmung zu einer Maßnahme nach Absatz 1 nur verweigern, wenn die Maßnahme gegen ein Gesetz, eine Verordnung, eine Bestimmung in einem Tarifvertrag, eine gerichtliche Entscheidung oder eine Verwaltungsanordnung oder gegen eine Richtlinie im Sinn des Absatzes 4 Satz 1 Nr. 13 verstößt oder die durch Tatsachen begründete Besorgnis besteht, dass durch die Maßnahme der betroffene Beschäftigte oder andere Beschäftigte benachteiligt werden, ohne dass dies aus dienstlichen oder persönlichen Gründen gerechtfertigt ist oder die durch Tatsachen begründete Besorgnis besteht, dass der Beschäftigte oder Bewerber den Frieden in der Dienststelle durch unsoziales oder gesetzwidriges Verhalten stören werde.

(3) [1] Der Personalrat hat mitzubestimmen in sozialen Angelegenheiten bei

1. Gewährung von Unterstützungen, Vorschüssen, Darlehen und entsprechenden sozialen Zuwendungen, wenn der Beschäftigte es beantragt;
2. Zuweisung und Kündigung von Wohnungen, über die die Dienststelle verfügt;
3. Zuweisung von Dienst- und Pachtland und Festsetzung der Nutzungsbedingungen.

[2] In den Fällen des Satzes 1 Nr. 1 bestimmt auf Verlangen des Antragstellers nur der Vorstand des Personalrats mit. 3 Die Dienststelle hat dem Personalrat nach Abschluss jedes Kalenderjahres einen Überblick über die Unterstützungen und entsprechenden sozialen Zuwendungen zu geben. 4 Dabei sind die Anträge und die Leistungen gegenüberzustellen. 5 Auskunft über die von den Antragstellern angeführten Gründe wird hierbei nicht erteilt.

(4) [1] Der Personalrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, ferner mitzubestimmen über

1. Beginn und Ende der täglichen Arbeitszeit und der Pausen sowie die Verteilung der Arbeitszeit auf die einzelnen Wochentage;
2. Zeit, Ort und Art der Auszahlung der Dienstbezüge und Arbeitsentgelte;
3. Aufstellung des Urlaubsplans;
4. Fragen der Lohngestaltung innerhalb der Dienststelle, insbesondere die Aufstellung von Entlohnungsgrundsätzen, die Einführung und Anwendung von neuen Entlohnungsmethoden und deren Änderung sowie die Festsetzung der Akkord- und Prämiensätze und vergleichbarer leistungsbezogener Entgelte, einschließlich der Geldfaktoren;
5. Errichtung, Verwaltung und Auflösung von Sozialeinrichtungen ohne Rücksicht auf ihre Rechtsform;
6. Durchführung der Berufsausbildung bei Arbeitnehmern;
7. Bestellung von Vertrauens- und Betriebsärzten;
8. Maßnahmen zur Verhütung von Dienst- und Arbeitsunfällen und sonstigen Gesundheitsschädigungen;

9. Grundsätze über die Bewertung von anerkannten Vorschlägen im Rahmen des betrieblichen Vorschlagwesens;
10. Inhalt von Personalfragebogen;
11. Beurteilungsrichtlinien;
12. Aufstellung von Sozialplänen einschließlich Plänen für Umschulungen zum Ausgleich oder zur Milderung von wirtschaftlichen Nachteilen, die dem Beschäftigten infolge von Rationalisierungsmaßnahmen entstehen;
13. Erlass von Richtlinien über die personelle Auswahl bei Einstellungen, Versetzungen, Umgruppierungen und Kündigungen.

[2] Muss für Gruppen von Beschäftigten die tägliche Arbeitszeit (Satz 1 Nr. 1) nach Erfordernissen, die die Dienststelle nicht voraussehen kann, unregelmäßig und kurzfristig festgesetzt werden, so beschränkt sich die Mitbestimmung auf die Grundsätze für die Aufstellung der Dienstpläne.

Art. 75a BayPVG

(1) Der Personalrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, mitzubestimmen bei

1. Einführung, Anwendung und erheblicher Änderung technischer Einrichtungen zur Überwachung des Verhaltens oder der Leistung der Beschäftigten,
2. Einführung, Anwendung und erheblicher Änderung von automatisierten Verfahren zur Personalverwaltung.

(2) [1] Der Personalrat ist von der Erteilung von Aufträgen für Organisationsuntersuchungen, die Maßnahmen nach Absatz 1 vorausgehen, rechtzeitig und umfassend zu unterrichten. [2] Das Ergebnis dieser Organisationsuntersuchungen ist mit ihm zu erörtern.

Art. 76 BayPVG

(1) [1] Der Personalrat wirkt mit in sozialen und persönlichen Angelegenheiten bei

1. Vorbereitung von Verwaltungsanordnungen einer Dienststelle für die innerdienstlichen sozialen oder persönlichen Angelegenheiten der Beschäftigten ihres Geschäftsbereichs;
2. Regelung der Ordnung in der Dienststelle und des Verhaltens der Beschäftigten;
3. Erlass von Disziplinarverfügungen und bei Erhebung der Disziplinarklage gegen einen Beamten, wenn dem Disziplinarverfahren eine auf den gleichen Tatbestand gestützte Disziplinarverfügung nicht vorausgegangen ist;
4. Verlängerung der Probezeit
5. Entlassung von Beamten auf Probe oder auf Widerruf, wenn sie die Entlassung nicht selbst beantragt haben;
6. vorzeitiger Versetzung in den Ruhestand;
7. allgemeinen Fragen der Fortbildung der Beschäftigten;
8. Aufstellung von Grundsätzen für die Auswahl von Teilnehmern an Fortbildungsveranstaltungen.

[2] Satz 1 Nr. 2 gilt nicht für Polizei, Berufsfeuerwehr und Strafvollzug im Fall eines Notstands. [3] In den Fällen von Satz 1 Nrn. 3 bis 6 wird der Personalrat nur auf Antrag des Beschäftigten beteiligt; in diesen Fällen ist der Beschäftigte von der beabsichtigten Maßnahme rechtzeitig vorher in Kenntnis zu setzen. [4] Im Fall des Satzes 1 Nr. 3 kann der Beschäftigte die Beteiligung desjenigen Personalrats beantragen, der an der Dienststelle, der der betroffene Beschäftigte angehört, gebildet ist; in den Fällen des Art. 80 Abs. 2 und 3 kann der Beschäftigte stattdessen die Beteiligung der danach bestimmten Personalvertretung beantragen. [5] Der Personalrat kann bei der Mitwirkung nach Satz 1 Nr. 3 Einwendungen auf die in Art. 75 Abs. 2 Nrn. 1 und 2 bezeichneten Gründe stützen.

(2) Der Personalrat wirkt mit bei

1. Einführung grundlegend neuer Arbeitsmethoden;
2. Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufs;
3. Gestaltung der Arbeitsplätze;
4. Auflösung, Verlegung und Zusammenlegung von Dienststellen oder wesentlichen Teilen von ihnen;
5. Aufstellung von Grundsätzen für die Personalbedarfsberechnung.

(3) [1] Vor der Weiterleitung von Personalanforderungen zum Haushaltsvoranschlag ist der Personalrat anzuhören. [2] Gibt der Personalrat einer nachgeordneten Dienststelle zu den Personalanforderungen eine Stellungnahme ab, so ist diese mit den Personalanforderungen der übergeordneten Dienststelle vorzulegen. [3] Das gilt entsprechend für Neu-, Um- und Erweiterungsbauten von Diensträumen.

Verordnung zur elektronischen Signatur

Datum: 16. November 2001

Fundstelle: BGBl I 2001, 3074

Textnachweis ab: 22.11.2001
Amtlicher Hinweis des Normgebers auf EG-Recht:
Beachtung der
EGRL 34/98 (CELEX Nr: 398L0034)
(+++ Stand: Geändert durch Art. 2 G v. 4. 1.2005 I 2 +++)

Die Mitteilungspflichten der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften (ABl. EG Nr. L 204 S. 37), zuletzt geändert durch die Richtlinie 98/48/EG des Europäischen Parlaments und des Rates vom 20. Juli 1998 (ABl. EG Nr. L 217 S. 18) sind beachtet worden.

SigV 2001 Eingangsformel

Auf Grund des § 24 des Signaturgesetzes vom 16. Mai 2001 (BGBl. I S. 876) in Verbindung mit dem 2. Abschnitt des Verwaltungskostengesetzes vom 23. Juni 1970 (BGBl. I S. 821) verordnet die Bundesregierung:

SigV 2001 Inhaltsübersicht

SigV 2001 § 1 Form, Inhalt und Änderung der Anzeige

(1) Eine Anzeige nach § 4 Abs. 3 des Signaturgesetzes ist schriftlich oder mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen bei der

zuständigen Behörde vorzunehmen.

(2) Die Anzeige muss folgende Angaben und Unterlagen umfassen:

1. den Namen und die Anschrift des Zertifizierungsdiensteanbieters,
2. die Namen der gesetzlichen Vertreter,
3. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für den Zertifizierungsdiensteanbieter und seine gesetzlichen Vertreter,
4. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,
5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 4 Abs. 2 Satz 3 des Signaturgesetzes,
6. ein Sicherheitskonzept mit einer genauen Darlegung, wie dieses umgesetzt ist, einschließlich der Übertragung von Aufgaben an Dritte nach § 4 Abs. 5 des Signaturgesetzes, und
7. einen Nachweis der Deckungsvorsorge nach § 12 des Signaturgesetzes.

Ändern sich die Umstände nach Satz 1 Nr. 1 oder Nr. 2 oder sicherheitserhebliche Umstände nach Satz 1 Nr. 6, ist die zuständige Behörde schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu informieren. § 2 bleibt unberührt.

(3) Soweit Teile des Zertifizierungsdienstes in einem Staat nach § 23 Abs. 1 Satz 1 des Signaturgesetzes oder unter den Bedingungen des § 23 Abs. 1 Satz 2 Nr. 3 des Signaturgesetzes in einem Drittstaat betrieben werden, sind zusätzlich Nachweise darüber vorzulegen, dass der Betrieb einer gleichwertigen Aufsicht unterliegt. Der Betrieb von Teilen des Zertifizierungsdienstes in einem anderen als in Satz 1 genannten Staat ist nur im Rahmen einer freiwilligen Akkreditierung zulässig, soweit die Sicherstellung der Aufsicht nachgewiesen wird.

SigV 2001 § 2 Inhalt des Sicherheitskonzepts

Das Sicherheitskonzept nach § 4 Abs. 2 Satz 4 des Signaturgesetzes hat Folgendes zu enthalten:

1. eine Beschreibung aller erforderlichen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und deren Eignung,
2. eine Übersicht über die eingesetzten Produkte für qualifizierte elektronische Signaturen mit Herstellererklärungen nach § 17 Abs. 4 Satz 2 oder Bestätigungen nach § 17 Abs. 4 Satz 1 oder nach § 15 Abs. 7 Satz 1 des Signaturgesetzes,
3. eine Übersicht über die Aufbau- und Ablauforganisation sowie die Zertifizierungstätigkeit,
4. die Vorkehrungen und Maßnahmen zur Sicherstellung und Aufrechterhaltung des Betriebes, insbesondere bei Notfällen,
5. die Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals und
6. eine Abschätzung und Bewertung verbleibender Sicherheitsrisiken.

SigV 2001 § 3 Identitätsprüfung und Attributsnachweise

(1) Der Zertifizierungsdiensteanbieter hat die Identifizierung des Antragstellers nach § 5 Abs. 1 des Signaturgesetzes anhand des Personalausweises oder eines Reisepasses, der auf eine Person mit Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union oder eines Staates des Europäischen Wirtschaftsraumes ausgestellt worden ist, oder anhand von Dokumenten mit gleichwertiger Sicherheit vorzunehmen. Soweit ein Antrag auf ein qualifiziertes Zertifikat mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments des Antragstellers gestellt wird, kann der Zertifizierungsdiensteanbieter von einer erneuten Identifizierung absehen. Die Identifizierung ist vor Übergabe des qualifizierten Zertifikats und vor Einstellung in das Zertifikatsverzeichnis gemäß § 4 Abs. 1 vorzunehmen.

(2) Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein qualifiziertes Zertifikat Attribute aufgenommen werden, muss die nach § 5 Abs. 2 Satz 2 oder Satz 4 oder Abs. 3 Satz 2 des Signaturgesetzes erforderliche Einwilligung oder Bestätigung mittels eines

mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich vorliegen. Die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle ist mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments oder schriftlich über den Inhalt des qualifizierten Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung hinzuweisen.

SigV 2001 § 4 Führung eines Zertifikatsverzeichnisses

(1) Der Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens fünf weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.

(2) Ein akkreditierter Zertifizierungsdiensteanbieter hat die von ihm ausgestellten qualifizierten Zertifikate, vorbehaltlich eines späteren Zeitpunktes nach § 5 Abs. 2 Satz 2, ab dem Zeitpunkt ihrer Ausstellung für den im jeweiligen Zertifikat angegebenen Gültigkeitszeitraum sowie mindestens 30 weitere Jahre ab dem Schluss des Jahres, in dem die Gültigkeit des Zertifikates endet, in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen.

(3) Im Falle der Übernahme von qualifizierten Zertifikaten nach § 13 Abs. 1 Satz 2 des Signaturgesetzes gelten die Absätze 1 und 2 entsprechend.

SigV 2001 § 5 Einzelne Sicherheitsvorkehrungen des Zertifizierungsdiensteanbieters

(1) Der Zertifizierungsdiensteanbieter hat durch geeignete Maßnahmen sicherzustellen, dass Signaturschlüssel nur auf der jeweiligen sicheren Signaturerstellungseinheit oder bei ihm oder einem anderen Zertifizierungsdiensteanbieter unter Nutzung von technischen Komponenten nach § 17 Abs. 3 Nr. 1 des Signaturgesetzes erzeugt und auf sichere Signaturerstellungseinheiten übertragen werden. Soweit er auch Wissensdaten zur Identifikation des Signaturschlüssel-Inhabers gegenüber einer sicheren Signaturerstellungseinheit oder technische Komponenten zur Erfassung biometrischer Merkmale und Übertragung von Referenzdaten auf die sichere Signaturerstellungseinheit bereitstellt, hat er auch Vorkehrungen zu treffen, um die Geheimhaltung der Identifikationsdaten zu gewährleisten und deren Speicherung außerhalb der jeweiligen sicheren Signaturerstellungseinheit nach Einbringen in dieselbe auszuschließen.

(2) Der Zertifizierungsdiensteanbieter hat von ihm bereitgestellte Signaturschlüssel und Identifikationsdaten dem Signaturschlüssel-Inhaber auf der sicheren Signaturerstellungseinheit persönlich zu übergeben und die Übergabe von diesem schriftlich oder als mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenes elektronisches Dokument bestätigen zu lassen, es sei denn, es wird eine andere Übergabe vereinbart. Erst nachdem der Signaturschlüssel-Inhaber den Erhalt der sicheren Signaturerstellungseinheit gegenüber dem Zertifizierungsdiensteanbieter bestätigt hat, darf das zugehörige qualifizierte Zertifikat nach § 5 Abs. 1 Satz 2 und 3 des Signaturgesetzes nachprüfbar und, soweit vereinbart, abrufbar gehalten werden.

(3) Der Zertifizierungsdiensteanbieter hat sich zur Erfüllung der Voraussetzungen nach § 5 Abs. 5 des Signaturgesetzes von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren mitwirken, auf geeignete Weise zu überzeugen. Er kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren auszuschließen. Der Zertifizierungsdiensteanbieter hat sich darüber hinaus anhand der Herstellerangaben oder in anderer geeigneter Weise von der Eignung der von ihm eingesetzten Produkte für qualifizierte elektronische Signaturen zu überzeugen und Vorkehrungen zu treffen, um diese vor unbefugtem Zugriff zu schützen.

SigV 2001 § 6 Ausgestaltung der Unterrichtung

Die Unterrichtung des Antragstellers nach § 6 Abs. 1 des Signaturgesetzes hat in allgemein verständlicher Sprache zu erfolgen und sich mindestens auf Folgendes zu erstrecken:

1. die Aufbewahrung und Anwendung der sicheren Signaturerstellungseinheit und geeignete Maßnahmen im Verlustfalle oder bei Verdacht des Mißbrauchs,
2. die Geheimhaltung von persönlichen Identifikationsnummern oder anderen

Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber der sicheren Signaturerstellungseinheit,
3. die erforderlichen Sicherheitsmaßnahmen bei Erzeugung und Prüfung einer qualifizierten elektronischen Signatur,
4. die Möglichkeit von Beschränkungen in qualifizierten Zertifikaten nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes,
5. die Notwendigkeit, Daten mit einer qualifizierten elektronischen Signatur neu zu signieren, falls die Signatur durch Zeitablauf ihren Sicherheitswert verliert,
6. die Existenz eines freiwilligen Akkreditierungssystems,
7. die dem Antragsteller zur Verfügung stehenden Beschwerde- und Schlichtungsmöglichkeiten sowie die Einzelheiten der Inanspruchnahme solcher Verfahren und
8. das Verfahren der Sperrung nach § 7.

Die Informationen sind auf Antrag auch Dritten zur Verfügung zu stellen.

SigV 2001 § 7 Sperrung von qualifizierten Zertifikaten

(1) Der Zertifizierungsdiensteanbieter hat den nach § 8 des Signaturgesetzes zur Sperrung Berechtigten eine Rufnummer bekannt zu geben, unter der diese unverzüglich eine Sperrung der qualifizierten Zertifikate veranlassen können.

(2) Der Zertifizierungsdiensteanbieter hat sich vor Sperrung auf geeignete Weise von der Identität des zur Sperrung Berechtigten zu überzeugen. Die Sperrung von qualifizierten Zertifikaten ist mit Angabe des Datums und der zu diesem Zeitpunkt gültigen gesetzlichen Zeit im Zertifikatsverzeichnis nach § 4 eindeutig kenntlich zu machen.

SigV 2001 § 8 Umfang der Dokumentation

(1) Die Dokumentation nach § 10 des Signaturgesetzes hat sich auf das Sicherheitskonzept, einschließlich aller Änderungen, die Unterlagen zur Fachkunde der im Betrieb tätigen Personen und die vertraglichen Vereinbarungen mit den Antragstellern zu erstrecken.

(2) Zum jeweiligen Antragsteller sind mindestens folgende Angaben und Unterlagen zu dokumentieren:

1. eine Ablichtung des vorgelegten Ausweises oder andere Identitätsnachweise,
2. ein vergebenes Pseudonym,
3. der Nachweis über die Unterrichtung des Antragstellers nach § 6 des Signaturgesetzes,
4. die Nachweise über die Einwilligungen der Berechtigten nach § 5 Abs. 2 Satz 2 und 4 und Abs. 3 Satz 2 des Signaturgesetzes,
5. die Bestätigungen der zuständigen Stellen nach § 5 Abs. 2 Satz 2 des Signaturgesetzes,
6. die ausgestellten qualifizierten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe sowie der Zeitpunkt der Einstellung in das Zertifikatsverzeichnis,
7. die Sperrung von qualifizierten Zertifikaten,
8. Auskünfte nach § 14 Abs. 2 Satz 2 des Signaturgesetzes und
9. die Übergabebestätigungen für Signaturschlüssel und Identifikationsdaten nach § 5 Abs. 2 Satz 1 oder die Erklärung des Signaturschlüssel-Inhabers, wenn er eine andere Übergabe verlangt hat, und gegebenenfalls einen anderen Nachweis.

(3) Die Dokumentation ist vorbehaltlich des Satzes 3 mindestens für den nach § 4 Abs. 1 genannten Zeitraum und bei akkreditierten Zertifizierungsdiensteanbietern mindestens für den nach § 4 Abs. 2 genannten Zeitraum aufzubewahren. Im Falle eines Gerichtsverfahrens, in dem der Nachweis der Zertifizierung von Belang ist, ist unbeschadet des Satzes 1 die Dokumentation mindestens bis zum rechtskräftigen Abschluss des Verfahrens aufzubewahren. Die Dokumentation von Auskünften nach § 14 Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren.

SigV 2001 § 9 Ausgestaltung der Deckungsvorsorge

(1) Die Deckungsvorsorge nach § 12 des Signaturgesetzes kann erbracht werden

1. durch eine Haftpflichtversicherung bei einem im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Versicherungsunternehmen oder
2. durch eine Freistellungs- oder Gewährleistungsverpflichtung eines im Geltungsbereich dieses Gesetzes zum Geschäftsbetrieb befugten Kreditinstituts, wenn gewährleistet ist, dass sie einer Haftpflichtversicherung vergleichbare Sicherheit bietet.

(2) Soweit die Deckungsvorsorge durch eine Versicherung nach Absatz 1 Nr. 1 erbracht wird, gelten die folgenden Bestimmungen:

1. Auf diese Versicherung finden § 158b Abs. 2 und die §§ 158c bis 158k des Gesetzes über den Versicherungsvertrag Anwendung. Zuständige Behörde nach § 158c Abs. 2 des Gesetzes über den Versicherungsvertrag ist die Behörde nach § 66 des Telekommunikationsgesetzes.
2. Die Mindestversicherungssumme muss 2,5 Millionen Euro für den einzelnen Versicherungsfall betragen. Versicherungsfall ist jedes auf den Einzelfall bezogene haftungsauslösende Ereignis im Sinne des § 12 Satz 1 des Signaturgesetzes, unabhängig von der Anzahl der dadurch ausgelösten Schadensfälle. Eine Vereinbarung, wonach ein Fehler, der sich in mehreren Zertifikaten, Zeitstempeln oder in der Auskunft nach § 5 Abs. 1 Satz 2 des Signaturgesetzes auswirkt, als ein Versicherungsfall gilt, ist nicht zulässig. Wird eine Jahreshöchstleistung für alle in einem Versicherungsjahr verursachten Schäden vereinbart, muss sie mindestens das Vierfache der Mindestversicherungssumme betragen.
3. Der räumliche Geltungsbereich des Versicherungsschutzes kann auf den Geltungsbereich der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000, Nr. L 13 S. 2) beschränkt werden.
4. Von der Versicherung kann die Leistung nur ausgeschlossen werden für Ersatzansprüche aus vorsätzlich begangener Pflichtverletzung des Zertifizierungsdiensteanbieters oder der Personen, für die er einzustehen hat.
5. Die Vereinbarung eines Selbstbehaltes bis zu 1 Prozent der Mindestversicherungssumme ist zulässig.

SigV 2001 § 10 Einstellen der Tätigkeit

(1) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der zuständigen Behörde nach § 13 Abs. 1 Satz 1 des Signaturgesetzes spätestens zwei Monate vor Einstellung des Betriebes vornehmen.

(2) Der Zertifizierungsdiensteanbieter soll die Unterrichtung der Signaturschlüssel-Inhaber nach § 13 Abs. 1 Satz 3 des Signaturgesetzes mindestens zwei Monate vor Betriebsaufgabe vornehmen. Er hat den Signaturschlüssel-Inhabern mitzuteilen, ob ein anderer Zertifizierungsdiensteanbieter die Zertifikate übernimmt, und diesen zu benennen.

SigV 2001 § 11 Freiwillige Akkreditierung

(1) Der Antrag auf Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes ist schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu stellen. Der Antrag auf freiwillige Akkreditierung gilt als Anzeige nach § 1, wenn die dort genannten Voraussetzungen erfüllt sind.

(2) Die Nachweise nach § 15 Abs. 1 Satz 2, Abs. 2 Satz 2 und Abs. 7 des Signaturgesetzes sind durch Vorlage der Ergebnisse der Prüf- und Bestätigungsstelle in schriftlicher Form oder mittels eines mit einer qualifizierten elektronischen

Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments zu erbringen. Die regelmäßigen Prüfungen nach § 15 Abs. 2 Satz 2 des Signaturgesetzes sind im Abstand von drei Jahren durchzuführen. Der Prüfbericht und die Bestätigung darüber, dass die Anforderungen des Signaturgesetzes und dieser Verordnung weiterhin in vollem Umfang erfüllt werden, ist der zuständigen Behörde unaufgefordert vorzulegen.

(3) Bei der Prüfung und Bestätigung der Sicherheit von Produkten für qualifizierte elektronische Signaturen nach § 15 Abs. 7 Satz 1 des Signaturgesetzes sind die Vorgaben des Abschnitts I der Anlage 1 zu dieser Verordnung zu beachten.

SigV 2001 § 12 Festsetzung und Erhebung von Kosten

(1) Die gebührenpflichtigen Tatbestände für Amtshandlungen nach § 22 des Signaturgesetzes ergeben sich aus der Anlage 2 zu dieser Verordnung. Auslagen werden nach § 10 des Verwaltungskostengesetzes erhoben. Für den Widerruf oder die Rücknahme oder die Ablehnung eines Antrags oder einer Verwaltungshandlung werden Gebühren nach Maßgabe des § 15 des Verwaltungskostengesetzes erhoben.

(2) Für die Stundensätze nach Nummer 2 der Anlage 2 zu dieser Verordnung ist für jede angefangene Viertelstunde ein Viertel dieser Stundensätze zu berechnen. Werden öffentliche Leistungen durch Angehörige der zuständigen Behörde außerhalb der Behörde erbracht, so sind Gebühren ferner zu berechnen, die innerhalb der üblichen Arbeitszeit liegen oder von der zuständigen Behörde besonders abgegolten werden, sowie für Wartezeiten, die der Kostenschuldner verursacht hat.

SigV 2001 § 13 Festsetzung und Erhebung von Beiträgen

(1) Die Beiträge nach § 22 Abs. 2 Satz 1 des Signaturgesetzes berechnen sich nach dem hierfür erforderlichen Personal- und Sachaufwand der zuständigen Behörde unter Einschluss des Aufwandes für Investitionen. Der Beitragssatz beträgt 0,48 Euro für jedes vom Beitragspflichtigen ausgestellte qualifizierte Zertifikat. Der auf das Allgemeininteresse entfallende Kostenanteil wurde beitragsmindernd berücksichtigt. Die Anteile am verbleibenden Aufwand werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 1 im Zertifikatsverzeichnis zu führen sind, zugeordnet. Die Beitragspflichtigen haben der zuständigen Behörde die Zahl der Zertifikate nach Satz 2 jährlich, spätestens am 31. Januar des Folgejahres mitzuteilen. Kommt ein Beitragspflichtiger der Verpflichtung nach Satz 5 nicht nach, kann die zuständige Behörde eine Schätzung der ausgestellten qualifizierten Zertifikate eines Beitragspflichtigen vornehmen.

(2) Die Kosten des Investitionsaufwandes werden entsprechend den jeweils gültigen steuerlichen Regelungen zur Abschreibung von Investitionsgütern festgelegt.

(3) Für die Beiträge nach § 22 Abs. 2 Satz 2 des Signaturgesetzes gelten die Regelungen der Absätze 1 und 2, mit Ausnahme des Absatzes 1 Satz 4, entsprechend. Die Anteile am verbleibenden Aufwand nach Absatz 1 Satz 1 werden den Beitragspflichtigen entsprechend der Zahl der von ihnen ausgestellten qualifizierten Zertifikate, die nach § 4 Abs. 2 im Zertifikatsverzeichnis zu führen sind, zugeordnet.

(4) Die Beitragspflicht nach § 22 Abs. 2 Satz 1 des Signaturgesetzes beginnt mit dem Monat der Anzeige nach § 4 Abs. 3 des Signaturgesetzes, die Beitragspflicht nach § 22 Abs. 2 Satz 2 des Signaturgesetzes mit dem Monat der Akkreditierung. Die Beitragspflicht endet mit Ablauf des Monats der Einstellung der Tätigkeit nach § 13 Abs. 1 des Signaturgesetzes sowie bei freiwilliger Akkreditierung auch mit Ablauf des Monats des Widerrufs oder der Rücknahme einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes. Der Beitrag wird jährlich erhoben. Maßgeblich ist das Kalenderjahr. Besteht die Beitragspflicht nicht das volle Kalenderjahr, so ist der Beitrag anteilig zu berechnen; die Sätze 1 und 2 gelten entsprechend. Die Beiträge werden nach den Vorschriften des Verwaltungsvollstreckungsgesetzes beigetrieben.

SigV 2001 § 14 Inhalt und Gültigkeitsdauer von qualifizierten Zertifikaten

(1) Die Angaben nach § 7 Abs. 1 des Signaturgesetzes in einem qualifizierten Zertifikat müssen eindeutig sein.

(2) Ein qualifiziertes Attribut-Zertifikat nach § 7 Abs. 2 des Signaturgesetzes muss außer einer eindeutigen Referenz auf das zugrunde liegende qualifizierte Zertifikat mindestens folgende Angaben enthalten und eine qualifizierte elektronische Signatur des Zertifizierungsdiensteanbieters tragen:

1. die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,
2. die Nummer des Attribut-Zertifikates,

3. den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,
4. Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und
5. ein oder mehrere Attribute nach § 5 Abs. 2 des Signaturgesetzes.

(3) Die Gültigkeitsdauer eines qualifizierten Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nicht überschreiten. Die Gültigkeit eines qualifizierten Attribut-Zertifikates endet spätestens mit der Gültigkeit des qualifizierten Zertifikates, auf das es Bezug nimmt.

SigV 2001 § 15 Anforderungen an Produkte für qualifizierte elektronische Signaturen

(1) Sichere Signaturerstellungseinheiten nach § 17 Abs. 1 Satz 1 des Signaturgesetzes müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann. Der Signaturschlüssel darf nicht preisgegeben werden. Bei Nutzung biometrischer Merkmale muss hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein. Die zur Erzeugung und Übertragung von Signaturschlüsseln erforderlichen technischen Komponenten nach § 17 Abs. 1 Satz 2 oder Abs. 3 Nr. 1 des Signaturgesetzes müssen gewährleisten, dass aus einem Signaturprüfschlüssel oder einer Signatur nicht der Signaturschlüssel errechnet werden kann und die Signaturschlüssel nicht dupliziert werden können.

(2) Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass

1. bei der Erzeugung einer qualifizierten elektronischen Signatur
   a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
   b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
   c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird und
2. bei der Prüfung einer qualifizierten elektronischen Signatur
   a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
   b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.

(3) Technische Komponenten nach § 17 Abs. 3 des Signaturgesetzes müssen gewährleisten, dass die Sperrung eines qualifizierten Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte nach Satz 1 müssen beinhalten, ob die nachgeprüften qualifizierten Zertifikate im Verzeichnis der qualifizierten Zertifikate zum angegebenen Zeitpunkt vorhanden und ob sie nicht gesperrt waren. Nur nachprüfbar gehaltene qualifizierte Zertifikate dürfen nicht öffentlich abrufbar sein. Im Falle des § 17 Abs. 3 Nr. 3 des Signaturgesetzes muss gewährleistet sein, dass die zum Zeitpunkt der Erzeugung des qualifizierten Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird.

(4) Sicherheitstechnische Veränderungen an technischen Komponenten nach den Absätzen 1 bis 3 müssen für den Nutzer erkennbar werden.

(5) Eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes muss

1. den Aussteller und das Produkt genau bezeichnen und
2. genaue Angaben darüber enthalten, welche Anforderungen des Signaturgesetzes und dieser Verordnung im Einzelnen erfüllt sind.

Bei der Prüfung und Bestätigung der Sicherheit von Produkten nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes sind die Vorgaben des Abschnitts II der Anlage 1 zu dieser Verordnung zu beachten.

(6) Soweit im Rahmen des Verfahrens nach Artikel 3 Abs. 5 und Artikel 9 der Richtlinie 1999/93/EG in der jeweils geltenden Fassung Referenznummern für allgemein anerkannte Normen für Produkte für qualifizierte elektronische Signaturen festgelegt und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht werden, haben diese abweichend von den Absätzen 1 bis 5 Geltung, mit Ausnahme der Produkte nach § 15 Abs. 7 des Signaturgesetzes. Die zuständige Behörde veröffentlicht im Bundesanzeiger die aktuell gültigen Anforderungen auf Grund der Festlegungen nach Satz 1.

SigV 2001 § 16 Verfahren der Anerkennung sowie der Tätigkeit von Prüf- und Bestätigungsstellen

(1) Ein Antrag einer Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes muss Folgendes umfassen:

1. Namen und Anschrift des Antragstellers und seiner gesetzlichen Vertreter,
2. aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes des Antragstellers nach Nummer 1 und seiner gesetzlichen Vertreter,
3. einen aktuellen Handelsregisterauszug oder eine vergleichbare Unterlage,
4. Belege zum Nachweis der finanziellen Unabhängigkeit, insbesondere über Mindestkapital und vergleichbare Sicherheiten,
5. Belege zum Nachweis der erforderlichen technischen, administrativen und juristischen Fachkunde nach § 18 Abs. 1 Satz 1 des Signaturgesetzes und
6. eine Erklärung, auf welche gesetzliche Tätigkeiten des Signaturgesetzes sich der Antrag bezieht.

(2) Für eine Anerkennung als Bestätigungsstelle für Tätigkeiten nach § 15 Abs. 7 und § 17 Abs. 4 Satz 1 des Signaturgesetzes muss der Antragsteller nachweisen, dass er über ausreichende Erfahrungen in der Anwendung der Prüfkriterien nach Anlage 1 zu dieser Verordnung verfügt. Er muss außerdem darlegen, wie er eine geeignete Überwachung der Prüftätigkeit sicherstellen wird.

(3) Die für die Tätigkeit als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes und der Entscheidung der Kommission 2000/709/EG vom 6. November 2000 (ABl. EG Nr. L 289 S. 42) über die Mindestkriterien gemäß Artikel 3 Abs. 4 der Richtlinie 1999/93/EG erforderliche

1. Zuverlässigkeit besitzt, wer auf Grund seiner persönlichen Eigenschaften, seines Verhaltens und seiner Fähigkeiten zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist,
2. Unabhängigkeit besitzt, wer keinem wirtschaftlichen, finanziellen oder sonstigen Druck unterliegt, der sein Urteil beeinflussen oder das Vertrauen in die unparteiische Aufgabenwahrnehmung in Frage stellen kann,
3. Fachkunde besitzt, wer auf Grund seiner Ausbildung, beruflichen Bildung und praktischen Erfahrung zur ordnungsgemäßen Erfüllung der ihm obliegenden Aufgaben geeignet ist.

(4) Der Betreiber einer Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 des Signaturgesetzes hat sich von der Zuverlässigkeit und Fachkunde von Personen, die an der Prüfung oder Bestätigung mitwirken, auf geeignete Weise zu überzeugen. Er kann von diesen Personen die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen.

(5) Die zuständige Behörde veröffentlicht im Bundesanzeiger die Einzelheiten zu den Anforderungen nach den Absätzen 1 bis 4 und den Mindestkriterien nach Artikel 3 Abs. 4 der Richtlinie 1999/93/EG.

SigV 2001 § 17 Zeitraum und Verfahren zur langfristigen Datensicherung

Daten mit einer qualifizierten elektronischen Signatur sind nach § 6 Abs. 1 Satz 2 des Signaturgesetzes neu zu signieren, wenn diese für längere Zeit in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter als geeignet beurteilt sind. In diesem Falle sind die Daten vor dem Zeitpunkt des Ablaufs der Eignung der Algorithmen oder der zugehörigen Parameter mit einer neuen qualifizierten elektronischen Signatur zu versehen. Diese muss mit geeigneten neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere Signaturen einschließen und einen qualifizierten Zeitstempel tragen.

SigV 2001 § 18 Verfahren zur Feststellung der gleichwertigen Sicherheit von von ausländischen elektronischen Signaturen und Produkten

(1) Ein Zertifizierungsdiensteanbieter, der nach § 23 Abs. 1 Satz 2 Nr. 2 des Signaturgesetzes für qualifizierte Zertifikate mit Rechtswirkung nach Artikel 5 Abs. 1 der Richtlinie 1999/93/EG eines außerhalb des Europäischen Wirtschaftsraumes (Drittstaat) niedergelassenen Zertifizierungsdiensteanbieters einsteht, hat dies der zuständigen Behörde spätestens zu dem Zeitpunkt, zu dem diese Zertifikate im

Geltungsbereich des Signaturgesetzes rechtswirksam werden sollen, schriftlich oder mittels eines mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehenen elektronischen Dokuments anzuzeigen. Er hat dafür Sorge zu tragen, dass die qualifizierten Zertifikate des ausländischen Zertifizierungsdiensteanbieters und die darauf basierenden qualifizierten elektronischen Signaturen die Anforderungen des Signaturgesetzes und dieser Verordnung erfüllen und zu dem ausländischen Zertifizierungsdiensteanbieter die Unterlagen entsprechend § 1 Abs. 2 vorzulegen. § 2 gilt für die Angaben zu dem ausländischen Zertifizierungsdiensteanbieter entsprechend. Die zuständige Behörde hat den Namen des ausländischen Zertifizierungsdiensteanbieters unter Angabe des Zertifizierungsdiensteanbieters, der für seine qualifizierten Zertifikate eintritt, nach § 19 Abs. 6 des Signaturgesetzes abrufbar zu halten.

(2) Die gleichwertige Sicherheit ausländischer elektronischer Signaturen nach § 23 Abs. 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde festgestellt hat, dass

1. die Sicherheitsanforderungen an Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen,
2. die Prüfungsmodalitäten für Zertifizierungsdiensteanbieter und Produkte für qualifizierte elektronische Signaturen sowie die Anforderungen an die Prüf- und Bestätigungsstellen und
3. das Akkreditierungs- und Aufsichtssystem

eine gleichwertige Sicherheit bieten. Zur Feststellung der gleichwertigen Sicherheit kann die zuständige Behörde mit der zuständigen ausländischen Stelle die Verfahren zur Anerkennung vereinbaren, soweit nicht entsprechende überstaatliche oder zwischenstaatliche Vereinbarungen getroffen sind.

(3) Die Gleichwertigkeit von Produkten nach § 23 Abs. 3 Satz 2 des Signaturgesetzes ist gegeben, wenn die zuständige Behörde diese nach entsprechender Anwendung der Vorgaben nach Absatz 2 festgestellt hat.

(4) Die zuständige Behörde hat in ihr Verzeichnis nach § 16 Abs. 2 des Signaturgesetzes auch die qualifizierten Zertifikate für Signaturprüfschlüssel oberster ausländischer Zertifizierungsdiensteanbieter, die nach § 23 Abs. 2 des Signaturgesetzes als gleichwertig anerkannt sind, aufzunehmen. Sie hat die Anerkennung durch eine qualifizierte elektronische Signatur mit Anbieterakkreditierung nach § 15 des Signaturgesetzes zu bestätigen.

SigV 2001 § 19 Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft; ...

SigV 2001 Anlage 1 (zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2) Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen

< Fundstelle des Originaltextes: BGBl. I 2001, 3081 - 3082 >

I. Zu § 11 Abs. 3 dieser Verordnung und nach § 15 Abs. 7 des Signaturgesetzes (freiwillige Akkreditierung)

1. Prüfvorgaben

1.1 Anforderungen an Prüftiefen

Die Prüfung der Produkte für qualifizierte elektronische Signaturen nach Maßgabe des § 15 Abs. 7 und des § 17 Abs. 4 des Signaturgesetzes hat nach den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (Common Criteria for Information Technology Security Evaluation, BAnz. 1999 S. 1945, - ISO/IEC 15408) oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC - GMBl vom 8. August 1992, S. 545) in der jeweils geltenden Fassung zu erfolgen.

Die Prüfung muss

a) bei technischen Komponenten nach § 2 Nr. 12 Buchstabe a des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,

b) bei sicheren Signaturerstellungseinheiten nach § 2 Nr. 10 des Signaturgesetzes mindestens die Prüftiefe EAL 4 oder E 3 umfassen,

c) i) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die außerhalb eines besonders gesicherten Bereichs ("Trustcenter") eingesetzt werden, mindestens die Prüfstufe "EAL 4" oder "E3" umfassen,

ii) bei technischen Komponenten für Zertifizierungsdienste nach § 2 Nr. 12 Buchstabe b und c des Signaturgesetzes, die innerhalb eines besonders gesicherten Bereichs eingesetzt werden, mindestens die Prüfstufe "EAL 3" oder "E 2" umfassen,

d) bei Signaturanwendungskomponenten nach § 2 Nr. 11 des Signaturgesetzes mindestens die Prüfstufe "EAL 3" oder "E 2" umfassen.

1.2 Anforderungen an Schwachstellenbewertung/Mechanismenstärke

Bei den Prüfstufen "EAL 4" und bei "EAL 3" gemäß Abschnitt I Nr. 1.1 Buchstabe a bis c i) und Buchstabe d ist ergänzend zu den bei dieser Prüfstufe vorgeschriebenen Maßnahmen gegen ein hohes Angriffspotenzial zu prüfen und eine vollständige Missbrauchsanalyse durchzuführen.

Die Stärke der Sicherheitsmechanismen muss bei allen Produkten gemäß Abschnitt I Nr. 1.1 Buchstabe a bis d im Fall "E 3" und "E 2" mit "hoch" bewertet werden.

Abweichend hiervon genügt für den Mechanismus zur Identifikation durch biometrische Merkmale eine Bewertung der Sicherheitsmechanismen mit "mittel", wenn diese zusätzlich zur Identifikation durch Wissensdaten genutzt werden.

1.3 Anforderungen an Algorithmen

Die Algorithmen und zugehörigen Parameter müssen nach Abschnitt I Nr. 1.2 dieser Anlage als geeignet beurteilt sein.

2. Algorithmen - Veröffentlichung und Neubestimmung der Eignung

Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraumes nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von qualifizierten elektronischen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

3. Sicherheitsbestätigungen für Signaturprodukte

In der Bestätigung der Erfüllung der Anforderungen für Produkte für qualifizierte elektronische Signaturen ist anzugeben,

a) für welche Anforderungen nach § 17 des Signaturgesetzes und nach § 15 dieser Verordnung die Bestätigung gilt und unter welchen Einsatzbedingungen,

b) welche Algorithmen und zugehörigen Parameter nach Abschnitt I Nr. 2 eingesetzt und bis zu welchem Zeitpunkt diese mindestens geeignet sind sowie

c) nach welcher Stufe die Produkte geprüft wurden und welche Mechanismenstärke erreicht wurde.

Eine Ausfertigung des Prüfberichtes, der Bewertung durch die

Bestätigungsstelle und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Auf Anforderung sind dieser auch alle weiteren Prüfunterlagen vorzulegen. Sie kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten Produkten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die Produkte gemäß dieser Anlage geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen. Betroffene Hersteller, Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren. Wird diese nicht gewährt oder stellt sich heraus, dass bestätigte Produkte nicht ausreichend geprüft wurden oder Anforderungen nicht erfüllen, so kann die zuständige Behörde erteilte Bestätigungen für ungültig erklären.

4. Veröffentlichung der Sicherheitsbestätigung für Produkte
Die zuständige Behörde hat Produkte für qualifizierte elektronische Signaturen, die von einer nach § 18 des Signaturgesetzes anerkannten Stelle eine Bestätigung gemäß Abschnitt I Nr. 3 erhalten haben, im Bundesanzeiger zu veröffentlichen. Dabei ist anzugeben, bis zu welchem Zeitpunkt die Bestätigung mindestens gilt. Wird eine Bestätigung für ungültig erklärt, so hat die zuständige Behörde dies unter Angabe des Zeitpunktes, ab dem diese Maßnahme gilt, ebenfalls im Bundesanzeiger zu veröffentlichen.

II. Zu § 15 Abs. 5 dieser Verordnung und nach § 17 Abs. 1 und 3 Nr. 1 des Signaturgesetzes (nach § 4 Abs. 3 des Signaturgesetzes angezeigte Zertifizierungsdiensteanbieter ohne freiwillige Akkreditierung)
Für die Prüfung von Produkten nach § 15 Abs. 5 gelten die Anforderungen nach Abschnitt I entsprechend.
Abweichend hiervon können

- Produkte zum Einsatz kommen, die den Normen nach § 15 Abs. 6 entsprechen,
- Produkte nach § 17 Abs. 2 und 3 Nr. 2 und 3 des Signaturgesetzes (bzw. nach Abschnitt I Nr. 1.1 Buchstabe c und d) zum Einsatz kommen, bei denen anstelle der Bestätigung eine Herstellererklärung nach § 17 Abs. 4 des Signaturgesetzes vorliegt.

SigV 2001 Anlage 2 (zu § 12) Kosten

< Fundstelle des Originaltextes: BGBl. I 2001, 3083 - 3084 >

Kosten für Amtshandlungen nach § 22 Abs. 1 des Signaturgesetzes

1.1 Kosten nach § 22 Abs. 1 Nr. 1 des Signaturgesetzes

Kostennummer	Amtshandlung	Euro
1	Prüfung und Erteilung einer Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes	Gebühr nach Zeitaufwand
2	Ablehnung eines Antrages auf Akkreditierung nach § 15 Abs. 4 des Signaturgesetzes oder Rücknahme oder Widerruf einer Akkreditierung nach § 15 Abs. 5 des Signaturgesetzes	Gebühr nach Zeitaufwand
3	Vollständige oder teilweise Zurückweisung eines Widerspruchs im Rahmen des Verfahrens nach § 15 Abs. 1 bis 6 des Signaturgesetzes	2.500

4	Überprüfung von Prüfberichten und Bestätigungen nach § 15 Abs. 2 des Signaturgesetzes	3.500
5	Maßnahmen im Falle des Widerrufs oder der Rücknahme einer Akkreditierung oder im Falle der Einstellung der Tätigkeit eines akkreditierten Zertifizierungsdienste-anbieters nach § 15 Abs. 6 des Signaturgesetzes	Gebühr nach Zeitaufwand
6	Prüfungen und andere Maßnahmen nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand

1.2 Kosten nach § 22 Abs. 1 Nr. 2 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
7	Ausstellung eines qualifizierten Zertifikates sowie dessen Sperrung nach nach § 16 Abs. 1 des Signaturgesetzes	500
8	Ausstellung einer Bescheinigung nach § 16 Abs. 3 des Signaturgesetzes	500

1.3 Kosten nach § 22 Abs. 1 Nr. 3 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
	Erteilung einer Anerkennung als Bestätigungsstelle oder Prüf- und Bestätigungsstelle nach § 18 Abs. 1 des Signaturgesetzes nach	
9	a) § 15 Abs. 2 des Signaturgesetzes	2.500
10	b) § 15 Abs. 7 des Signaturgesetzes	2.500
11	c) § 17 Abs. 3 des Signaturgesetzes	1.000
	Ablehnung eines Antrages auf Anerkennung oder Rücknahme oder Widerruf einer Anerkennung für Tätigkeiten nach	
12	a) § 15 Abs. 2 des Signaturgesetzes	2.500
13	b) § 15 Abs. 7 des Signaturgesetzes	2.500
14	c) § 17 Abs. 4 des Signaturgesetzes	1.000
15	Vollständige oder teilweise Zurückweisung eines Widerrufs im Rahmen des Verfahrens nach § 18 Abs. 1 des Signaturgesetzes	1.000

1.4 Kosten nach § 22 Abs. 1 Nr. 4 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
16	Bearbeitung einer Anzeige nach § 4 Abs. 2 und 3 des Signaturgesetzes und erstmalige Überprüfung der Einhaltung des Signatur-gesetzes und dieser Verordnung nach § 19 des Signaturgesetzes	Gebühr nach Zeitaufwand
17	Stichprobenartige Prüfungen im Rahmen der Aufsicht nach § 19 Abs. 1 des Signatur-gesetzes im Falle der Feststellung eines Verstoßes gegen die für den Betrieb eines Zertifizierungsdienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand
18	Anlassbezogene Prüfungen und andere Maßnahmen nach § 19 Abs. 1 des Signatur-gesetzes im Falle eines Verstoßes gegen die für den Betrieb eines Zertifizierungs-dienstes maßgeblichen Vorschriften des Signaturgesetzes oder dieser Verordnung	Gebühr nach Zeitaufwand

1.5 Kosten nach § 23 Abs. 1 des Signaturgesetzes

Kosten-nummer	Amtshandlung	Euro
19	Bearbeitung einer Anzeige nach § 18 Abs. 1 Satz 1 dieser Verordnung einschließlich der Aufnahme in das Zertifikatsverzeichnis nach § 18 Abs. 1 Satz 4 dieser Verordnung	Gebühr nach Zeitaufwand

2. Stundensätze und Km-Pauschale für Kfz-Einsatz

Kosten-nummer	Amtshandlung	Euro
20	Beamte des höheren Dienstes oder vergleichbare Angestellte	125
21	Beamte des gehobenen Dienstes oder vergleichbare Angestellte	95
22	Beamte des mittleren Dienstes oder vergleichbare Angestellte	69
23	Kraftfahrzeugeinsatz	0,70 Euro/km

Stand: 12.12.2006 **Herausgeber: Prof. Dr. Maximilian Herberger**

Oberlandesgericht Karlsruhe
Beschluss vom 10.01.2005

1 Ws 152/04

Strafbarkeit des Ausfilterns von E-Mail

JurPC Web-Dok. 52/2005, Abs. 1 - 33

StGB: § 206 Abs.2 Nr. 2; StPO: §§ 172, 152 Abs. 2, 160; PostG: §§ 39 Abs. 2 und Abs. 3; TKG: §§ 88 Abs. 2 und Abs. 3, 85

Leitsätze

1. Im Klageerzwingungsverfahren kann die Staatsanwaltschaft durch eine gerichtliche Entscheidung zur Aufnahme von Ermittlungen aufgefordert werden, wenn sie eine Strafbarkeit aus unzutreffenden rechtlichen Gründen verneint (Fortführung von Senat, Die Justiz 2003, 270 ff.).
2. a. Der Begriff des Unternehmens i.S.v. § 206 StGB ist weit auszulegen. Hierunter ist jede Betätigung im geschäftlichen Verkehr anzusehen, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist.
   b. Stellt eine Hochschule ihre Telekommunikationseinrichtungen zur Versendung und Empfang elektronischer Post (E-mail) ihren Mitarbeitern und anderen Nutzergruppen auch für private und wirtschaftliche Zwecke zur Verfügung, so wird sie damit außerhalb ihres hoheitlichen Aufgabengebietes tätig und ist als Unternehmen i.S.v. § 206 StGB anzusehen.
3. a. Dem Tatbestandsmerkmal "unbefugt" kommt in § 206 StGB eine Doppelfunktion zu. Ein Einverständnis schließt bereits die Tatbestandsmäßigkeit des § 206 StGB aus, im übrigen handelt es sich um ein allgemeines Rechtswidrigkeitsmerkmal.
   b. Als Rechtfertigungsgründe für Eingriffe in das Post- und Fernmeldegeheimnis kommen Erlaubnissätze in Betracht, die in einer gesetzlichen Vorschrift, d.h. in einem formellen Gesetz oder einer Rechtsverordnung niedergelegt sind, und die sich ausdrücklich auf Postsendungen, den Postverkehr oder Telekommunikationsvorgänge beziehen. Auch ein Rückgriff auf allgemeine Rechtfertigungsgründe ist möglich, so dass das technische Herausfiltern einer E-Mail gerechtfertigt sein kann, wenn ansonsten Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten können.

I.

Mit Schreiben vom 28.12.2003 erstattete der Antragsteller C. bei der Staatsanwaltschaft Strafanzeige gegen die Angehörigen der Hochschule H. nämlich X., Y. und Z. wegen des Verdachts der Verletzung des Post- und Fernmeldegeheimnisses, der Datenveränderung und der Störung von Telekommunikationsanlagen. Zur Begründung führte er aus, dass er vom 01.03.1994 bis 30.06.1998 wissenschaftlicher Mitarbeiter an der Hochschule H. gewesen sein. Eine von ihm im Herbst 1999 eingereichte Arbeit sei abgelehnt worden. Seine hiergegen eingereichte Klage vor dem Verwaltungsgericht sei erfolgreich gewesen. Die Hochschule H. habe vor dem Verwaltungsgerichtshof die Rücknahme des Prüfungsbescheides erklärt, um einer Verurteilung zu entgehen. Auch gegen den erneuten Prüfungsbescheid habe er Klage eingereicht. JurPC Web-Dok. 52/2005, Abs. 1

Mit Schreiben vom 24.10.2003 sei ihm von X. mitgeteilt worden, dass er ihm aus gegebenem Abs. 2

Anlass das Privileg entziehe, die Kommunikationseinrichtungen der Fakultät einschließlich E-Post zu benutzen. Der Antragsteller trägt vor, dass es keinen konkreten Anlass für das Verbot gegeben habe. Nachdem er das Schreiben am 29.10.2004 erhalten habe, habe er noch am selben Abend eine E-Mail an den X. gesandt und darauf hingewiesen, dass er keinerlei Anlass gegeben oder Angriff unternommen habe, und dass man ihm wohl fälschlicherweise einen Angriff anderer unterstelle. Am nächsten Morgen habe er in seinem Posteingang eine Fehlermeldung des Mailservers des Vereins gefunden, über den er seine E-Mails ausliefere. Der Server habe mitgeteilt, dass er die Mail noch nicht habe zustellen können. Er habe festgestellt, dass zumindest einer der beiden Mail-Server der Fakultät die Annahme von E-Mails an diesem Abend dauerhaft und wegen Überlastung! verweigert habe. Auf telefonische Nachfrage nach dem Grund für die Sperre habe ihm X. erklärt, dass es keinen Anlass gebe, und dass man auch nicht angegriffen worden sei, dass man ihn aber für gefährlich halte und als Bedrohung ansehe.

Nach dem Gespräch habe der Antragsteller festgestellt, dass sämtlicher Internet-Verkehr vom Vereinsrechner in das Fakultätsnetz gesperrt worden sei. Er habe daraufhin seinen Privatrechner so umgestellt, dass seine E-Mails nicht mehr den Umweg über den Vereinsrechner genommen hätten, sondern direkt über das Internet ausgeliefert worden seien. Da nur der Vereinsrechner, nicht aber sein Privatrechner gesperrt worden sei, sei die Mail-Auslieferung zunächst wieder normal verlaufen. Er habe trotzdem Widerspruch gegen die Sperrung erhoben. Abs. 3

Am übernächsten Tag sei der E-Mail-Verkehr nicht mehr möglich gewesen, weil eine zweite Maßnahme ergriffen worden sei, die Gegenstand der Strafanzeige sei. Abs. 4

Der Antragsteller trägt hierzu vor, dass er nun festgestellt habe, dass er mit Dozenten, anderen Wissenschaftlern und Freunden an der Fakultät nicht mehr per E-Mail habe kommunizieren können. Zum einen seien sämtliche E-Mails gesperrt worden, in deren Absenderadresse sein Name vorgekommen sei, und zwar auch dann, wenn die E-Mails von anderen Accounts gekommen seien. Im Gegensatz zu der Sperrung des Vereinsservers sei jedoch nicht schon der Verbindungsaufbau gesperrt gewesen. Die E-Mails seien ordnungsgemäß angenommen, quittiert und in den Verantwortungsbereich der Fakultätssysteme übernommen worden. Erst einige Minuten später seien sie fakultätsintern ausgefiltert worden. Der Antragsteller habe verzögert die Meldung "delivery cancelled" erhalten. Der potentielle Empfänger habe von der Nachricht gar nichts erhalten. Zum anderen habe die Sperrung aber auch solche E-Mails betroffen, die von Mitarbeitern der Fakult&aum! l;t an den Antragsteller gesendet worden seien, d.h. bei denen der Antragsteller Empfänger gewesen, auf dem Verteiler gestanden oder nur im Betreff erwähnt worden sei, d.h. in deren Kopfzeile "C" vorgekommen sei. Hiervon seien sämtliche Mitarbeiter der Fakultät betroffen gewesen, ohne vorher befragt oder informiert worden zu sein. Abs. 5

II.

Mit Verfügung vom 16.01.2004 hat die Staatsanwaltschaft von der Einleitung eines Ermittlungsverfahrens aus rechtlichen Gründen abgesehen (§ 152 Abs.2 StPO). Sie vertrat die Ansicht, dass es den Beschuldigten freistehe, die Zusendung unerwünschter E-Mails zu blockieren. Abs. 6

Der hiergegen fristgerecht eingelegten Beschwerde hat die Generalstaatsanwaltschaft mit Bescheid vom 11.03.2004 keine Folge gegeben. Zur Begründung wurde ausgeführt, dass auch im Ausfiltern bzw. anderweitigen technischen "Sperren" eingehender E-Mails grundsätzlich ein Unterdrücken i.S. von § 206 Abs. 2 Nr. 2 StGB liegen könne. Auch könne es unter Zugrundelegung des Schutzzwecks der Norm rechtlich nicht ohne weiteres im Belieben des Trägers der jeweiligen Institution oder des Eigentümers der betreffenden EDV-Anlage stehen, unliebsamen E-Mail-Verkehr zwischen Angehörigen/Mitarbeitern untereinander oder mit Außenstehenden ohne deren Kenntnis bzw. Zustimmung technisch zu unterbinden. Die Hochschule H. sei aber kein Unternehmen i.S. der genannten Vorschrift. Der Gesetzgeber habe bei Schaffung der Norm erwerbswirtschaftlich betätigende Organisationsformen im Auge gehabt, nicht aber Behörden und andere hoheitlich han! delnde Zweige. Die Hochschule H. handle in erster Linie hoheitlich in Erfüllung eines entsprechenden gesetzlichen Auftrags, weshalb sie nicht unter den Unternehmensbegriff des § 206 StGB zu subsumieren sei. Auch die Tatbestände des § 303 a und § 317 StGB seien nicht erfüllt. Abs. 7

Mit Rechtsanwaltsschriftsatz vom 15.04.2004 hat der Antragsteller C. beantragt, die Erhebung der öffentliche Klage wegen Verletzung des Post- und Fernmeldegeheimnisses anzuordnen. Abs. 8

III.

Der rechtzeitig und in der vorgeschriebenen Form des § 172 Abs. 3 StPO angebrachte Antrag auf gerichtliche Entscheidung ist zulässig, soweit er sich gegen X. richtet. Abs. 9

1. Der Antragsteller ist Verletzter i.S.d. § 172 Abs. 1 StPO. Das Rechtsgut der Vorschrift des § 206 StGB ist durch unterschiedliche Aspekte gekennzeichnet. Einerseits wird das Vertrauen der Allgemeinheit in die Sicherheit und Zuverlässigkeit des Post- und Telekommunikationsverkehrs geschützt, andererseits geht es aber auch um den Schutz des Individualrechtsguts, nämlich den Schutz des Interesses der im Einzelfall am Post- und Fernmeldeverkehr Beteiligten. Abs. 10

2. Der Zulässigkeit des Antrags steht nicht entgegen, dass das Gesetz in § 172 StPO die Statthaftigkeit des Klageerzwingungsverfahrens an sich nur für den Fall vorsieht, dass die Staatsanwaltschaft überhaupt Ermittlungen aufgenommen und das Verfahren sodann mangels Abs. 11

genügendem Anlass zur Erhebung der öffentlichen Klage gemäß § 170 Abs. 2 StPO eingestellt hat. Der nicht ausdrücklich geregelte Fall, dass die Ermittlungsbehörde überhaupt von der Einleitung eines Ermittlungsverfahrens absieht, weil nach ihrer Ansicht hierfür keine zureichenden tatsächlichen Anhaltspunkte vorliegen, kann nicht anders behandelt werden. Denn für die rechtliche Bewertung macht es keinen Unterschied, ob die Staatsanwaltschaft formell Ermittlungen durchführt oder diese ablehnt, weil in beiden Fällen die Beachtung des Legalitätsprinzips in Frage steht (OLG Karlsruhe, Die Justiz 2003, 270 ff).

IV.

1. Der Antrag ist auch begründet, weil die Staatsanwaltschaft zu Unrecht von der Einleitung eines Ermittlungsverfahrens wegen des Verdachts der Verletzung des Post- und Fernmeldgeheimnisses abgesehen hat. Er führt zum Auftrag, die Ermittlungen wegen des Verdachts der Verletzung des Post- und Fernmeldegeheimnisses (§ 206 Abs. 2 Nr.2 StGB) gegen X. aufzunehmen. Abs. 12

2. Der Senat hält eine solche Verpflichtung der Staatsanwaltschaft ausnahmsweise dann für zulässig, wenn diese aus Rechtsgründen einen Anfangsverdacht verneint und deshalb jede tatsächliche Aufklärung des Sachverhalts unterlassen hat. Die Vorschrift des § 173 Abs. 3 StPO, wonach der Senat zur Vorbereitung seiner Entscheidung die Durchführung von Ermittlungen anordnen und damit einen beauftragten oder ersuchten Richter beauftragen kann, erfasst nur diejenigen Fälle, in welchen bereits ein weitgehend aufgeklärter Sachverhalt vorliegt, der lediglich in einzelnen Punkten näherer Vertiefung bedarf (Meyer-Goßner, StPO, 47 Auflage 2004, § 173 Rn. 3). Abs. 13

3. Auch besteht vorliegend - ein aus Rechtsgründen nicht ausgeschlossener - Anfangsverdacht einer Verletzung des Post- und Fernmeldegeheimnisses. Abs. 14

a. Aus dem Vortrag des Antragsstellers ergibt sich zunächst der durch Beweisumstände belegte Verdacht, dass ihm X. mit Schreiben vom 24.10.2003 mitgeteilt hat, dass er ihm das Privileg entzieht, die Kommunikationseinrichtungen der Fakultät einschließlich E-Post zu benutzen und in der Folgezeit veranlasst hat, dass auf den E-Mail Systemen der Fakultät jede E-Mail gesperrt wurde, in deren Kopfzeile "C" vorkam, mit der Folge, dass einerseits die E-Mails des Antragstellers den Empfänger nicht mehr erreichten, andererseits aber auch solche E-Mails, die von Mitarbeitern der Fakultät an den Antragsteller gerichtet waren, bei denen er also der Empfänger war, nicht ankamen. E-Mails des Antragstellers wurden zwar noch ordnungsgemäß vom Mail-Server der Fakultät angenommen, dann allerdings fakultätsintern ausgefiltert, so dass sie den Empfänger nicht erreichten, der hiervon auch keine Nachricht erhielt. Lediglich d! er Antragsteller erhielt verzögert die Meldung "delivery cancelled". Zum anderen betraf die Sperrung aber auch solche E-Mails, die von Mitarbeitern der Fakultät an den Anzeigeerstatter gesendet wurden, d.h. bei denen der Antragsteller Empfänger war, auf dem Verteiler stand oder nur im Betreff erwähnt wurde, d.h. in deren Kopfzeile "C" vorkam. Hiervon waren sämtliche Mitarbeiter der Fakultät betroffen, ohne vorher befragt oder informiert worden zu sein. Abs. 15

b. Entgegen der Ansicht der Ermittlungsbehörden scheitert eine Verfolgung aus Rechtsgründen nicht daran, dass die vom Anzeigeerstatter behauptete Unterdrückung seiner E-Mails deswegen nicht strafbar sei, weil die Hochschule kein Unternehmen i.S.v. § 206 StGB sei. Abs. 16

Nach § 206 Abs. 2 Nr.2 StGB macht sich strafbar, wer als Beschäftigter oder Inhaber eines Unternehmens, - das geschäftsmäßig Post- oder Telekommunikationsdienst erbringt -, unbefugt eine einem solchen Unternehmen anvertraute Sendung unterdrückt. Abs. 17

Die Generalstaatsanwaltschaft führt zutreffend aus, dass der Tatbestand des geschäftsmäßigen Erbringens von Telekommunikationsdienstleistungen lediglich das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte verlangt; auf eine Gewinnerzielungsabsicht kommt es hierbei nicht an. Soweit die Generalstaatsanwaltschaft die Ablehnung einer Strafbarkeit im vorliegenden Fall damit begründet, dass die Hochschule H. kein Unternehmen i.S.v. § 206 StGB sei, da der Gesetzgeber bei Schaffung der Norm erwerbswirtschaftlich betätigende Organisationsformen im Auge gehabt habe, nicht aber Behörden und andere hoheitlich handelnde Zweige, trägt dies im vorliegenden Fall nicht. Es ist zwar richtig, dass grundsätzlich Behörden und andere hoheitlich handelnde Zweige, zu denen auch die Hochschule H. als Körperschaft des öffentlichen Rechts zählt, dann, wenn sie a! usschließlich zur Erfüllung ihrer hoheitlichen Aufgaben tätig werden, nicht als Unternehmen i.S.v. § 206 StGB anzusehen sind. Betätigt sich aber eine Hochschule nicht ausschließlich hoheitlich, sondern stellt ihre Telekommunikationsanlage unterschiedlichen Nutzergruppen (Mitarbeitern der Hochschule, Vereinen, außenstehenden Dritten) zur Verfügung, so ist eine Abgrenzung zwischen dienstlichen, wissenschaftlichen und Studienzwecken, privaten und auch wirtschaftlichen Zwecken nicht mehr möglich. Dadurch aber wird die Hochschule auch außerhalb ihres hoheitlichen Aufgabengebietes tätig und nimmt wie jeder beliebige Dritte am geschäftlichen Verkehr teil, so dass für diesen Betätigungsbereich auch die Maßstäbe gelten müssen, wie für jedermann, der auf diesem Gebiet geschäftlich tätig wird. Abs. 18

Der Begriff des Unternehmens i.S.v. § 206 StGB ist weit auszulegen, denn nur dann kann dem Zweck gerecht werden, das subjektive Recht auf Geheimhaltung des Inhalts und der näheren Umstände des Postverkehrs oder der Telekommunikation und - wie vorliegend - den Anspruch auf Übermittlung der Sendung zu schützen. Der Begriff des Unternehmens ist wegen der Anknüpfung an §§ 39 Abs. 2 Post G, 88 Abs. 2 TKG n.F. im Kontext des PostG und TKG auszulegen. Ausgehend davon ist als Unternehmen jede Betätigung im geschäftlichen Verkehr anzusehen, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist. Übertragen auf die Hochschule H. bedeutet dies, dass sie dann, wenn sie nicht ausschließlich hoheitlich tätig wird, Abs. 19

als Unternehmen i.S. v. § 206 StGB einzustufen ist.

Nach dem Vortrag des Anzeigerstatters gestattet die Hochschule nicht nur ihren Mitarbeitern die Nutzung von Internet und elektronischer Post, sondern darüber hinaus sind verschiedene Vereine an den Server der Hochschule angeschlossen und können das System nutzen. Zudem aber können auch außerhalb der Hochschule stehende Personen das System nutzen, um mit den Mitarbeitern der Hochschule - Verwaltungspersonal, wissenschaftlichen Mitarbeitern und Studierenden - per E-Mail zu kommunizieren, und zwar nicht nur zu wissenschaftlichen oder dienstlichen Zwecken, sondern auch zu privaten, aber auch in Bereichen, in denen die Hochschule nicht hoheitlich, sondern wirtschaftlich orientiert tätig wird. Zu denken ist hierbei an die vielfältigen Verflechtungen und wirtschaftlichen Interessen einer Hochschule und einzelner Mitarbeiter mit privaten Unternehmen und damit in Zusammenhang stehenden Tätigkeiten. Die Hochschule wird in diesem Bereich quasi wie ei! n Wirtschaftsunternehmen tätig und beschränkt sich hier gerade nicht auf ihre hoheitlichen Funktionen. Stellt die Hochschule ihre Telekommunikationsanlage aber verschiedenen Nutzergruppen zu deren vielfältigen Zwecken und unterschiedlichen Interessen zur Verfügung, so gestattet sie damit die Nutzung der Telekommunikationsanlage zu Zwecken, die nicht im unmittelbaren oder nur mittelbaren Zusammenhang mit ihren hoheitlichen Aufgaben stehen und wird dadurch auch außerhalb ihres hoheitlichen Aufgabengebietes tätig; dann aber kann sie sich nicht mehr auf ihre hoheitliche Stellung zurückziehen, sondern unterliegt dem Unternehmensbegriff i.S.v. § 206 StGB (siehe Münchner Kommentar, 2003, § 206 StGB, Rn. 13; Erbs-Kohlhaas, Telekommunikationsgesetz § 85 a. F. Rn. 8; Schönke-Schröder, 26. Auflage, § 206 Rn. 8; a. M. Tröndle-Fischer, 52. Auflage, § 206 StGB, Rn. 2b). Abs. 20

c. Die Sendung muss dem Unternehmen "zur Übermittlung anvertraut" sein. Der Begriff Sendung i.S.v. § 206 Abs. 2 Nr. 2 StGB erstreckt sich auch auf unkörperliche Gegenstände, da § 206 Abs. 2 Nr. 2 StGB nicht - wie § 206 Abs. 2 Nr.1 StGB - auf verschlossene Sendungen beschränkt ist. Tatobjekte des § 206 Abs. 2 Nr. 2 StGB sind daher nicht nur unverschlossene Postsendungen, sondern auch jede Form der dem Fernmeldegeheimnis unterliegenden Telekommunikation (Münchner Kommentar, § 206, Rn. 52; Schönke-Schröder, § 206, Rn. 20). Anvertraut ist eine Sendung dann, wenn sie auf vorschriftsmäßige Weise in den Verkehr gelangt ist und sich im Gewahrsam des Unternehmens befindet. Unproblematisch liegt der Gewahrsam an einer E-Mail spätestens dann vor, wenn die Anfrage zur Übermittlung von Daten den Mail-Server des Unternehmens erreicht hat und der versendende Mailserver die Daten dem empfangenden Ser! ver übermittelt hat (Tschoepe, Rechtsprobleme der E-Mail-Filterung, MMR 2004, 75 ff, 77). Nach dem Vortrag des Anzeigerstatters war dies der Fall; die von ihm von seinem Privatrechner aus versandten E-Mails wurden ordnungsgemäß vom Mail-Server der Fakultät angenommen und quittiert, und erst dann fakultätsintern ausgefiltert. Für die E-Mails, die von Mitarbeitern der Fakultät an den Anzeigeerstatter gesandt wurden, d.h. bei denen der Anzeigeerstatter Empfänger war, gilt entsprechendes. Abs. 21

d. Ein Unterdrücken der E-Mail ist dann anzunehmen, wenn durch technische Eingriffe in den technischen Vorgang des Aussendens, Übermittelns oder Empfangens von Nachrichten mittels Telekommunikationsanlagen verhindert wird, dass die Nachricht ihr Ziel vollständig oder unverstümmelt erreicht (Schönke-Schröder, § 206, Rn. 20; Tschoepe, Rechtsprobleme der E-Mail-Filterung, MMR 2004, 75 ff., 78). Soweit auch die Auffassung vertreten wird, dass ein Unterdrücken bei einer E-Mail nicht das Zerstören oder Beschädigen der Nachricht, also ihr Löschen, Verstümmeln oder Verkürzen ist, sondern nur ihr vollständiges oder vorübergehendes Zurückhalten oder Umleiten an eine andere Adresse (Münchner-Kommentar, § 206, Rn .56), greift dies zu kurz; denn letztlich kann es keinen Unterschied machen, wie verhindert wird, dass die Nachricht ihren Empfänger erreicht, nämlich ob dies durch Zur&uum! l;ckhalten oder Umleiten der E-Mail oder durch deren Löschung oder sonstige Verstümmelung geschieht. Hierauf kommt es aber hier nicht an. Das Tatbestandsmerkmal "Unterdrücken" wird jedenfalls durch eine Ausfilterung der E-Mail erreicht. In diesem Fall findet die Weiterleitung, also das Übermitteln der eingehenden Mail vom Mailserver an den einzelnen Clienten nicht statt - dies war nach der Schilderung des Anzeigenerstatters der Fall -. Abs. 22

e. Dem Tatbestandsmerkmal "unbefugt" kommt in § 206 StGB eine Doppelfunktion zu: Ein Einverständnis schließt bereits die Tatbestandsmäßigkeit des § 206 StGB aus, im übrigen handelt es sich um ein allgemeines Rechtswidrigkeitsmerkmal. Ein Einverständnis kann aber nur dann von Bedeutung sein, wenn es von allen an dem konkreten Fernmeldeverkehr Beteiligten erteilt wird. Hier lag weder das Einverständnis des Antragstellers vor noch - nach seinem Vortrag - das Einverständnis der Mitarbeiter der Hochschule, die E-Mails herauszufiltern. Abs. 23

Als Rechtfertigungsgründe für Eingriffe in das Post- und Fernmeldegeheimnis kommen nur Erlaubnissätze in Betracht, die in einer gesetzlichen Vorschrift, d.h. in einem formellen Gesetz oder einer Rechtsverordnung niedergelegt sind, und die sich ausdrücklich auf Postsendungen, den Postverkehr oder Telekommunikationsvorgänge beziehen (§§ 39 Abs. 3 Satz 3 Post G, 88 Abs.3 Satz 3 n.F ,85 Abs. 3 Satz 3 TKG a.F). Ob daneben auch allgemeine Rechtfertigungsgründe eingreifen können, ist umstritten. Allerdings dann, wenn besondere Fallgestaltungen vorliegen, die den Rahmen der §§ 39 Abs. 3 Satz 3 Post G, 88 Abs.3 Satz 3 n.F sprengen, gelten auch die allgemeinen Rechtfertigungsgründe (Leipziger Kommentar, § 206 Rn. 54; Tröndle/Fischer, 52. Auflage, §206 Rn. 9; a.M. Münchner Kommentar, § 206, Rn. 68). Abs. 24

Unter Umständen kann es daher gerechtfertigt sein, eine E-Mail herauszufiltern, beispielsweise dann, wenn eine E-Mail mit Viren behaftet ist, so dass bei deren Verbreitung Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten. Irgendwelche dementsprechenden Anhaltspunkte aber, die zu einem Herausfiltern der E-Mails, die von Mitarbeitern der Hochschule an den Antragsteller gerichtet waren, berechtigt hätten, fehlen, so dass in diesen Fällen ein "Herausfiltern" der E-Mails unbefugt erfolgte. Abs. 25

Soweit die E-Mails, bei denen der Antragsteller Versender war, herausgefiltert wurden, wird im Rahmen der Ermittlungen zu prüfen sein, ob es einen konkreten Anlass gegeben hat, der zu einer solchen Maßnahme berechtigte. In dem Schreiben vom 24.10.2003, in dem X. dem Antragsteller Abs. 26

mitteilte, dass er ihm das Privileg entzieht, die Kommunikationseinrichtungen der Fakultät einschließlich E-Post zu benutzen, bezieht er sich auf einen "gegebenen Anlass", den der Antragsteller allerdings bestreitet. Im Rahmen der Ermittlungen wird daher aufzuklären sein, ob es einen solchen konkreten Anlass gegeben hat. Nur wenn ein solcher konkreter Anlass vorgelegen hat und davon auszugehen war, dass die E-Mails des Antragstellers eine Störung oder einen Schaden in dem Telekommunikationssystem der Hochschule hätten auslösen können, wird je nach Art und Ausmaß des möglichen Schadens zu prüfen sein, ob und welche mögliche "Abwehrmaßnahme" gerechtfertigt gewesen sein könnte.

f. Der Senat braucht nicht zu entscheiden, ob die Staatsanwaltschaft im Rahmen eines Klageerzwingungsverfahrens über die obergerichtlich anerkannten Fälle hinaus auch dann mit der Durchführung von Ermittlungen beauftragt werden kann, wenn sie nicht aus rechtlichen, sondern aus tatsächlichen Gründen einen Anfangsverdacht verneint, etwa weil sie die vorhandenen Verdachtsmomente nicht als zureichende Anhaltspunkte zur Bejahung eines Anfangsverdachts ansieht. Um einen solchen Fall handelt es sich vorliegend nicht, denn die Ermittlungsbehörde hat ohne nähere Sachaufklärung eine Strafbarkeit aus rechtlichen Gründen verneint. Sie hat damit in rechtlicher Hinsicht die Reichweite der Vorschrift des § 152 Abs.2 StPO verkürzt. Abs. 27

§ 152 Abs. 2 StPO ist Ausfluss des Legalitätsprinzips und verpflichtet die Staatsanwaltschaft immer dann zur Aufnahme von Ermittlungen, wenn nach kriminalistischer Erfahrung die Möglichkeit einer verfolgbaren Straftat besteht. Hierzu bedarf es tatsächlicher Anhaltspunkte, bloße Vermutungen genügen nicht. Ergeben sich - wie hier - zureichende tatsächliche Anhaltspunkte einer Straftat, so obliegt es der Staatsanwaltschaft und der Polizei, durch ihr Einschreiten aufzuklären, ob eine solche tatsächlich vorliegt und auf welche Weise sich deren Begehung nachweisen lässt (§ 160 StPO). Das Legalitätsprinzip gebietet es, den Ermittlungsansätzen, - soweit eine Durchbrechung aufgrund der Vorschriften der §§ 153 ff StPO nicht angezeigt erscheint -, im Rahmen der vorhanden Möglichkeiten und Ressourcen zunächst einmal nachzugehen (Senat Die Justiz 2003, 270 ff.). Abs. 28

Ob sich in Anbetracht des wenig aufgeklärten Sachverhalts vorliegend der Nachweis einer strafrechtlich erheblichen Verletzung des Post- und Fernmeldegeheimnisses wird führen lassen, lässt sich derzeit nicht beurteilen. Dies enthebt die Staatsanwaltschaft aber nicht von ihrer gesetzlichen Verpflichtung, den vom Antragsteller vorgetragenen tatsächlichen Anhaltspunkten einer Verletzung des Post- und Fernmeldegeheimnisses nachzugehen und hierzu in der gebotenen Weise unter anderem Zeugen und den namhaft gemachten Tatverdächtigen zu vernehmen. Abs. 29

IV.

Der Antrag ist, soweit er sich gegen Y. und Z. richtet, unzulässig. Abs. 30

Zu den formellen, den Rechtsweg zum Oberlandesgericht erst eröffnenden Zulässigkeitsvoraussetzungen für einen Antrag auf gerichtliche Entscheidung gehört, dass der Antrag die Tatsachen, welche die Erhebung der öffentlichen Klage begründen sollen, und die Beweismittel angeben muss. Die Rechtsprechung hat dies dahin konkretisiert, dass allein das Vorbringen in der Antragsschrift das Gericht in die Lage versetzen muss, ohne Rückgriff auf die Ermittlungsakten der Staatsanwaltschaft und in der Regel auf Anlagen, eine Schlüssigkeitsprüfung hinsichtlich der Erfolgsaussichten in formeller und materieller Hinsicht vorzunehmen (Meyer-Goßner, a.a.O., § 172 Rn. 27 m.w.N.). Abs. 31

Diesen Anforderungen genügt die Antragsschrift nicht in vollem Umfang. Aus der Darstellung des Sachverhalts in der Antragsschrift ergibt sich nicht, woraus sich eine Beteiligung des Y. an der Tat ergeben soll. Soweit der Antragsteller vorträgt, dass in dem Schreiben des X. vom 24.10.2003 im Briefkopf noch Z. aufgeführt ist und in diesem Zusammenhang behauptet, Z. könnte möglicherweise an der Tat beteiligt gewesen sein, handelt es sich um eine Vermutung des Antragstellers. Abs. 32

Eine Kostenentscheidung ist nicht veranlasst.

JurPC Web-Dok. 52/2005, Abs. 33

[*online seit: 29.04.2005*]

Zitiervorschlag: *Gericht, Datum, Aktenzeichen, JurPC Web-Dok., Abs.*

Entscheidungen

Siehe auch: **Pressemitteilung Nr. 43/05 vom 7.7.2005**

BUNDESARBEITSGERICHT Urteil vom 7.7.2005, 2 AZR 581/04

Außerordentliche Kündigung - "Surfen" im Internet

Leitsätze

Ein wichtiger Grund zur außerordentlichen Kündigung an sich kann vorliegen, wenn der Arbeitnehmer das Internet während der Arbeitszeit zu privaten Zwecken in erheblichem zeitlichen Umfang ("ausschweifend") nutzt und damit seine arbeitsvertraglichen Pflichten verletzt.

Tenor

> Auf die Revision der Beklagten wird das Urteil des Landesarbeitsgerichts Rheinland-Pfalz vom 12. Juli 2004 - 7 Sa 1243/03 - aufgehoben.
>
> Die Sache wird zur neuen Verhandlung und Entscheidung - auch über die Kosten der Revision - an das Landesarbeitsgericht zurückverwiesen.

Tatbestand

1 Die Parteien streiten über die Wirksamkeit einer außerordentlichen, hilfsweise ordentlichen Kündigung wegen unerlaubter privater Nutzung des Internets während der Arbeitszeit mit Zugriff auf pornografische Seiten.

2 Der am 28. Juni 1962 geborene, geschiedene und zwei Kindern zum Unterhalt verpflichtete Kläger ist bei der Beklagten seit dem 3. Januar 1985 beschäftigt.

3 Zuletzt arbeitete der Kläger als Chemikant und sog. Erstmann (Schichtführer) in der T-Fabrik. Nach der Arbeitsplatzbeschreibung vertritt der Erstmann bei Abwesenheit den Vorarbeiter. Zu den Aufgaben des Klägers gehört ua. die Überwachung und Kontrolle der Anlagen. Der Kläger war in vollkontinuierlicher Wechselschicht eingesetzt. Je 12-Stunden-Schicht beträgt die Pausenzeit eine Stunde, wobei die Lage der Pausen nicht festliegt.

4 Seit September 1999 befindet sich auf der Intranet-Startseite der Beklagten oben links ein rot unterlegter Hinweis “Intranet und Internet nur zum dienstlichen Gebrauch”. Wird dieser Hinweis angeklickt, erfolgt eine Warnung, dass jeder Zugriff auf Internetseiten mit pornografischem, gewaltverherrlichendem oder rassistischem Inhalt registriert und gespeichert wird und Mitarbeiter, die entsprechende Internetseiten aufrufen, mit arbeitsrechtlichen Konsequenzen rechnen müssen. Die Beklagte hatte über die Werkszeitung und den sog. Online-Reporter auf dieses Verbot hingewiesen.

5 Anfang 2002 wurde für die Mitarbeiter der T-Fabrik der Zugang zum Internet freigeschaltet. Eine Schulung für die Internetnutzung fand aus diesem Anlass nicht statt.

6 Im Oktober 2002 fielen dem Betriebsleiter der T-Fabrik die gestiegenen Internet-Nutzungskosten des Betriebs von 13,83 Euro im Juni 2002 auf über 400,00 Euro im Oktober 2002 auf. Der werkseigene Ermittlungsdienst stellte für den Zeitraum September bis November 2002 einen Zugriff auf Internetseiten mit erotischen und pornografischen Inhalten von den Schichtführer-Zimmern D 3 und D 3 fest, und zwar in Zeiten, in denen der Kläger und/oder der stellvertretende Schichtführer R. bzw. der Schichtführer C. im

Betrieb anwesend waren. Es wurde weiter festgestellt, dass die vom System automatisch angelegte Liste der im Internet angewählten Seiten gelöscht worden war.

7 Bei einer ersten Befragung durch den Ermittlungsdienst am 26. November 2002 räumte der Kläger ein, den Rechner im Schichtführer-Zimmer D 3 vor allem in den Pausenzeiten in unregelmäßigen Abständen öfter privat genutzt zu haben. Er habe im Internet gesurft und vorrangig Seiten mit erotischem Inhalt, manchmal aber auch Seiten, die man als pornografisch bezeichnen könne, aufgerufen.

8 In einer zweiten Befragung am 16. Dezember 2002 gab er auf Vorhalt an, er habe sich zeitweise per Internet kurze Videosequenzen mit pornografischem Inhalt sowie einzelne pornografische Bilder angeschaut. Auf die Seiten mit den Videosequenzen sei er mehr oder weniger zufällig gelangt, aus Neugierde habe er sich die Videos mehrmals angeschaut.

9 Der Ermittlungsdienst vermerkte in seinem Abschlussbericht vom 17. Dezember 2002, der Kläger habe nicht abgestritten, von den Anweisungen und Bestimmungen der Beklagten über die Internetnutzung gewusst zu haben.

10 Mit Schreiben vom 17. Dezember 2002 hörte die Beklagte den Betriebsrat zur beabsichtigten Kündigung des Klägers an. Mit Schreiben vom 20. Dezember 2002 erhob der Betriebsrat Bedenken gegen die beabsichtigte fristlose Kündigung und widersprach auch der hilfsweisen ordentlichen Kündigung.

11 Mit Schreiben vom 20. Dezember 2002 kündigte die Beklagte das Arbeitsverhältnis des Klägers fristlos, hilfsweise fristgemäß zum 31. März 2003.

12 Hiergegen hat sich der Kläger mit seiner Kündigungsschutzklage gewandt. Er hat die Auffassung vertreten, sein Verhalten rechtfertige ohne Abmahnung nicht die Beendigung des Arbeitsverhä ltnisses. Er habe nicht gewusst, dass der Zugang zum Internet den Mitarbeitern nur zu dienstlichen Zwecken gestattet gewesen sei. Er habe keine Kenntnis von den von der Beklagten hinterlegten Warnhinweisen auf der Intranet-Startseite gehabt. Er sei grundsätzlich über die Windows-Schaltfläche und damit über einen anderen Weg in das Internet gelangt. Hinweise, Schulungen oder andere ausdrückliche Anweisungen der Beklagten bezüglich der Internetnutzung habe es nicht gegeben. Das Internet habe er nicht umfangreich privat genutzt; er habe lediglich etwa 5 bis 5 ½ Stunden privat im Internet gesurft und dabei maximal zwischen 55 und 70 Minuten Seiten mit pornografischem Inhalt aufgerufen. Darüber hinausgehende Zeiten seien ihm nicht zuzurechnen. Der Beklagten sei durch seine private Nutzung des Internets kein finanzieller Schaden entstanden.

13 Der Kläger hat zuletzt beantragt,

1. festzustellen, dass das zwischen den Parteien bestehende Arbeitsverhältnis durch die Kündigung vom 20. Dezember 2002 nicht aufgelöst worden ist;

2. die Beklagte zu verurteilen, ihn bis zum rechtskräftigen Abschluss des Kündigungsschutzverfahrens zu unveränderten arbeitsvertraglichen Bedingungen als Chemikant weiterzubeschäftigen.

14 Die Beklagte hat zur Begründung ihres Klageabweisungsantrags vorgetragen: Es liege ein wichtiger Grund zur außerordentlichen Kündigung des Arbeitsverhältnisses vor. Der Kläger habe in einem nicht mehr tolerierbaren Ausmaß und gegen eindeutige Verbote sich Zugang zu Internetseiten mit erotischem und pornografischem Inhalt während der Arbeitszeit verschafft und damit seine arbeitsvertraglichen Pflichten in erheblichem Umfang verletzt. Der Kläger habe ohne weiteres erkennen können, dass ein exzessiver Zugriff auf das Internet verboten sei. Deshalb habe es keiner Abmahnung vor dem Ausspruch der Kündigung bedurft. Er habe in der Zeit vom 9. September 2002 bis zum 31. November 2002 insgesamt 18 Stunden und 14 Minuten vom Rechner des Schichtführerzimmers D 3 und 22 Minuten vom Rechner des Schichtführerzimmers D 3 zu privaten Zwecken auf das Internet zugegriffen. Davon entfielen 4 Stunden und 53 Minuten auf Seiten mit pornografischem Inhalt. Alle Mitarbeiter der T-Fabrik seien im Rahmen einer Schulung eines Anwendungsprogramms auf die Warnhinweise der Intranet-Startseite und das Verbot des Zugriffs auf Internetseiten mit pornografischen Inhalten durch den zuständigen EDV-Verantwortlichen ausdrücklich hingewiesen worden. Anlässlich der erstmaligen Freischaltung des Internets im Jahre 2002 sei die Internetnutzung auch allgemeines Gesprächsthema im Betrieb gewesen. Der Kläger könne nicht ernsthaft behaupten, er habe als einziger diese Diskussion nicht mitbekommen. Im Übrigen habe der Kläger mit seiner privaten Nutzung des Internets während der Arbeitszeit massiv gegen die Sicherheitsbestimmungen der Beklagten verstoßen und die ihm obliegende Aufsichtspflicht über die ihm anvertrauten Anlagen erheblich missachtet.

15 Das Arbeitsgericht hat nach Durchführung einer Beweisaufnahme der Kündigungsschutzklage des Klägers stattgegeben und die Beklagte zur vorläufigen Weiterbeschäftigung des Klägers verurteilt. Das

Landesarbeitsgericht hat die Berufung der Beklagten zurückgewiesen. Mit der vom Landesarbeitsgericht zugelassenen Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter.

Entscheidungsgründe

16 Die Revision der Beklagten ist begründet. Das Landesarbeitsgericht konnte mit der gegebenen Begründung die Berufung der Beklagten nicht zurückweisen.

17 A. Das Landesarbeitsgericht hat zur Begründung seiner der Klage stattgebenden Entscheidung im Wesentlichen ausgeführt: Es liege kein wichtiger Grund für eine außerordentliche Kündigung iSv. § 626 Abs. 1 BGB vor. Nutze der Arbeitnehmer entgegen einer einschlägigen Abmahnung oder einem ausdrücklichen Verbot des Arbeitgebers das Internet für private Zwecke, stelle dies eine die außerordentliche Kündigung rechtfertigende arbeitsvertragliche Pflichtverletzung dar. Genehmige oder dulde der Arbeitgeber eine private Nutzung des Internets, komme eine Kündigung nur ausnahmsweise in Betracht, wenn die Nutzung in einem solchen Ausmaß erfolge, dass der Arbeitnehmer nicht mehr annehmen könne, sie sei vom Einverständnis des Arbeitgebers gedeckt. Der Kläger habe vorliegend bisher weder eine Abmahnung erhalten noch habe die Beklagte nachgewiesen, dass er von der Anweisung, das Internet nur dienstlich zu nutzen, und dem Verbot, keine Seiten mit pornografischem Inhalt aufzurufen, eine positive Kenntnis gehabt habe. Auch wenn ein vernünftiger Arbeitnehmer nicht annehmen könne, ein Arbeitgeber werde Ausflüge in das Internet von bis zu 134 Minuten hinnehmen, erfordere die bestehende betriebliche Unklarheit über die berechtigte Internetnutzung und der Umstand, dass die private Internetnutzung auch während der Arbeitszeit inzwischen sozialadäquat sei, vor dem Ausspruch einer Kündigung eine eindeutige Klarstellung durch den Arbeitgeber bzw. eine vergebliche Abmahnung. Da beides nicht vorliege, sei ein wichtiger Grund zur außerordentlichen Beendigung des Arbeitsverhältnisses nicht gegeben. Ob durch die private Nutzung des Internets der Beklagten ein Schaden entstanden sei, sei angesichts der bestehenden Unklarheiten unbeachtlich. Unter Abwägung dieser Umstände sei auch die ordentliche Kündigung nicht gerechtfertigt.

18 B. Dem folgt der Senat nicht. Die Revision der Beklagten fü hrt zur Aufhebung der Berufungsentscheidung und zur Zurückverweisung des Rechtsstreits an das Landesarbeitsgericht (§ 563 Abs. 1 ZPO). Die Revision rügt zu Recht eine fehlerhafte Anwendung von § 626 Abs. 1 BGB und § 1 KSchG. Mit der bisherigen Begründung kann die Unwirksamkeit der außerordentlichen Kündigung wie auch der hilfsweise ordentlichen Kündigung nicht begründet werden.

19 I. Gemäß § 626 Abs. 1 BGB kann ein Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Da der in § 626 Abs. 1 BGB verwendete Begriff des wichtigen Grundes ein unbestimmter Rechtsbegriff ist, kann seine Anwendung durch die Tatsachengerichte im Revisionsverfahren nur darauf überprüft werden, ob das Berufungsgericht den Rechtsbegriff selbst verkannt hat, ob es bei der Unterordnung des Sachverhalts unter die Rechtsnorm Denkgesetze oder allgemeine Erfahrungssätze verletzt und ob es alle vernünftigerweise in Betracht kommenden Umstände, die für oder gegen die außerordentliche Kündigung sprechen, widerspruchsfrei beachtet hat *(st. Rspr. des Senats, vgl. beispw. 4. Juni 1997 - 2 AZR 526/96 - BAGE 86, 95; 13. April 2000 - 2 AZR 259/99 - BAGE 94, 228; 15. November 2001 - 2 AZR 605/00 - BAGE 99, 331; zuletzt: 25. März 2004 - 2 AZR 341/03 - AP BGB § 626 Nr. 189 = EzA BG 2002 § 626 Nr. 6)* . Ebenfalls ist die Prüfung, ob auf Grund des Verhältnismäßigkeitsgrundsatzes vor Ausspruch einer Kündigung eine Abmahnung erforderlich ist, weitgehend Aufgabe der Tatsacheninstanz und unterliegt nur einer eingeschränkten revisionsrechtlichen Prüfung *(vgl. beispw. zuletzt 15. November 2001 - 2 AZR 605/00 - aaO)* .

20 II. Dieser eingeschränkten Prüfung hält das Berufungsurteil nicht stand. Das Landesarbeitsgericht hat bei der Beurteilung des wichtigen Grundes nicht alle fallrelevanten Umstände berücksichtigt.

21 1. Im Ausgangspunkt zutreffend geht das Landesarbeitsgericht von einer zweistufigen Prüfung des wichtigen Grundes aus *(vgl. beispw. Senat 17. Mai 1984 - 2 AZR 3/83 - AP BGB § 626 Verdacht strafbarer Handlung Nr. 14 = EzA BGB § 626 nF Nr. 90; 2. März 1989 - 2 AZR 280/88 - AP BGB § 626 Nr. 101 = EzA BGB § 626 nF Nr. 118; 14. September 1994 - 2 AZR 164/94 - BAGE 78, 18)* . Im Rahmen von § 626 Abs. 1 BGB ist zunächst zu prüfen, ob ein bestimmter Sachverhalt ohne die besonderen Umstände des Einzelfalls als wichtiger Kündigungsgrund an sich geeignet ist. Liegt ein solcher Sachverhalt vor, bedarf es der weiteren Prüfung, ob die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Einzelfalls und unter Abwägung der Interessen beider

Vertragsteile zumutbar ist oder nicht.

22 2. Schon bei der Prüfung des wichtigen Grundes “an sich” hat das Landesarbeitsgericht nicht alle fallrelevanten Aspekte berücksichtigt.

23 a) Das Landesarbeitsgericht will einen wichtigen Grund “an sich” annehmen, wenn ein Arbeitnehmer entgegen einem ausdrücklichen Verbot oder nach einer einschlägigen Abmahnung das Internet für private Zwecke genutzt habe. Darüber hinaus kommt nach Auffassung des Landesarbeitsgerichts eine außerordentliche Kündigung bei einer privaten Nutzung des Internets nur ausnahmsweise dann in Betracht, wenn eine Nutzung in einem solchen Ausmaß erfolge, dass der Arbeitnehmer nicht annehmen könne, sie sei vom Einverständnis des Arbeitgebers gedeckt.

24 Entgegen der Auffassung des Landesarbeitsgerichts kommt eine kündigungsrelevante Verletzung der arbeitsvertraglichen Pflichten jedoch nicht nur in den von ihm skizzierten Fallgestaltungen in Betracht. Eine Verletzung der arbeitsvertraglichen Leistungspflicht sowie anderer vertraglicher Nebenpflichten kann sich auch aus anderen Umständen ergeben. Neben den vom Berufungsgericht genannten Pflichtverletzungen kommen bei einer privaten Nutzung des Internets allgemein und im vorliegenden Fall im Besonderen ua. in Betracht:

- das Herunterladen einer erheblichen Menge von Daten aus dem Internet auf betriebliche Datensysteme (“unbefugter download”), insbesondere wenn damit einerseits die Gefahr möglicher Vireninfizierungen oder anderer Störungen des - betrieblichen - Betriebssystems verbunden sein können oder andererseits von solchen Daten, bei deren Rückverfolgung es zu möglichen Rufschädigungen des Arbeitgebers kommen kann, beispielsweise weil strafbare oder pornografische Darstellungen heruntergeladen werden (*Hanau/Hoeren Private Internetnutzung durch Arbeitnehmer, S. 31; Mengel NZA 2005, 752, 753*);
- die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internetanschlusses als solche, weil durch sie dem Arbeitgeber - zusätzliche - Kosten entstehen und der Arbeitnehmer die Betriebsmittel - unberechtigterweise - in Anspruch genommen hat;
- die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internets während der Arbeitszeit, weil der Arbeitnehmer während des Surfens im Internet zu privaten Zwecken seine arbeitsvertraglich geschuldete Arbeitsleistung nicht erbringt und dadurch seine Arbeitspflicht verletzt (*Kramer NZA 2004, 457,459; Mengel NZA 2005, 752, 753*).

25 Das Landesarbeitsgericht hat sich lediglich mit dem Aspekt der privaten Nutzung des Internets an sich näher auseinander gesetzt. Eine umfassende Prüfung der weiteren Aspekte hat es unterlassen, obwohl die Beklagte hierzu - teilweise streitig - vorgetragen hat.

26 b) Das Landesarbeitsgericht hat insbesondere dem Umstand, dass der Kläger das Internet während der Arbeitszeit privat genutzt und damit seine arbeitsvertragliche Leistungspflicht verletzt hat, keine hinreichende Beachtung geschenkt.

27 Bei einer privaten Internetnutzung während der Arbeitszeit verletzt der Arbeitnehmer grundsätzlich seine (Hauptleistungs-) Pflicht zur Arbeit *(Balke/Müller DB 1997, 326; Beckschulze DB 2003, 2777, 2781; Kramer NZA 2004, 457, 461; Mengel NZA 2005, 752, 753)* . Die private Nutzung des Internets darf die Erbringung der arbeitsvertraglich geschuldeten Arbeitsleistung nicht erheblich beeinträchtigen *(Däubler Internet und Arbeitsrecht 3. Aufl. Rn. 189; Hanau/Hoeren Private Internetnutzung durch Arbeitnehmer S. 29; Kramer NZA 2004, 457, 460)* . Die Pflichtverletzung wiegt dabei um so schwerer, je mehr der Arbeitnehmer bei der privaten Nutzung des Internets seine Arbeitspflicht in zeitlicher und inhaltlicher Hinsicht vernachlässigt.

28 aa) Unstreitig ist der Kläger mehrfach seiner Arbeitspflicht nicht nachgekommen. Er hat eingeräumt, 5 bis 5 ½ Stunden privat im Internet gesurft zu haben. Er hat weiter eingeräumt, am 3. Oktober 2002 von 7.05 Uhr bis 8.32 Uhr, am 16. Oktober 2002 von 23.06 Uhr bis 1.20 Uhr, am 2. November 2002 von 11.24 Uhr bis 12.12 Uhr und am 10. November 2002 von 0.18 Uhr bis 0.38 Uhr das Internet für private Zwecke genutzt zu haben. Selbst wenn man unterstellt und zugunsten des Klägers berücksichtigt, dass er täglich eine einstündige Pause hat und zumindest der ganz überwiegende Teil der privaten Internetnutzung in seinen Pausenzeiten erfolgte, liegt zumindest am 3. Oktober 2002 und 16. Oktober 2002 ein über die - maximale tägliche - Pausenzeiten hinausgehende zeitlich ungewöhnliche umfangreiche private Nutzung des Internets vor, die mit den arbeitsvertraglichen Pflichten des Klägers zwingend nicht zu vereinbaren ist.

29

bb) Ob, wie die Beklagte behauptet, der Kläger auch an anderen Tagen und in noch weit erheblicherem

Umfange seine vertragliche Leistungspflicht verletzt hat, hat das Landesarbeitsgericht nicht festgestellt.

30 cc) Selbst unter Berücksichtigung möglicher Pausenzeiten des Klägers lässt sich im Ergebnis jedenfalls festhalten, dass der Kläger zumindest an zwei Tagen nicht nur kurzfristig und unerheblich, sondern in einem beträchtlichen zeitlichen Umfang seiner Arbeitspflicht nicht nachgekommen ist, indem er während der Arbeitszeit privat im Internet gesurft hat. Diese Arbeitsvertragspflichtverletzung wird auch nicht dadurch relativiert, dass die Beklagte dem Kläger die private Nutzung des Internets - was im Ü brigen vom Kläger zunächst näher darzulegen gewesen wäre - gestattet bzw. diese geduldet hätte. Eine solche Gestattung oder Duldung würde sich nämlich - ohne weitere Erklärungen - allenfalls auf eine private Nutzung im normalen bzw. angemessenen zeitlichen Umfang erstrecken *(Hanau/Hoeren Privat Internetnutzung durch Arbeitnehmer S. 24 und 29; Kramer NZA 2004, 457, 459)* . Etwas anderes könnte allenfalls dann gelten, wenn der Kläger in dem konkreten Zeitraum, in dem er das Internet privat genutzt hat, mangels Arbeitsanfall ohnehin untätig gewesen wäre *(siehe hierzu: Mengel NZA 2005, 752, 753)* . Dies wäre aber vom Kläger ggf. zunächst näher darzulegen gewesen.

31 dd) Weiter ist zu berücksichtigen, dass die Verletzung seiner arbeitsvertraglichen Leistungspflicht umso schwerer wiegt, als zur Tätigkeit des Klägers als Erstmann auch wesentlich eine Aufsichtsfunktion gehö rt. Er hat die Einhaltung von sicherheitsrelevanten Standards zu überwachen. Die Außerachtlassung dieser Aufsichtsfunktion an den genannten Tagen hat das Landesarbeitsgericht nicht einmal erwähnt.

32 c) Die unzureichende Berücksichtigung der verletzten Arbeitspflicht bei der Prüfung des wichtigen Grundes durfte das Landesarbeitsgericht nicht mit dem Hinweis auf eine “sozialadäquate” Nutzung des Internets zu privaten Zwecken während der Arbeitszeit herunterspielen. Zum einen ist nicht ersichtlich, woraus sich eine solche “Sozialadäquanz” ergeben soll. Zum anderen mag allenfalls eine kurzfristige private Nutzung des Internets während der Arbeitszeit allgemein gerade noch als hinnehmbar angesehen werden, wenn keine ausdrücklichen betrieblichen Verbote zur privaten Nutzung existieren. Bei einer solchen exzessiven privaten Nutzung des Internets während der Arbeitszeit wie hier lässt sich jedoch auf keinen Fall noch von einem “sozialadäquanten” Verhalten sprechen und eine arbeitsvertragliche Pflichtverletzung negieren.

33 d) Ähnliches gilt für die vom Landesarbeitsgericht angeführten Unklarheiten zur privaten Nutzungsberechtigung des Internets. Aus einer möglichen Berechtigung zur privaten Nutzung des Internets - die im Übrigen vom Landesarbeitsgericht auch nicht positiv festgestellt worden ist - folgt noch nicht, dass der Arbeitnehmer das Medium intensiv während der Arbeitszeit nutzen darf. Selbst wenn im Betrieb der Beklagten eine private Nutzung des Internets an sich erlaubt bzw. geduldet wäre, lässt sich daraus nicht zwingend schließen, diese Nutzung dürfe auch während der Arbeitszeit zeitlich unbegrenzt bzw. in erheblichem Umfang und nicht nur außerhalb der Arbeitszeit, beispielsweise während der Pausen, erfolgen *(so auch Kramer NZA 2004, 457, 460)* . Dies gilt umso mehr, als die Tätigkeit des Klägers nicht zwangsläufig - wie beispielsweise bei einem Außendienstmitarbeiter - zumeist mit einer Nutzung des Internets verbunden ist.

34 III. Die Entscheidung des Landesarbeitsgerichts stellt sich auch nicht aus anderen Gründen als richtig dar (§ 561 ZPO). Die außerordentliche Kündigung vom 20. Dezember 2002 ist nicht schon unwirksam, weil die Beklagte - wie das Landesarbeitsgericht angenommen hat - den Kläger vor ihrem Ausspruch nicht abgemahnt hat.

35 1. Nicht in allen Fällen einer privaten Nutzung des Internets und damit im Zusammenhang stehender vertraglichen Pflichtverletzungen muss der Arbeitgeber den Arbeitnehmer vorher abgemahnt haben. Es sind zahlreiche Fallgestaltungen denkbar, in denen es einer Abmahnung nicht bedarf.

36 2. Nutzt der Arbeitnehmer während seiner Arbeitszeit das Internet in erheblichem zeitlichen Umfang *(“ausschweifend”: Däubler Internet und Arbeitsrecht Rn. 189)* privat, so kann er grundsätzlich nicht darauf vertrauen, der Arbeitgeber werde dies tolerieren. Er muss damit rechnen, dass der Arbeitgeber nicht damit einverstanden ist, wenn sein Arbeitnehmer seine Arbeitsleistung in dieser Zeit nicht erbringt und gleichwohl eine entsprechende Vergütung dafür beansprucht. Dies gilt selbst dann, wenn der Arbeitgeber keine klarstellende Nutzungsregelungen für den Betrieb aufgestellt hat. Bei einer fehlenden ausdrücklichen Gestattung oder Duldung des Arbeitgebers ist eine private Nutzung des Internets grundsätzlich nicht erlaubt *(Beckschulze DB 2003, 2777; Ernst NZA 2002, 585, 586; Dickmann NZA 2003, 1010; Kramer NZA 2004, 458, 461; Mengel NZA 2005, 752, 753)* . Weist in diesen Fällen die Nichtleistung der vertraglich geschuldeten Arbeit einen erheblichen zeitlichen Umfang, wie hier vor allem am 3. und 16. Oktober 2002, auf, kann der Arbeitnehmer in keinem Fall mit einer Duldung bzw. Gestattung durch den Arbeitgeber ernsthaft rechnen.

37

Der Arbeitnehmer kann weiter auch nicht damit rechnen, der Arbeitgeber sei, selbst wenn er prinzipiell

eine private Nutzung des Internets duldet, damit einverstanden, dass er sich umfangreiche pornografische Dateien aus dem Internet herunterlädt *(ArbG Frankfurt a.M. 2. Januar 2002 - 2 Ca 5340/01 - NZA 2002, 1093)* . Der Arbeitgeber hat ein Interesse daran, von Dritten nicht mit solchen Aktivitäten seiner Mitarbeiter in Verbindung gebracht zu werden *(BAG 6. November 2003 - 2 AZR 631/02 - AP BGB § 626 Verdacht strafbarer Handlung Nr. 39 = EzA BGB 2002 § 626 Verdacht strafbarer Handlung Nr. 2, sog. Integritätsinteresse; aA Däubler Internet und Arbeitsrecht Rn. 192)* .

38 Deshalb muss es jedem Arbeitnehmer klar sein, dass er mit einer exzessiven Nutzung des Internets während der Arbeitszeit seine arbeitsvertraglichen Haupt- und Nebenpflichten erheblich verletzt. Es bedarf daher in solchen Fällen auch keiner Abmahnung. Mit dem Erfordernis einer einschlägigen Abmahnung vor Kündigungsausspruch soll vor allem dem Einwand des Arbeitnehmers begegnet werden, er habe die Pflichtwidrigkeit seines Verhaltens nicht erkennen bzw. nicht damit rechnen können, der Arbeitgeber werde sein vertragswidriges Verhalten als so schwerwiegend ansehen *(KR-Fischermeier 7. Aufl. § 626 BGB Rn. 273 mwN)* . Dementsprechend bedarf es einer Abmahnung, wenn der Arbeitnehmer mit vertretbaren Gründen annehmen konnte, sein Verhalten sei nicht vertragswidrig oder werde vom Arbeitgeber zumindest nicht als ein erhebliches, den Bestand des Arbeitsverhältnisses gefährdendes Fehlverhalten angesehen *(Senat 9. Januar 1986 - 2 ABR 24/85 - AP BGB § 626 Ausschlussfrist Nr. 20 = EzA BGB § 626 nF Nr. 98; zuletzt: 25. März 2004 - 2 AZR 341/03 - AP BGB § 626 Nr. 189 = EzA BGB 2002 § 626 Nr. 6)* .

39 IV. Der Rechtsstreit war an das Landesarbeitsgericht zurückzuverweisen. Der Senat kann in der Sache selbst noch nicht abschließend entscheiden. Es steht noch nicht fest, ob ein wichtiger Grund nach § 626 Abs. 1 BGB bzw. ein verhaltensbedingter Kündigungsgrund nach § 1 Abs. 2 KSchG zur Beendigung des Arbeitsverhältnisses des Klägers vorliegt.

40 Auf Grund der bisherigen Feststellungen des Landesarbeitsgerichts ist zwar eine hinreichende kündigungsrelevante Pflichtenverletzung des Klägers und damit ein wichtiger Grund für eine außerordentliche Kündigung an sich bzw. ein verhaltensbedingter Kündigungsgrund im Prinzip gegeben. Denn unstreitig hat der Kläger an zwei Tagen seine Hauptleistungspflicht in erheblichem zeitlichen Umfang verletzt und seine Aufsichtsfunktion während der privaten Nutzung des Internets erheblich vernachlässigt.

41 Allerdings muss das Landesarbeitsgericht noch die notwendige umfassende Interessenabwägung vornehmen. Dabei wird es vor dem Hintergrund der - offensichtlich im Wesentlichen beanstandungsfreien - bisherigen Dauer des Beschäftigungsverhältnisses und der Position des Klägers als Erstmann mit Aufsichtsfunktionen zunächst die Schwere der Pflichtverletzung zu berücksichtigen haben. Sollte das Landesarbeitsgericht auf Grund der durchzuführenden Interessenabwägung zu dem Ergebnis kommen, die unstreitigen Pflichtverletzungen reichten in Anbetracht der abzuwägenden Interessen noch nicht als ein Kündigungsgrund für eine außerordentliche oder eine ordentliche Kündigung aus, wird es weiter aufklären müssen, ob der Kläger nicht auch noch an weiteren Tagen - wie die Beklagte behauptet - seine arbeitsvertraglichen Pflichten verletzt hat, in dem er während der Arbeitszeit das Internet privat genutzt hat. Auch wäre weiter festzustellen, in welchem Umfang er an den entsprechenden Tagen zu welchen Zeiten Pause gemacht hat. Des weiteren müsste das Landesarbeitsgericht der Frage vertieft nachgehen, ob und in welchem Umfang der Kläger seine Aufsichtsfunktion während der privaten Nutzung des Internets vernachlässigt hat.

42 Das Landesarbeitsgericht wird bei der vorzunehmenden Interessenabwägung weiter zu berücksichtigen und abzuwägen haben, dass die Beklagte die Nutzungsbedingungen für das Internet zwar nicht eindeutig festgelegt hat, ihr aber durch das Herunterladen von pornografischem Bildmaterial nicht nur Kosten bzw. ein Schaden entstanden sein könnte, sondern sie sich der Gefahr ausgesetzt sehen könnte, in der Öffentlichkeit in ein problematisches Licht gesetzt zu werden. Schließlich wird das Landesarbeitsgericht auch den Umstand würdigen müssen, dass der Kläger das Internet nicht für unverfängliche private Zwecke genutzt (vergleichbar dem Lesen einer Tageszeitung), sondern sich mit pornografischen Bildern und Videosequenzen während der Arbeitszeit versorgt hat.

Rost Bröhl Eylert

Fischer J. Walter

Entscheidungen

BUNDESARBEITSGERICHT Urteil vom 12.1.2006, 2 AZR 179/05

Verhaltensbedingte Kündigung wegen privater Internetnutzung

Tenor

Auf die Revision des Beklagten wird das Urteil des Landesarbeitsgerichts Nürnberg vom 26. Oktober 2004 - 6 Sa 348/03 - teilweise aufgehoben, soweit es über die Kündigung vom 25. Oktober 2002, den Weiterbeschäftigungsantrag und den Auflösungsantrag sowie über die Kosten entschieden hat.

Der Rechtsstreit wird insoweit zur neuen Verhandlung und Entscheidung - auch über die Kosten der Revision - an das Landesarbeitsgericht zurückverwiesen.

Im Übrigen wird die Revision des Beklagten zurückgewiesen.

Tatbestand

1 Die Parteien streiten über die Beendigung ihres Arbeitsverhältnisses auf Grund mehrerer außerordentlicher und (hilfsweise) ordentlicher Kündigungen, die der Beklagte wegen der unerlaubten Installierung einer Anonymisierungssoftware auf dem Dienst-PC und der unerlaubten Nutzung des Internets erklärt hat, sowie über die Wirksamkeit eines vom Beklagten hilfsweise gestellten Auflösungsantrags.

2 Der am 13. Dezember 1953 geborene, verheiratete Kläger ist seit dem 1. Mai 1991 als Angestellter im Wasserwirtschaftsamt W beschäftigt. Er ist Diplomingenieur und bezog zuletzt eine Vergütung nach der VergGr. III BAT. Das Arbeitsverhältnis der Parteien richtet sich nach den Bestimmungen des Bundes-Angestelltentarifvertrags (BAT).

3 Der Kläger ist mit einem Grad von 50 seit 11. Oktober 1999 als Schwerbehinderter anerkannt. Diese Schwerbehinderung teilte er dem Beklagten erstmals mit Schreiben vom 19. August 2002 mit.

4 Nachdem es auf dem dienstlichen Rechner des Klägers im Juni 2002 wiederholt zu Störungen gekommen war, wurde auf ihm eine neue Festplatte installiert. Der Kläger erhielt am 5. Juli 2002 den Rechner zurück. Bei einer Nachkontrolle des Rechners am 15. Juli 2002 wurde festgestellt, dass die Software-Programme JAVA und JAP - Software zur Anonymisierung von Internet-Zugriffen - sowohl auf der alten, defekten Festplatte als auch auf der neuen Festplatte installiert worden waren. Die erneute Installation der Anonymisierungsprogramme war bereits am 5. Juli 2002 nach der Rückgabe des in Stand gesetzten Rechners erfolgt. Darüber hinaus befanden sich sowohl auf der ausgewechselten als auch auf der neu installierten Festplatte eine Reihe von Internet-Adressen für private Nutzungen.

5 Nach einer für das Wasserwirtschaftsamt W geltenden Dienstanweisung aus dem Jahre 1992, deren Erhalt der Kläger bestätigt hatte, darf nur dienstliche Software und der Rechner nur zu dienstlichen Zwecken genutzt werden. In der “Dienstvereinbarung zur Nutzung des elektronischen Dokumentenaustausches mit E-Mail, des Internets und Intranets sowie des Telefax” idF vom 26. April 2001 (im Folgenden: DV) haben der Personalrat und die Dienststelle geregelt, dass eine Softwareinstallation auf den PCs nicht zulässig und eine private Nutzung des Internets grundsätzlich unzulässig ist (II 3 der DV). Der Dienststellenleiter hatte mit Informationsschreiben vom April 2000 die

Mitarbeiter auf die Dienstvereinbarung hingewiesen. Mit dem Informationsschreiben von Januar 2001 wurde an das Verbot der privaten Internet-Nutzung erinnert. Im Dezember 2001 wurde nochmals schriftlich auf die notwendige Zustimmung der Fachabteilung bei der Beschaffung von Hard- und Software hingewiesen.

6 Mit Schreiben vom 31. Juli 2002 forderte der Dienststellenleiter den Kläger auf, zu den Vorwürfen einer verbotenen Installation von JAP und JAVA, der unerlaubten Privatnutzung des Internets und den damit verbundenen Verstößen gegen die Dienstvereinbarung bis zum 2. August 2002 Stellung zu nehmen. Der Prozessbevollmächtigte des Klägers bat um eine Verlängerung der Stellungnahmefrist bis 9. August 2002, die der Dienststellenleiter ablehnte. Eine Stellungnahme des Klägers unterblieb.

7 Mit Schreiben vom 8. August 2002, unterzeichnet vom Baudirektor G des Wasserwirtschaftsamts W, kündigte der Beklagte das Arbeitsverhältnis des Klägers außerordentlich, hilfsweise ordentlich zum 31. März 2003. Die Unwirksamkeit dieser Kündigung steht inzwischen außer Streit.

8 Nachdem der Kläger mit Schreiben vom 19. August 2002 seine Anerkennung als Schwerbehinderter mitgeteilt hatte, informierte der Beklagte den Personalrat mit Schreiben vom 23. August 2002 von einer erneut beabsichtigten Kündigung des Klägers. Der Personalrat teilte mit Schreiben vom 26. August 2002 mit, er widerspreche der Kündigung nicht. Die Schwerbehindertenvertretung stimmte der beabsichtigten Kündigung mit Schreiben vom 26. August 2002 zu. Mit Bescheid vom 3. September 2002, dem Beklagten am 4. September 2002 zugegangen, stimmte das Integrationsamt der außerordentlichen Kündigung des Arbeitsverhältnisses des Klägers zu. Mit Schreiben vom 5. September 2002, unterzeichnet durch den Bauoberrat R, kündigte der Beklagte das Arbeitsverhältnis des Klägers erneut außerordentlich, hilfsweise ordentlich zum 31. März 2003. Der Kläger ließ diese Kündigung mit Telefax und Schreiben seines Prozessbevollmächtigten vom 5. September 2002 wegen fehlender Vollmachtsvorlage zurückweisen.

9 Mit Schreiben vom 6. September 2002, unterzeichnet vom Bauoberrat des Wasserwirtschaftsamts W R, kündigte der Beklagte erneut das Arbeitsverhältnis außerordentlich, hilfsweise ordentlich unter Beifügung einer Originalvollmacht für R.

10 Mit einem vom Baudirektor G unterzeichneten Schreiben vom 9. September 2002 kündigte der Beklagte das Arbeitsverhältnis des Klägers noch einmal außerordentlich, hilfsweise ordentlich.

11 Mit Schreiben vom 7. Oktober 2002 unterrichtete das Wasserwirtschaftsamt W den Personalrat über die beabsichtigte ordentliche Kündigung des Klägers. Der Personalrat stimmte mit Schreiben vom 21. Oktober 2002 der Kündigung des Klägers zu. Mit Bescheid vom 14. Oktober 2002 stimmte das Integrationsamt der beabsichtigten ordentlichen Kündigung des Klägers zu. Der Widerspruch des Klä gers gegen den Bescheid des Integrationsamts wurde mit Bescheid vom 17. März 2003 zurückgewiesen. Die dagegen gerichtete Klage hat das Verwaltungsgericht W wegen Vorgreiflichkeit ausgesetzt.

12 Mit dem vom Baudirektor und Behördenleiter G unterzeichneten Schreiben vom 25. Oktober 2002 kündigte der Beklagte das Arbeitsverhältnis des Klägers nochmals hilfsweise ordentlich zum 31. März 2003. Der Kläger wies die Kündigung mit Schreiben seines Prozessbevollmächtigten vom 25. Oktober 2002 wegen Nichtvorlage der Originalvollmacht für G zurück.

13 Der Kläger hat sich gegen alle Kündigungen mit seiner Kündigungsschutzklage gewandt und seine Weiterbeschäftigung begehrt. Er hat vorgetragen: Die Kündigungen seien schon aus formalen Gründen rechtsunwirksam. Die Kündigungen vom 5. September 2002 und 25. Oktober 2002 seien unwirksam, weil er sie wegen fehlenden Vorlage der Originalvollmacht wirksam zurückgewiesen habe. Als hilfsweise ordentliche sei die Kündigung vom 5. September 2002 schon wegen der fehlenden Zustimmung des Integrationsamts nicht wirksam. Die Kündigungen vom 6. September und 9. September 2002 seien sowohl wegen der fehlenden Beteiligung des Personalrats als auch wegen der fehlenden Zustimmung des Integrationsamts unwirksam. Zudem seien sie nicht unverzüglich ausgesprochen worden.

14 Sämtlichen Kündigungen liege kein wichtiger Grund iSd. § 626 Abs. 1 BGB oder ein verhaltensbedingter Kündigungsgrund iSv. § 1 Abs. 2 KSchG zugrunde. Er bestreite, einen erheblichen Teil seiner Arbeitszeit mit einer privaten Nutzung des PCs und des Internets verbracht zu haben. Das System sei durch das installierte Anonymisierungsprogramm nicht beeinträchtigt worden. Er habe dieses nur installiert und verwendet, weil er Einblicke Außenstehender in die dienstliche Nutzung habe verhindern wollen. Es sei ihm nicht bekannt gewesen, dass dadurch auch Einblicke des Arbeitgebers verhindert würden. Die nicht dienstlich zuordenbaren Internet-Adressen rechtfertigten keinen Schluss auf eine umfangreiche Privatnutzung. Dies gelte umso mehr, als über 80 % der gespeicherten Adressen dem dienstlichen Gebrauch zuzuordnen seien. Im Übrigen seien die persönlichen Daten unter Verstoß gegen sein Persönlichkeitsrecht ermittelt worden. Der Beklagte dürfe deshalb seine Kündigung hierauf nicht stützen. Außerdem hätte der Beklagte ihn vor dem Ausspruch der Kündigungen zunächst abmahnen bzw.

anhören müssen.

15 Der Kläger hat zuletzt beantragt

1. festzustellen, dass das Arbeitsverhältnis durch die Kündigungen vom 8. August 2002, vom 5. September 2002, vom 6. September 2002, vom 9. September 2002 und vom 25. Oktober 2002 nicht aufgelöst worden ist,
2. den Beklagten zu verurteilen, ihn bis zum rechtskräftigen Abschluss des Rechtsstreits zu unveränderten Bedingungen als Diplomingenieur weiterzubeschäftigen.

16 Der Beklagte hat beantragt

die Klage abzuweisen,

hilfsweise

das Arbeitsverhältnis gegen Zahlung einer Abfindung, deren Höhe in das Ermessen des Gerichts gestellt werde, aber 13.000,00 Euro nicht überschreiten solle, zum 31. März 2003 aufzulösen.

17 Zur Begründung seines Klageabweisungsantrags hat der Beklagte vorgetragen: Sämtliche Kündigungen seien auf Grund der erheblichen arbeitsvertraglichen Pflichtverletzungen gerechtfertigt. Es liege sowohl ein wichtiger Grund zur außerordentlichen Beendigung des Arbeitsverhältnisses als auch ein verhaltensbedingter Grund iSv. § 1 Abs. 2 KSchG vor. Der Kläger habe seinen dienstlichen PC und das Internet umfangreich privat genutzt. Auf Grund der installierten Anonymisierungssoftware sei es für den Arbeitgeber nicht mehr nachvollziehbar, auf welche Internet-Adressen der Kläger wie lange privat zugegriffen habe. Jedenfalls lasse die Speicherung einer Vielzahl von privaten Adressen darauf schließen, dass er den Rechner umfangreich für private Zwecke während der Arbeitszeit genutzt habe. Der Kläger habe im Zeitraum vom 1. Februar bis 16. Juli 2002 das Internet an 89 Arbeitstagen für ca. 89 Stunden genutzt, davon an einigen Tagen mehrere Stunden lang, zB am 29. April 2002 für sechs Stunden. Dies sei auf keinen Fall dienstlich veranlasst gewesen. Auch durch die zweimalige Installation der Anonymisierungssoftware JAP und JAVA auf dem dienstlichen Rechner habe er seine arbeitsvertraglichen Pflichten in erheblichem Maße verletzt. Dem Kläger seien die Verbote der privaten Nutzung und vor allem der privaten Installationen von fremden Rechnerprogrammen bekannt gewesen. Zumindest aus der Kumulation dieser Vorwürfe ergebe sich ein wichtiger Grund zur außerordentlichen Kündigung. Auf Grund der krassen Rechtsverletzungen habe es keiner Abmahnung bedurft, zumal es auf der Hand gelegen habe, dass seine Handlungsweise nicht erlaubt sei. Durch das Programm JAP sei das Schutzsystem (Firewall) des Beklagten umgangen worden. Es habe die Gefahr bestanden, dass das gesamte EDV-System der Dienststelle durch die Installation der privaten Software beschädigt werde. Durch seine Handlungen habe der Kläger das Vertrauensverhältnis endgültig zerstört. Dies gelte umso mehr, als er sich durch die Installation einer Anonymisierungssoftware bewusst einer Kontrolle bei der unerlaubten privaten Nutzung des Internets entzogen habe. Sowohl der Personalrat als auch der Datenschutzbeauftragte hätten im Übrigen am 15. Juli bzw. 19. Juli 2002 ihre Zustimmung zu einer umfassenden Überprüfung der Rechnernutzung gegeben.

18 Die hilfsweise begehrte Auflösung des Arbeitsverhältnisses sei schon deshalb begründet, weil das Vertrauensverhältnis zwischen den Arbeitsvertragsparteien auf Grund des Verhaltens des Klägers dauerhaft erheblich gestört sei. Mit der Installation des Anonymisierungsprogramms habe der Kläger raffiniert seine Spuren bei der privaten Nutzung des Internets verwischt.

19 Der Kläger hat zuletzt beantragt

den hilfsweise gestellten Auflösungsantrag zurückzuweisen.

20 Seiner Ansicht nach komme eine Auflösung des Arbeitsverhältnisses schon deshalb nicht in Betracht, weil sämtliche Kündigungen bereits aus formellen Gründen unzulässig seien.

21 Das Arbeitsgericht hat nach den Klageanträgen des Klägers erkannt und die Unwirksamkeit der Kündigungen festgestellt sowie den Beklagten zur Weiterbeschäftigung des Klägers verurteilt. Die Berufung des Beklagten hat das Landesarbeitsgericht zurückgewiesen und den hilfsweise gestellten Auflösungsantrag abgewiesen. Mit der vom Landesarbeitsgericht zugelassenen Revision begehrt der Beklagte weiterhin die Abweisung der Klage, hilfsweise die Auflösung des Arbeitsverhältnisses gegen Zahlung einer Abfindung.

Entscheidungsgründe

22 Die Revision des Beklagten hat, soweit sie die ordentliche Kündigung vom 25. Oktober 2002 betrifft, teilweise Erfolg.

23 A. Das Landesarbeitsgericht hat seine der Klage stattgebende Entscheidung im Wesentlichen wie folgt begründet: Die Berufung des Beklagten sei unzulässig, soweit er die Kündigung vom 8. August 2002 angegriffen habe. Er habe insoweit nicht nur selbst eingeräumt, dass es an der notwendigen Zustimmung des Integrationsamts zu dieser Kündigung gefehlt habe, sondern sich auch nicht mit der erstinstanzlichen Entscheidung auseinander gesetzt.

24 Die im Übrigen zulässige Berufung sei unbegründet. Zwar seien die Kündigungen vom 6. September und 9. September 2002 nicht wegen einer nicht ordnungsgemäßen Beteiligung des Personalrats unwirksam, da auf Grund des einheitlichen Lebenssachverhalts die Beteiligung der Personalvertretung am 23. August 2002 ausgereicht habe. Die außerordentlichen Kündigungen vom 5. September, 6. September und 9. September 2002 seien aber unwirksam, weil kein wichtiger Grund iSv. § 626 Abs. 1 BGB bzw. § 54 Abs. 1 BAT vorliege. Zwar könne in der privaten Nutzung des Internets ein arbeitsvertraglicher Pflichtenverstoß liegen, der eine außerordentliche Kündigung rechtfertigen könne. Eine solche exzessive Nutzung des Internets habe der Beklagte aber nicht dargelegt. Sie ergebe sich auch nicht aus der Anzahl der privaten Adressen bzw. aus dem Stundenumfang der Internet-Nutzung. Allein der Umstand einer unberechtigten Installation von Software auf dem Dienststellenrechner rechtfertige die außerordentliche Kündigung nicht. Zwar habe der Kläger damit gegen seine arbeitsvertraglichen Pflichten verstoßen. Die bloße abstrakte Gefahr für die Sicherheit des Behördennetzes wiege aber nicht so schwer, dass das Arbeitsverhältnis sofort beendet werden müsse. Es sei dem Beklagten zuzumuten, auf diese Pflichtverletzung mit einer Abmahnung zu reagieren. Der berechtigte Verdacht des Beklagten, der Kläger habe seine Vorgesetzten täuschen wollen, rechtfertige die Kündigung nicht, weil sie als Tatkündigung ausgesprochen worden sei. Eine Täuschungsabsicht stehe nicht fest. Dem Beklagten sei es im Übrigen zumutbar, den Kläger zumindest bis zum Ablauf der Kündigungsfrist weiterzubeschäftigen. Selbst wenn man in einer Privatnutzung des Internets sowie der unberechtigten Installation von fremder Software auf dem Dienstrechner zusammen betrachtet eine schwere Pflichtverletzung sehen würde, sei es dem Beklagten, bei dem kein konkreter Schaden entstanden sei und sich der behauptete Vertrauensverlust lediglich auf einen Verdacht stütze, in Anbetracht des Alters, der bisherigen Dauer des Arbeitsverhältnisses und der Schwerbehinderung des Klägers zuzumuten, das Arbeitsverhältnis noch bis zum Ablauf der Kündigungsfrist fortzusetzen.

25 Die hilfsweise als ordentliche Kündigungen erklärten Kündigungen vom 5. September, 6. September und 9. September 2002 einerseits und die vom 25. Oktober 2002 andererseits seien nach § 1 Abs. 2 KSchG unwirksam. Die möglichen Pflichtverletzungen rechtfertigten eine verhaltensbedingte Kündigung nicht. Zwar lägen in der verbotenen Nutzung des Internet-Zugangs zu privaten Zwecken auch ohne erkennbare Schäden für den Arbeitgeber, dem Herunterladen von Software und der sich hieraus ergebenden abstrakten Gefährdung des EDV-Netzes sowie dem objektiven Herunterladen einer Software, die die Internet-Auftritte des Klägers auch für den Arbeitgeber nicht mehr nachvollziehbar machten, erhebliche Verstöße gegen die arbeitsvertraglichen Pflichten des Klägers. Gleichwohl hätte der Beklagte unter Berücksichtigung des “ultima ratio Grundsatzes” vor dem Ausspruch einer Kündigung auf diese Pflichtenverstöße zunächst mit einer Abmahnung reagieren müssen. Die Vorwürfe seien nicht so schwerwiegend. Ein verständig abwägender Arbeitgeber hätte sie nicht zum Anlass einer Kündigung wegen Vertrauensverlustes genommen. Insoweit überwiege in Anbetracht des nicht erkennbaren Schadens für das EDV-System das Bestandsschutzinteresse des langjährig beschäftigten, älteren und schwerbehinderten Klägers die Interessen des Beklagten an einer Beendigung des Arbeitsverhältnisses.

26 Schließlich sei der Auflösungsantrag unbegründet. Aus den vom Beklagten vorgetragenen Aspekten ergebe sich nicht, dass ein weiteres gedeihliches Zusammenarbeiten zwischen den Arbeitsvertragsparteien zukünftig nicht mehr möglich sei.

27 B. Den Ausführungen des Landesarbeitsgerichts folgt der Senat nur teilweise im Ergebnis und in den Begründungen.

28 Im Ergebnis zutreffend hat das Landesarbeitsgericht erkannt, dass die außerordentlichen Kündigungen vom 5., 6. und 9. September 2002 unwirksam sind. Weiter hat das Landesarbeitsgericht im Ergebnis zutreffend erkannt, dass die (hilfsweise erklärten) ordentlichen Kündigungen vom 5., 6. und 9. September 2002 rechtsunwirksam sind. Die Ausführungen zur Unzulässigkeit der Berufung des Beklagten gegen die Kündigung vom 8. August 2002 hat die Revision nicht angegriffen.

29 Soweit das Berufungsgericht auch die ordentliche Kündigung vom 25. Oktober 2002 als sozial ungerechtfertigt angesehen hat, folgt ihm der Senat jedoch nicht.

30 I. Die außerordentliche - und hilfsweise ordentliche - Kündigung vom 5. September 2002 ist unwirksam nach § 174 Satz 1 BGB. Sie scheitert an der fehlenden Vorlage einer auf den Bauoberrat R ausgestellten Vollmachtsurkunde.

31 1. Nach § 174 Satz 1 BGB ist ein einseitiges Rechtsgeschäft, das ein Bevollmächtigter einem anderen gegenüber vornimmt, unwirksam, wenn der Bevollmächtigte eine Vollmachtsurkunde nicht vorlegt und der andere das Rechtsgeschäft aus diesem Grund unverzüglich zurückweist. Diese Voraussetzungen sind vorliegend erfüllt.

32 a) Die Kündigung ist eine einseitige Willenserklärung.

33 Es kann dahinstehen, ob der Bauoberrat R Vertretungsmacht zum Ausspruch dieser Kündigung hatte. Es entspricht jedenfalls der allgemeinen Meinung in Rechtsprechung und Literatur, dass bei der Kündigung eines Arbeitsverhältnisses durch einen Bevollmächtigten des Arbeitgebers grundsätzlich die Vorlage einer Vollmachtsurkunde erforderlich ist *(BAG 30. Mai 1972 - 2 AZR 298/71 - BAGE 24, 273; 29. Juni 1989 - 2 AZR 482/88 - AP BGB § 174 Nr. 7 = EzA BGB § 174 Nr. 6)* . Dies gilt auch für den öffentlichen Dienst *(Senat 29. Juni 1989 aaO)* . Die Ungewissheit, ob ein einseitiges Rechtsgeschäft von einem wirklich Bevollmächtigten ausgeht und der Vertretene dieses Rechtsgeschäft gegen bzw. für sich gelten lassen muss, besteht im gleichen Maß, wenn - vorbehaltlich der Sonderregelung des § 174 Satz 2 BGB - der Bevollmächtigte eines privaten oder eines öffentlichen Arbeitgebers handelt. In beiden Fällen können beispielsweise eine Vollmachtsüberschreitung, ein Vollmachtsmissbrauch oder überhaupt nur Zweifel am Bestehen einer Vollmacht vorliegen, so dass der Dritte durch das Zurückweisungsrecht geschü tzt werden muss. Der gesetzlich geforderte Nachweis der Vollmacht erschwert dabei den Geschäftsverkehr nicht unnötig.

34 b) Der Kläger bzw. dessen Prozessbevollmächtigter hat die Kündigung unverzüglich, nämlich am 5. September 2002, dh. am selben Tage, wegen fehlender Vorlage der Vollmachtsurkunde zurückgewiesen.

35 2. Die Zurückweisung der Kündigung war auch nicht gemäß § 174 Satz 2 BGB ausgeschlossen, weil der Kläger vom Beklagten bzw. dem Wasserwirtschaftsamt W von der Bevollmächtigung des Bauoberrats R in Kenntnis gesetzt worden war.

36 a) § 174 Satz 2 BGB bildet die Ausnahme zu § 174 Satz 1 BGB. Das Zurückweisungsrecht ist nach § 174 Satz 2 BGB nur dann ausgeschlossen, wenn der Vollmachtgeber demjenigen, gegenüber dem das einseitige Rechtsgeschäft vorgenommen werden soll, die Bevollmächtigung (vorher) mitgeteilt hat. Eine konkludente Mitteilung genügt, die Erlangung der Kenntnis auf anderem Wege dagegen nicht *(Erman/Palm BGB 11. Aufl. § 174 Rn. 6; Soergel/Leptien BGB 13. Aufl. § 174 Rn. 4)* .

37 aa) Der Kläger ist weder ausdrücklich noch konkludent über die Bevollmächtigung des Bauoberrats R in Kenntnis gesetzt worden.

38 bb) Entgegen der Auffassung des Beklagten ergibt sich eine solche In-Kenntnis-Setzung auch nicht aus dem “Vertretungszusatz”, mit dem der Bauoberrat R das Kündigungsschreiben unterzeichnet hat. Das In-Kenntnis-Setzen im Sinne dieser Norm setzt eine entsprechende Information über die Bevollmächtigung durch den Vollmachtgeber und nicht einen Hinweis des Vertreters auf seine Vertreterstellung voraus. Dafür sieht das Gesetz gerade die Vorlage der Vollmachtsurkunde vor. Auch ist das Kündigungsschreiben nicht “gesiegelt” worden *(vgl. BAG 29. Juni 1988 - 7 AZR 180/87 - BAGE 59, 93)* .

39 cc) Schließlich folgt aus dem Hinweis auf die allgemeinen Vertretungsregeln der Behö rden des Beklagten bei Abwesenheit des Behördenleiters bzw. seines Vertreters nicht hinreichend, dass damit der Empfä nger einer Kündigung von der Bevollmächtigung eines entsprechenden Vertreters ausreichend iSv. § 174 Abs. 2 BGB in Kenntnis gesetzt worden ist. Zum einen hat der Beklagte diese “Vertretungsregelung” nicht im Einzelnen in den Prozess eingeführt. Zum anderen kommt entscheidend hinzu, dass der Beklagte auch nicht die Abwesenheit des Behördenleiters bzw. dessen Vertreters und deren Grund und Dauer dargelegt hat. Diese Aspekte zeigen schon, dass zwar der Bauoberrat R auf Grund der allgemeinen Vertretungsregelung zu diesem Zeitpunkt zum Ausspruch der Kündigung ggf. bevollmächtigt gewesen sein mag, es aber für den Empfänger der Kündigungserklärung, den Kläger, nicht deutlich erkennbar gewesen ist, ob überhaupt ein Vertretungsfall und damit die Voraussetzungen der Vertretung bzw. Bevollmächtigung im konkreten Einzelfall vorgelegen haben. Gerade für diese Fälle sieht das Gesetz aber die Vorlage der Kündigungsvollmacht mit der Kündigungserklärung vor.

40 dd) Schließlich hat der Bauoberrat R auch keine solche Stellung inne, die zwingend mit einem Kündigungsrecht verbunden zu sein pflegt. Nach der Rechtsprechung des Senats kann ein In-Kenntnis-Setzen von einer Bevollmächtigung zum Ausspruch der Kündigung auch darin liegen, dass der

Arbeitgeber bestimmte Mitarbeiter, zB durch Bestellung zum Prokuristen, Generalbevollmächtigten oder Leiter einer Personalabteilung, in eine Stellung beruft, mit der das Kündigungsrecht üblicherweise verbunden zu sein pflegt *(BAG 30. Mai 1972 - 2 AZR 289/71 - BAGE 24, 273; 11. Juli 1991 - 2 AZR 107/91 - AP BGB § 174 Nr. 9 = EzA BGB § 174 Nr. 9)* . Davon kann vorliegend, bei einem Bauoberrat ohne allgemeine Personalkompetenz, nicht ausgegangen werden. Der Hinweis des Beklagten, die Mitarbeiter des höheren Dienstes seien stets in einer Stellung, die üblicherweise auch mit einer entsprechenden Vollmacht ausgestattet sei, vermag die Voraussetzungen des § 174 Satz 2 BGB nicht zu erfüllen. Mit einer Tätigkeit im höheren Dienst ist nicht stets und ständig eine Bevollmächtigung zu Personalentscheidungen, insbesondere zu Kündigungen, verbunden. Eine generelle Ausnahme und Ausweitung einer solchen Kompetenz auf alle Mitarbeiter des höheren Dienstes würde zu einer konturenlosen Verwässerung der Ausnahmevorschrift des § 174 Satz 2 BGB führen.

41 II. Die außerordentlichen und hilfsweise ordentlichen Kündigungen vom 6. und 9. September 2002 sind wegen der fehlenden Beteiligung des Personalrats nach Art. 77 Abs. 4 Bay. PersVG unwirksam.

42 1. Nach Art. 77 Abs. 1 Satz 1 Bay. PersVG wirkt der Personalrat bei der ordentlichen Kündigung durch den Arbeitgeber mit. Nach Art. 77 Abs. 3 Satz 1 Bay. PersVG ist der Personalrat vor einer außerordentlichen Kündigung anzuhören. Die Beteiligungspflicht des Personalrats besteht vor jeder Kündigung durch den Arbeitgeber *(Ballerstedt/Schleicher/Faber/Eckinger Bay. Personalvertretungsgesetz Art. 77 Rn. 2)* .

43 Vor den genannten Kündigungen ist der Personalrat nicht - bzw. nicht erneut - beteiligt worden. Deshalb liegt ein Beteiligungsfehler vor, der zur Unwirksamkeit der Kündigung führt.

44 2. Entgegen der Auffassung des Landesarbeitsgerichts und des Beklagten konnte von einer Beteiligung des Personalrats nicht deshalb abgesehen werden, weil dieser bereits zur Kündigung vom 5. September 2002 beteiligt worden war und die erneuten Kündigungen auf demselben Lebenssachverhalt beruhten. Die gesetzliche Regelung des Art. 77 Bay. PersVG verlangt vielmehr eine Beteiligung des Personalrats vor jeder Kündigung.

45 a) Der öffentliche Arbeitgeber hat grundsätzlich für jede Kündigung das Mitwirkungs- oder Anhörungsverfahren nach Art. 77 Bay. PersVG durchzuführen. Deshalb bedarf es einer - erneuten - Beteiligung des Personalrats immer dann, wenn der öffentliche Arbeitgeber nach Anhörung bzw. Mitwirkung des Personalrats bereits eine Kündigung erklärt hat und nunmehr eine neue (weitere) Kündigung aussprechen will. Das gilt auch, wenn der Arbeitgeber zwar die Kündigung auf den gleichen Sachverhalt stützt, die erste Kündigung dem Arbeitnehmer aber zugegangen ist und der Arbeitgeber damit seinen Kündigungswillen bereits verwirklicht hat. Das Gestaltungsrecht und die damit im Zusammenhang stehende Beteiligung des Personalrats ist mit dem Zugang der Kündigungserklärung verbraucht *(BAG 16. September 1993 - 2 AZR 267/93 - BAGE 74, 185; 5. September 2002 - 2 AZR 523/01 - AP LPVG Sachsen § 78 Nr. 1; zuletzt 10. November 2005 - 2 AZR 623/04 -)* . Etwas anderes kommt nur in den Ausnahmefällen in Betracht, in denen der Arbeitgeber seinen Kündigungsentschluss noch nicht verwirklicht hat. Nur dann kann eine erneute Beteiligung des Personalrats entbehrlich sein, wenn das frühere Beteiligungsverfahren ordnungsgemäß war, der Personalrat der Kündigung vorbehaltlos zugestimmt hat und eine Wiederholungskündigung im angemessenen zeitlichen Zusammenhang ausgesprochen und auf denselben Sachverhalt gestützt wird *(BAG aaO)* .

46 b) Durch den Ausspruch der außerordentlichen - und hilfsweise ordentlichen - Kündigung vom 5. September 2002 hatte der Beklagte seinen Kündigungswillen bereits verwirklicht. Damit war die Beteiligung des Personalrats vom 23. August 2002 “verbraucht”. Es liegt auch kein Fall vor, in dem ausnahmsweise eine erneute Beteiligung des Personalrats entbehrlich wäre. Die außerordentliche - hilfsweise ordentliche - Kündigung vom 5. September 2002 war dem Kläger bereits zugegangen. Im Übrigen fehlt es auch an den weiteren Voraussetzungen, um ausnahmsweise von einer erneuten Beteiligung des Personalrats absehen zu können. So hatte der Personalrat der beabsichtigten Kü ndigung schon nicht vorbehaltlos zugestimmt.

47 III. Die Revision ist jedoch begründet, soweit sie die Entscheidung des Landesarbeitsgerichts zur Unwirksamkeit der ordentlichen Kündigung vom 25. Oktober 2002 angreift.

48

Auf Grund der bisherigen tatsächlichen Feststellungen hätte das Landesarbeitsgericht dem Feststellungsantrag des Klägers nicht stattgeben dürfen. Es liegt - was das Landesarbeitsgericht auch zutreffend erkannt hat - eine schuldhafte Arbeitsvertragspflichtverletzung des Klägers und damit an sich ein erheblicher verhaltensbedingter Grund zur Kündigung vor. Entgegen der Auffassung des Landesarbeitsgerichts bedurfte es vorliegend jedoch keiner Abmahnung. Da auch die vom Berufungsgericht vorgenommene Interessenabwägung Defizite aufweist, kann der Senat aber nicht

abschließend über die Sozialwidrigkeit der Kündigung entscheiden. Der Rechtsstreit muss daher zur neuen Verhandlung und Entscheidung an das Landesarbeitsgericht zurückverwiesen werden (§ 563 ZPO).

49 1. Bei der Frage der Sozialwidrigkeit einer Kündigung gemäß § 1 Abs. 2 KSchG handelt es sich um die Anwendung eines unbestimmten Rechtsbegriffs, die vom Revisionsgericht nur darauf überprüft werden kann, ob das Landesarbeitsgericht in dem angefochtenen Urteil den Rechtsbegriff selbst verkannt hat, ob es bei der Unterordnung des Sachverhalts unter die Rechtsnorm des § 1 KSchG Denkgesetze oder allgemeine Erfahrungssätze verletzt hat, ob es bei der gebotenen Interessenabwägung, bei der dem Tatsachengericht ein Beurteilungsspielraum zusteht, alle wesentlichen Umstände berücksichtigt hat und ob das Urteil in sich widerspruchsfrei ist *(st. Rspr. des Senats, beispw. 10. Oktober 2002 - 2 AZR 472/01 - BAGE 103, 111; 24. Juni 2004 - 2 AZR 63/03 - AP KSchG 1969 § 1 Verhaltensbedingte Kü ndigung Nr. 49 = EzA KSchG § 1 Verhaltensbedingte Kündigung Nr. 65)* .

50 2. Diesem eingeschränkten Prüfungsmaßstab hält das Berufungsurteil nicht stand. Das Landesarbeitsgericht hat sowohl den Inhalt des Verhältnismäßigkeitsgrundsatzes überspannt als auch bei der notwendigen Interessenabwägung nicht alle fallrelevanten Aspekte berücksichtigt.

51 a) Zutreffend ist das Landesarbeitsgericht von einer arbeitsvertraglichen Pflichtenverletzung des Klägers ausgegangen. In welchem Umfang der Kläger allerdings durch eine verbotene Nutzung des Internet-Zugangs zu privaten Zwecken ohne erkennbare Schäden für den Arbeitgeber, durch das Herunterladen von Software und die sich daraus ergebende abstrakte Gefährdung des EDV-Netzes sowie durch das objektive Herunterladen einer Software, die die Internetnutzung des Klägers auch für den Arbeitgeber nicht mehr nachvollziehbar macht, seine Pflichten verletzt hat, kann nach den bisherigen lückenhaften tatsächlichen Feststellungen des Landesarbeitsgerichts nicht sicher beurteilt werden. Jedenfalls rechtfertigen die vom Berufungsgericht genannten Aspekte nach der Rechtsprechung des Senats *(7. Juli 2005 - 2 AZR 581/04 - EzA BGB 2002 § 626 Nr. 10, auch zur Veröffentlichung in der Amtlichen Sammlung vorgesehen)* die Annahme einer Verletzung der arbeitsvertraglichen Leistungs- und Nebenpflichten.

52 Es liegen zwar keine ausreichenden Feststellungen zu den möglichen Schäden beim Beklagten und vor allem zum Umfang der privaten Internet-Nutzung während der Arbeitszeit vor. Mögliche Pflichtverletzungen des Klägers insoweit können auf Grund der installierten Anonymisierungssoftware auch wohl nur im Stadium der Vermutung bzw. Unterstellung bleiben. Deshalb kommt vor allem dem unstreitigen Herunterladen und der Installation der JAP/JAVA-Anonymisierungssoftware entscheidungserhebliche Bedeutung zu.

53 Nach Auffassung des Senats hat der Kläger bereits mit der unerlaubten Installation der Anonymisierungssoftware seine Pflichten erheblich verletzt. Zum einen hat er das sich aus der Dienstanweisung und der Dienstvereinbarung ergebende Verbot einer Installation von privater Software missachtet. Zum anderen hat er durch seine eigenmächtige Veränderung von technischen Arbeitsmitteln des Arbeitgebers seine arbeitsvertragliche Rücksichtnahmepflicht (§ 241 Abs. 2 BGB) erheblich verletzt und durch sein Handeln seine Obhuts- und Betreuungspflicht gegenüber den ihm überlassenen und anvertrauten Betriebsmitteln missachtet.

54 b) Entgegen der Auffassung des Landesarbeitsgerichts konnte der Beklagte das Arbeitsverhältnis des Klägers auch ohne vorherige Abmahnung ordentlich kündigen.

55 aa) Für eine verhaltensbedingte Kündigung gilt das sog. Prognoseprinzip. Der Zweck der Kündigung ist nicht eine Sanktion für die Vertragspflichtverletzung, sondern dient der Vermeidung des Risikos weiterer Pflichtverletzungen. Die vergangene Pflichtverletzung muss sich deshalb noch in der Zukunft belastend auswirken *(BAG 21. November 1996 - 2 AZR 357/95 - AP BGB § 626 Nr. 130 = EzA KSchG § 1 Verhaltensbedingte Kündigung Nr. 56; ErfK/Ascheid 6. Aufl. § 1 KSchG Rn. 296)* . Eine negative Prognose liegt vor, wenn aus der konkreten Vertragspflichtverletzung und der daraus resultierenden Vertragsstörung geschlossen werden kann, der Arbeitnehmer werde den Arbeitsvertrag auch nach einer Kündigungsandrohung erneut in gleicher oder ähnlicher Weise verletzen *(ErfK/Ascheid 6. Aufl. § 1 KSchG Rn. 297)* . Deshalb setzt eine Kündigung wegen einer Vertragspflichtverletzung regelmäßig eine Abmahnung voraus. Sie dient der Objektivierung der negativen Prognose *(Staudinger/Preis § 626 BGB Rn. 103)* . Liegt eine ordnungsgemäße Abmahnung vor und verletzt der Arbeitnehmer erneut seine vertraglichen Pflichten, kann regelmäßig davon ausgegangen werden, es werde auch zukünftig zu weiteren Vertragsstörungen kommen *(ErfK/Ascheid 6. Aufl. § 1 KSchG Rn. 300; Staudinger/Preis § 626 BGB Rn. 106)* . Die Abmahnung ist insoweit notwendiger Bestandteil bei der Anwendung des Prognoseprinzips.

56 Sie ist zugleich auch Ausdruck des Verhältnismäßigkeitsgrundsatzes *(Staudinger/Preis § 626 BGB Rn. 105; Schlachter NZA 2005, 433, 435)* . Nach § 1 Abs. 2 KSchG muss die Kündigung durch das Verhalten des Arbeitnehmers bedingt sein. Eine Kündigung ist nicht gerechtfertigt, wenn es andere geeignete mildere Mittel gibt, um die Vertragsstörung zukünftig zu beseitigen. Dieser Aspekt hat durch die Regelung des § 314 Abs. 2 BGB eine gesetzgeberische Bestätigung erfahren *(Staudinger/Preis § 626 BGB Rn. 105; Stahlhacke/Preis/Vossen Kündigung und Kündigungsschutz im Arbeitsverhältnis 9. Aufl. Rn. 1172; Gotthardt Arbeitsrecht nach der Schuldrechtsreform Rn. 304 ff.; Kleinebrink FA 2002, 226 ff.; Schlachter NZA 2005, 433, 437)* . Nach dieser Norm ist eine Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe bestimmten Frist oder nach einer erfolglosen Abmahnung zulässig. Eine vorherige Abmahnung ist unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes aber ausnahmsweise entbehrlich, wenn eine Verhaltensänderung in Zukunft trotz Abmahnung nicht erwartet werden kann *(BAG 18. Mai 1994 - 2 AZR 626/93 - EzA BGB § 611 Abmahnung Nr. 31)* oder es sich um eine schwere Pflichtverletzung handelt, deren Rechtswidrigkeit dem Arbeitnehmer ohne weiteres erkennbar ist und die Hinnahme des Verhaltens durch den Arbeitgeber offensichtlich ausgeschlossen ist *(BAG 10. Februar 1999 - 2 ABR 31/98 - BAGE 91, 30; 21. Juli 1999 - 2 AZR 676/98 - AP BBiG § 15 Nr. 11 = EzA BBiG § 15 Nr. 13; siehe auch Gotthardt aaO Rn. 207; Staudinger/Preis § 626 BGB Rn. 118)* . Ähnliches ergibt sich aus § 314 Abs. 2 Satz 2 BGB, nach dem § 323 Abs. 2 BGB entsprechende Anwendung findet. Nach § 323 Abs. 2 BGB ist eine Fristsetzung bzw. damit auch eine Abmahnung entbehrlich, wenn der Schuldner die Leistung ernsthaft und endgültig verweigert oder besondere Umstände vorliegen, die unter Abwägung der beiderseitigen Interessen den sofortigen Rücktritt bzw. eine Kündigung rechtfertigen.

57 bb) Unter Berücksichtigung dieses rechtlichen Rahmens bedurfte es vorliegend keiner Abmahnung.

58 Durch die Installation der Anonymisierungssoftware auf dem betrieblichen Rechner des Beklagten hat der Kläger seine arbeitsvertraglichen Pflichten schwer verletzt. Die Rechtswidrigkeit seines Verhaltens war dem Kläger ohne weiteres erkennbar. Auch konnte er mit einer Hinnahme seines Handelns durch den Beklagten offensichtlich nicht rechnen. Auf Grund der Dienstanweisung und der Dienstvereinbarung wusste er, dass auf dem Dienstrechner keine private bzw. fremde Software geladen werden durfte. Ferner musste es sich ihm aufdrängen, dass insbesondere die Installation einer "Anonymisierungssoftware" dem Interesse des Beklagten eklatant zuwiderläuft. Aus den Hinweisen zum Programm JAP konnte der Kläger deutlich erkennen, dass niemand, also auch nicht der beklagte Arbeitgeber, herausbekommen kann, wann und welche Verbindungen zu einem bestimmten Rechner aufgebaut worden sind. Mit der Installation der Anonymisierungssoftware hat deshalb der Kläger nicht nur in das Betriebsmittel des Beklagten erheblich eingegriffen, sondern dem Arbeitgeber auch die Mö glichkeit genommen, seine technisches Betriebsmittel ggf. zu überwachen bzw. zu kontrollieren. Dies gilt umso mehr, als die Installation durch den Kläger heimlich erfolgte und er den Beklagten auch nicht später von der Installation in Kenntnis gesetzt hat. Insoweit liegt der Einwand des Klägers neben der Sache, es sei durchaus im Interesse des Arbeitgebers, sich gegen ein Ausspähen von Außen, das mit der Anonymisierungssoftware verhindert werden könne, zu schützen. Nicht der Kläger hat darüber zu befinden, ob es für den Beklagten notwendig und sinnvoll ist, einen zusätzlichen Datenschutz zu erlangen. Dies mag der Beklagte selbst entscheiden. Nichts wäre einfacher gewesen, als den Leiter der Dienststelle über einen solchen "Verbesserungsvorschlag" zu informieren und die Einführung dieser Anonymisierungssoftware in der Dienststelle des Beklagten anzuregen.

59 Es lag somit eine erhebliche Pflichtverletzung vor, bei der der Kläger nicht damit rechnen konnte, der Beklagte werde sie hinnehmen und dulden. Deshalb bedurfte es keiner Abmahnung. Genauso wenig bedurfte es einer Abmahnung im Hinblick auf die notwendige negative Prognose. Auf Grund der Verhaltensweisen des Klägers und seiner erheblichen Pflichtverletzung war der Schluss gerechtfertigt, er werde auch zukünftig seine arbeitsvertraglichen Pflichten nicht einhalten. Dies gilt umso mehr, als er sofort nach Erhalt des reparierten Rechners erneut die Anonymisierungssoftware installiert hatte.

60 c) Ob dieser erhebliche Pflichtenverstoß ausreichend ist, das Arbeitsverhältnis unter Beachtung der notwendigen umfassenden Interessenabwägung zu beenden, wird das Landesarbeitsgericht erneut zu prüfen haben. Die bisherige Interessenabwägung des Landesarbeitsgerichts weist Abwägungsdefizite auf. Das Berufungsgericht hat insoweit lediglich zu Gunsten des Arbeitgebers eine "Gesamtschau der Vorwürfe" vorgenommen und diesen Aspekten die sozialen Belange des Klägers gegenübergestellt. Damit wird es den anderen vom Beklagten vorgetragenen Interessen nicht gerecht.

61 aa) Bei der Interessenabwägung hat das Berufungsgericht einen umfassenden Beurteilungsspielraum, in dem das Revisionsgericht grundsätzlich nicht eingreifen kann. Lediglich in Ausnahmefällen, wenn sämtliche Abwägungsaspekte feststehen, ist eine eigene Abwägung durch das Revisionsgericht möglich. Daran fehlt es jedoch vorliegend.

62 bb) Bei der Interessenabwägung sind zugunsten des Klägers insbesondere die Dauer seiner Betriebszugehörigkeit, sein Lebensalter und vor allem seine Schwerbehinderteneigenschaft zu berücksichtigen.

63 Hinsichtlich des Beendigungsinteresses des Beklagten ist vor allem zu beachten, dass der Kläger seine arbeitsvertragliche Rücksichtnahmepflicht erheblich verletzt hat. Hinzu kommt der vom Landesarbeitsgericht bei der Interessenabwägung nicht hinreichend gewürdigte Umstand, dass der Kläger gerade eine Anonymisierungssoftware installiert hat, mit der dem Arbeitgeber jegliche Kontrollmöglichkeit seines technischen Betriebsmittels entzogen wird. Ist die Installation dieser Anonymisierungssoftware bewusst vom Kläger zur Umgehung einer möglichen Kontrolle durch den Arbeitgeber erfolgt, wozu das Berufungsgericht keine Feststellungen getroffen hat, so wird sich dies bei einer Abwägung der widerstreitenden Interessen erheblich zu Lasten des Klägers auswirken. Sollte dies nicht der Fall sein, müsste das Landesarbeitsgericht ggf. berücksichtigen und weiter aufklären, ob und in welchem Umfang eine private Nutzung des Internets durch den Kläger erfolgte und ob ggf. in der Dienststelle des Wasserwirtschaftsamtes W geringfügige private Nutzungen toleriert worden sind (“grundsätzlich”). Schließlich wäre in diesem Zusammenhang auch zu berücksichtigen, ob durch die Installation des Programms JAP/JAVA die Gefahr eines Virenbefalls durch Umgehung des rechnereigenen Schutzsystems bestand. Sollte dies der Fall sein, wäre dies zu Lasten des Klägers bei der Interessenabwägung ohne weiteres zu berücksichtigen.

64 3. Ob sich die Entscheidung des Landesarbeitsgerichts zur ordentlichen Kündigung vom 25. Oktober 2002 aus anderen Gründen (wegen einer fehlerhaften Zustimmung des Integrationsamts, der fehlerhaften Anhörung des Personalrats oder einer wirksamen Zurückweisung der Kündigungserklärung nach § 174 BGB) als richtig darstellt (§ 561 ZPO), kann auf Grund der fehlenden tatsächlichen Feststellungen einerseits und der fehlenden Prüfung dieser Aspekte durch das Berufungsgericht andererseits noch nicht abschließend festgestellt werden. Das Landesarbeitsgericht wird dies ggf. nachzuholen haben, wenn es unter Berücksichtigung der Interessenabwägung einen verhaltensbedingten Grund für gegeben ansieht. Dies gilt insbesondere für die Frage der wirksamen Zurückweisung der Kündigungserklärung nach § 174 BGB. Insoweit fehlt es an den notwendigen Feststellungen zur Vertretungsberechtigung des Baudirektors und Behördenleiters G.

65 Stellt das Landesarbeitsgericht wiederum die Sozialwidrigkeit der Kündigung fest, hat es erneut auch über den hilfsweise gestellten Auflösungsantrag des Beklagten zu entscheiden.

66 IV. Die Kostenentscheidung bleibt dem Berufungsurteil vorbehalten.

Rost Bröhl Eylert

Baerbaum Beckerle

Gericht:	VG Düsseldorf 1. Disziplinarkammer
Entscheidungsdatum:	26.02.2003
Aktenzeichen:	31 K 7892/02.O

Quelle:	juris
Normen:	§ 57 S 3 BG NW, § 58 S 2 BG NW, § 83 Abs 1 S 1 BG NW, § 5 Abs 1 DO NW, § 75 Abs 1 DO NW

Zur dienstanweisungswidrigen privaten Nutzung eines dienstlichen Computers und Internetzugangs am Arbeitsplatz

1. Orientierungssatz

1. Nutzt ein Beamter entgegen einer anders lautenden Dienstanweisung einen am Arbeitsplatz bereitgestellten Computer nebst Internetzugang zu privaten Zwecken, betrifft dieser Pflichtverstoß nicht den Kernbereich seiner Dienstpflichten, sondern stellt sich als ein Formalverstoß dar, der mit einer Ordnungswidrigkeit vergleichbar ist.

2. Die Qualität bzw das Gewicht eines in der dienstanweisungswidrigen Nutzung eines Dienstcomputers und eines dienstlichen Internetzugangs bestehenden Dienstvergehens wird nicht durch den Inhalt der Dateien bestimmt, die der Beamte aus dem Internet heruntergeladen und auf der Festplatte des Computers gespeichert hat.

3. Ebenso wenig kommt es für das Gewicht eines solchen Dienstvergehens darauf an, ob der Dienstvorgesetzte den Inhalt der aufgerufenen Internetseiten oder der heruntergeladenen und gespeicherten Dateien für anstößig oder unmoralisch hält.

2. Tenor

Gegen den Beamten wird wegen eines Dienstvergehens eine Warnung ausgesprochen.

Die Kosten des Verfahrens einschließlich der dem Beamten erwachsenen notwendigen Auslagen werden dem Dienstherrn auferlegt.

3. Gründe

1 I. Der am 0. 0 0000 geborene Beamte nahm nach dem Abitur das Studium der Architektur mit Schwerpunkt Städtebau an der Rheinisch-

Westfälischen Technischen Hochschule B auf, das er 1972 mit der Diplom-Hauptprüfung in der Fachrichtung Architektur erfolgreich abschloß.

2 Auf seinen Antrag wurde er am 4. April 1972 in den Vorbereitungsdienst für die Laufbahn des höheren bautechnischen Verwaltungsdienstes eingestellt und unter Berufung in das Beamtenverhältnis auf Widerruf zum Regierungsbaureferendar ernannt. Nach Absolvierung des Vorbereitungsdienstes bestand er am 7. August 1974 die Große Staatsprüfung in der Fachrichtung Städtebau mit dem Gesamturteil "befriedigend". Anschließend war er vom 1. Dezember 1974 bis 30. Juni 1975 als Angestellter bei der Landesplanungsgesellschaft Rheinland tätig. Mit Wirkung vom 1. Juli 1975 wurde er unter Berufung in das Beamtenverhältnis auf Probe zum Landesbaurat zur Anstellung bei dem Landschaftsverband Rheinland ernannt. Nach Auflösung der Landesplanungsgemeinschaften wurde er kraft Gesetzes am 1. Januar 1976 mit der Amtsbezeichnung "Regierungsbaurat z.A." in den Dienst des Landes Nordrhein-Westfalen übernommen, dem Regierungspräsidenten L1 zugewiesen und am 16. Mai 1977 zum Regierungsbaurat ernannt. Mit Wirkung vom 1. September 1977 wurde ihm die Eigenschaft eines Beamten auf Lebenszeit verliehen. Er wurde 1979 zum Oberregierungsbaurat und 1991 zum Regierungsbaudirektor ernannt.

3 Der Beamte war bis 1985 als Hauptdezernent im Dezernat 01 (Braunkohle) eingesetzt und übernahm 1987 nach einjähriger Tätigkeit bei der Bezirksplanungsbehörde L1 das Dezernat 02 (Verkehrs- und Leitungswege). 1990 wechselte er als Dezernent in das Dezernat03. Ab 1993 wurde er als Dezernent im Dezernat 04 (Raumordnungsverfahren/ GEP-Bearbeitung)eingesetzt und ab Juli 1995 zum Hauptdezernenten dieses Dezernates bestellt. Nach einem erlittenen Herzinfarkt wurde seine Bestellung auf eigenen Wunsch im Juli 1997 wieder aufgehoben. Seitdem wird er als Dezernent weiterhin im Dezernat 04 eingesetzt.

4 Der Beamte ist weder disziplinarrechtlich noch strafrechtlich vorbelastet. Er hat 1997 seine 25-jährige Dienstzeit vollendet und die Ehrenurkunde hierzu erhalten. Seine dienstlichen Leistungen im Amt des Regierungsbaudirektors sind 1993 und 1996 jeweils mit 4 Punkten ("übertrifft die Anforderungen"), 1999 mit 3 Punkten ("entspricht voll den Anforderungen") und 2002 ebenfalls mit 3 Punkten ("entspricht voll den Anforderungen") beurteilt worden.

5 Der Beamte hat 1997 einen Herzinfarkt erlitten und leidet seitdem unter gesundheitlichen Beeinträchtigungen, die mit einem Grad der Behinderung von 40 v.H. anerkannt sind. Er befindet sich wegen der Folgen des Herzinfarktes weiterhin in ärztlicher Behandlung und nimmt ärztlich verordnete Medikamente ein, die nach seiner Erfahrung ermüdend wirken und ihn bei der Arbeit beeinträchtigen. Hinzugekommen ist bei ihm ein Tinnitusleiden. Ferner leidet er an Krampfadern und hat

sich deswegen bereits sieben Operationen unterzogen. Er hat zudem an beiden Knien Meniskusbeschwerden, die ebenfalls operativ behandelt worden sind.

6 Der Beamte ist seit 1972 verheiratet. Seine Ehefrau ist als Angestellte bei der Stadt C halbtags tätig. Sie haben zwei erwachsene Kinder, die sie derzeit noch monatlich mit jeweils 500 Euro unterstützen. Der Beamte und seine Ehefrau sind Eigentümer eines lastenfreien Einfamilienhauses, das sie selbst bewohnen. Ihre wirtschaftlichen Verhältnisse sind geordnet, sie haben keine Schulden und verfügen über Rücklagen.

7 Wegen der gesundheitlichen, persönlichen und wirtschaftlichen Verhältnisse im übrigen wird auf die Angaben des Beamten in der Hauptverhandlung Bezug genommen.

II.

8 Die Bezirksregierung L1 leitete mit Verfügung vom 15. Juli 2002 - zugestellt am 18. Juli 2002 - das förmliche Disziplinarverfahren gegen den Beamten ein. Gegenstand der Einleitungsverfügung ist der Vorwurf, der Beamte habe ein Dienstvergehen begangen, indem er in der Zeit vom 3. Dezember 2001 bis 30. Juni 2002 während der Dienstzeit im Umfang von über 160 Stunden den ihm für dienstliche Zwecke zur Verfügung gestellten PC und den ebenfalls zur dienstlichen Nutzung zur Verfügung gestellten Internetzugang dazu genutzt habe, auf der lokalen Festplatte seines Computers in großem Umfang Videodateien zu speichern, die pornographische Darstellungen und Szenen zum Inhalt und keinen dienstlichen Bezug hätten. Außerdem habe er ausführbare Dateien gespeichert, die im Hausnetz nicht zur Verfügung gestellt würden und die nicht nach § 14 Abs. 1 der "Dienstanweisung über Datenschutz und Datensicherung beim Einsatz von Informationstechnik" von Dezernat 14 freigegeben worden seien (z.B. Moorhuhnjagd).

9 Der Beamte wurde am 5. September 2002 zu Beginn der Untersuchung zur Person und zur Sache vernommen. Er räumte die ihm in der Einleitungsverfügung zur Last gelegten Vorwürfe uneingeschränkt ein und erklärte, daß es sich um einen einmaligen Ausrutscher gehandelt habe, den er sehr bedaure. Er sei in die Sache "hereingerutscht" und nach dem ersten Aufrufen von Internetseiten mit pornographischem Inhalt immer neugieriger geworden.

10 Der Beamte erklärte auch von sich aus, daß er bereit sei, den entstandenen Schaden in Form von 160 Stunden Mehrarbeit zu ersetzen.

11 Nach Abschluß der Untersuchung und Vorlage des Untersuchungsberichts vom 18. September 2002 fertigte der Vertreter der Einleitungsbehörde unter dem 6. November 2002 die Anschuldigungsschrift, die am 11. November 2002 bei Gericht eingegangen ist.

12 In der Anschuldigungsschrift wird der Beamte wie folgt angeschuldigt:

13 1. Der Beamte hat in einem Umfang von mehr als 160 Stunden in der Zeit vom 03.12.2001 bis zum 30.06.2002 unter Verletzung von § 2 der Dienstanweisung für den Umgang und die Nutzung von Internetzugängen über Arbeitsplatzcomputer den dienstlich zur Verfügung gestellten Internetzugang und die dienstliche technische Ausrüstung für private Recherchen genutzt und in einem erheblichen Umfang (3,8 GB, 3474 Videoclips) Videodateien mit porno-graphischen Darstellungen und Szenen aus dem Internet heruntergeladen.

2.

14 3. Der Beamte hat auf seiner lokalen Festplatte ausführbare Dateien (z.B. Moorhuhnjagd, Videoplayer), die er zuvor aus dem Internet heruntergeladen hat, unter Verstoß gegen § 14 Abs. 1 der Dienstanweisung über Datenschutz und Datensicherung beim Einsatz von Informationstechnik der Bezirksregierung L1 (keine Freigabe des IT-Dezernates) abgespeichert und nach seiner eigenen Einlassung für das Anschauen der Videodateien betrieben.

4.

15 5. Der Beamte hat nach den Protokolldateien der IT bei wohlwollenden Betrachtung im genannten Zeitraum mehr als 160 Stunden während seiner Arbeitszeit für private, nicht dienstliche Zwecke im Internet gesurft und sich somit der Arbeitsleistung im gleichen Umfang entzogen. Eine höhere Ausfallzeit ist anzunehmen, da die Betrachtung der auf der Festplatte gespeicherten Videodateien nicht protokolliert wird.

6.

16 In der Hauptverhandlung hat der Vertreter der Einleitungsbehörde beantragt,

17 die Dienstbezüge des Beamten in einer Größenordnung von vier bis fünf Monatsgehältern zu kürzen.

18 Der Beamte und sein Verteidiger haben keinen förmlichen Antrag gestellt.

19 Der Disziplinarkammer haben die Gerichtsakten, die Personalakten und die Disziplinar-vorgänge (Beiakten Hefte 1 bis 5) vorgelegen. Die Akten waren Gegenstand der Hauptverhandlung.

III.

20 Die Hauptverhandlung hat aufgrund des Geständnisses des Beamten und der ihrem wesentlichen Inhalt nach zum Gegenstand der Hauptverhandlung gemachten Verfahrensakten den folgenden Sachverhalt ergeben:

21 Der Beamte hat seit ca. drei Jahren dienstlich einen Internetzugang, der ihm auf seinen Antrag hin eingerichtet worden ist. Er ist als Regionalplaner im Bereich von Abgrabungsvorhaben tätig und kann das Internet u.a. zum Abrufen entsprechender Pläne dienstlich einsetzen. Nach Maßgabe der Dienstanweisung für den Umgang und die Nutzung von Internetzugängen über Arbeitsplatzcomputer (Verfügung des Regierungspräsidenten L1 vom 01.04.1999) darf der Anschluß nur für dienstliche Zwecke genutzt werden. Eine private Nutzung ist nicht zulässig.

22 Der Beamte nutzte in der Zeit vom 3. Dezember 2001 bis 30. Juni 2002 während seiner Arbeitszeit im Umfang von mindestens 160 Stunden den Internetzugang für private Recherchen, lud in einem erheblichen Umfang (3,8 GB, 3474 Videoclips) Videodateien mit pornographischen Darstellungen und Szenen aus dem Internet herunter und speicherte diese auf der Festplatte seines Arbeitsplatzcomputers. Er speicherte außerdem auf der Festplatte ausführbare Dateien ab (z.B. Moorhuhnjagd, Videoplayer), die er zuvor aus dem Internet heruntergeladen hatte und die nicht durch das IT-Dezernat freigegeben waren. Die Auswertung der Protokolldateien des IT-Dezernates ergab, daß der Beamte in dem genannten Zeitraum mindestens 160 Stunden während seiner Arbeitszeit für private Zwecke im Internet gesurft und insoweit keine Arbeitsleistung erbracht hat. Ein darüber hinausgehender Zeitaufwand für das Betrachten der auf der Festplatte gespeicherten Videodateien ist weder von den Protokolldateien erfaßt noch in der Untersuchung festgestellt worden.

23 Der Beamte hat den ihm zur Last gelegten Sachverhalt von Anfang an vorbehaltlos und vollständig eingeräumt. Auch in der Hauptverhandlung hat er sich zur Sache eingelassen und im wesentlichen erklärt:

24 Das, was ihm in der Anschuldigungsschrift vorgeworfen werde, sei richtig. Er gestehe es ein. Der Bildschirm in seinem Dienstzimmer habe von einem Eintretenden nicht eingesehen werden können, so daß die Gefahr, beim Surfen auf Portalen dieser Art entdeckt zu werden, gering gewesen sei. Er habe damals nicht darüber nachgedacht, als er das

erste Mal eine entsprechende Seite aufgerufen habe. Dann sei er von Neugier und dem Gefühl getrieben worden, weitersuchen zu müssen. Sicherlich werde auch die Arbeitsleistung durch sein Verhalten gelitten haben. Allerdings sei der Arbeitsanfall im Bereich der Regionalplanung nicht kontinuierlich, sondern sei vergleichbar mit einem Stoßgeschäft. Wenn in seinem Dezernat ein erhöhter Arbeitsanfall bestehe, könne man die regelmäßige Arbeitszeit nicht einhalten und auch keine Pausen machen. Vielmehr sei dann die anfallende Arbeit zu bewältigen, auch unter Einsatz von Überstunden. Diese würden zwar im Umfang von bis zu 20 Stunden im Monat dem Zeitkonto gutgeschrieben. Darüber hinausgehende Überstunden verfielen jedoch. Hierzu sei es seit dem in Rede stehenden Vorfall vielleicht drei bis vier Mal gekommen. Einen privaten Internetanschluß habe er schon zu Hause gehabt, bevor es zu dem ihm vorgeworfenen Verhalten im Dienst gekommen sei.

25 Sein dienstlicher Internetzugang sei zu keiner Zeit gesperrt worden. Auch habe die Bezirksregierung seinen Fall nicht zum Anlaß genommen, die Belegschaft erneut über die Benutzung des Internets zu belehren. Mittlerweile seien alle Mitarbeiter seiner Behörde mit einem Internetzugang freigeschaltet.

IV.

26 Nach dem Ergebnis der Hauptverhandlung steht fest, daß der Beamte die ihm obliegenden Pflichten aus §§ 57 Satz 3 , 58 Satz 2 LBG schuldhaft verletzt und damit ein einheitlich zu wertendes Dienstvergehen nach § 83 Abs. 1 Satz 1 LBG begangen hat.

27 Dabei kann es dahinstehen, ob in jedem Einzelfall einer privaten Nutzung des dienstlichen Internetzugangs bereits ein disziplinarrechtlich relevantes Fehlverhalten zu sehen ist. Denn bei einer Dauer und einem Umfang wie hier ist die Grenze zur disziplinaren Relevanz jedenfalls überschritten, wovon im Ergebnis auch die Beteiligten ausgehen. Diese Feststellung bedeutet jedoch nicht, daß allein wegen eines solchen Dienstvergehens zwingend eine Disziplinarmaßnahme gegen den Beamten verhängt werden muß.

28 Der Dienstvorgesetzte hat im nichtförmlichen Disziplinarverfahren, wie die gesetzliche Regelung in §§ 6 Abs. 3, 27 Abs. 1, 28 Abs. 1 DO NW zeigt, einen erheblichen Entscheidungsspielraum. So kann er auch bei Vorliegen eines Dienstvergehens von der Verhängung einer Disziplinarmaßnahme absehen und das Verfahren einstellen. Er kann in einem solchen Fall eine Mißbilligung im Sinne des § 6 Abs. 3 DO NW aussprechen, die keine Disziplinarmaßnahme ist oder sich auf sonstige Maßnahmen im Rahmen der Dienstaufsicht beschränken. Die Einleitungsbehörde hat auch im förmlichen Disziplinarverfahren grundsätzlich vergleichbare Entscheidungsmöglichkeiten, die sich aus § 63 Abs. 2 DO NW ergeben. Nach Einreichung der Anschuldigungsschrift bei Gericht

bestehen diese Möglichkeiten für die Einleitungsbehörde allerdings nicht mehr. Das Disziplinargericht kann das Verfahren dann nur unter den Voraussetzungen der §§ 63 Abs. 1, 75 Abs. 3 DO NW einstellen. Diese Voraussetzungen liegen hier jedoch nicht vor. Gegen den Beamten ist daher eine Disziplinarmaßnahme zu verhängen (§ 75 Abs. 1 DO NW).

29 Nach dem Ergebnis der Hauptverhandlung steht zur Überzeugung der Kammer fest, daß eine über die Warnung hinausgehende Disziplinarmaßnahme weder erforderlich noch angemessen ist.

30 Bei der Bemessung der Disziplinarmaßnahme sind die disziplinaren Zwecke maßgeblich. Das Disziplinarverfahren dient - im Unterschied zum Strafverfahren - nicht etwa der Bestrafung eines Beamten wegen eines begangenen Dienstvergehens, sondern der Erhaltung der Funktionsfähigkeit und der Ansehenswahrung des öffentlichen Dienstes. Bei der disziplinaren Ahndung von Dienstvergehen im unteren bis mittleren Bereich ist vorrangiger Zweck die sog. Pflichtenmahnung, d.h. die erzieherische Einwirkung auf den Beamten selbst und mittelbar auch auf die Beamtenschaft. Für die Frage der Notwendigkeit einer Pflichtenmahnung kommt es wesentlich auf das Gewicht des Dienstvergehens und die sich aus dem Gesamtverhalten ergebende Persönlichkeit des Beamten an. Nach diesen Kriterien spricht im Zeitpunkt der Hauptverhandlung nichts dafür, daß der Beamte selbst (noch) einer disziplinaren Pflichtenmahnung bedarf. Sein Dienstvergehen ist von geringem Gewicht. Der Pflichtenverstoß betrifft nicht den Kernbereich seiner Dienstpflichten. Es handelt sich vielmehr um Formalverstöße gegen Dienstanweisungen, die mit Ordnungswidrigkeiten vergleichbar sind.

31 Entgegen der Ansicht des Vertreters der Einleitungsbehörde wird die Qualität des Dienstvergehens bzw. dessen Gewicht nicht bestimmt durch den Inhalt der Dateien, die der Beamte aus dem Internet heruntergeladen und auf der Festplatte gespeichert hat. Maßgeblich für den festgestellten Pflichtenverstoß ist vielmehr die Nichtbeachtung der Dienstanweisung, die eine Nutzung des Internetzugangs nur für dienstliche Zwecke zuläßt. Die Dienstanweisung untersagt jede Art der privaten Nutzung und macht dies nicht etwa davon abhängig, ob es sich um Internetseiten mit pornographischem Inhalt oder anderen Inhalten handelt. Ebensowenig kommt es für das Gewicht der Pflichtenverstöße darauf an, ob der Dienstvorgesetzte den Inhalt solcher Internetseiten, wie sie der Beamte aufgerufen hat, für anstößig oder unmoralisch hält. Anderenfalls würde dies im Ergebnis zu einer Zensur des Inhalts von Internetseiten und damit auch zu einer Ungleichbehandlung gleichartiger Pflichtenverstöße führen, was mit dem geltenden Dienstrecht nicht vereinbar wäre. Ein anderes und zwar wesentlich höheres Gewicht haben Pflichtenverstöße in diesem Bereich allerdings dann, wenn für die privaten Recherchen zusätzlich Gebühren zu Lasten des Dienstherrn anfallen oder wenn es sich um strafrechtlich relevante Sachverhalte

und strafbares Vorgehen handelt. Solche erschwerenden Umstände liegen hier ersichtlich nicht vor.

32 Auch sonst sind keine - über das Dienstvergehen hinausgehende - Umstände gegeben, die gegen den Beamten sprechen könnten. Sein Verhalten hat zu keinem wirtschaftlichen Schaden und zu keiner meßbaren Verzögerung von Dienstgeschäften geführt. Der Beamte hat in seiner langjährigen Dienstzeit durchweg anerkennenswerte Leistungen und pflichtbewußtes Verhalten gezeigt. Sein erstmaliger Pflichtenverstoß stellt sich auf diesem Hintergrund als einmaliges, persönlichkeitsfremdes Fehlverhalten dar, das nicht auf Uneinsichtigkeit oder Widersetzlichkeit beruht. Der Beamte hat sofort Einsicht in sein Fehlverhalten gezeigt, es eingestanden und umgehend beendet, als er durch Mitarbeiter des IT-Dezernates mit dem Ergebnis der Überprüfung konfrontiert wurde. Ebenso hat er im Disziplinarverfahren von Anfang an den ihm zur Last gelegten Sachverhalt vorbehaltlos eingeräumt und sein Fehlverhalten aufrichtig bedauert. Die Dienstbehörde hat diesen Vorfall auch nicht zum Anlaß genommen, den Internetzugang für den Beamten zu sperren. Bei verständiger Betrachtung und Würdigung aller Umstände spricht daher nichts dafür, daß der Beamte (noch) einer Pflichtenmahnung bedarf. Als disziplinarer Zweck der Maßnahme kommt daher nur die Ansehenswahrung und mittelbare Einwirkung auf die Beamtenschaft hinsichtlich der Einhaltung solcher Dienstanweisungen in Betracht. Dieser Zweck rechtfertigt - zumal unter Berücksichtigung des Grundsatzes der Stufenfolge von Disziplinarmaßnahmen (vgl. § 5 Abs. 1 DO NW) - keine weitergehende Disziplinarmaß-nahme als die gegen den Beamten ausgesprochene Warnung.

33 Die Kostenentscheidung beruht auf §§ 113 Abs. 1 Satz 1 Halbsatz 2, 115 Abs. 2 Satz 1 DO NW. Zwar hat das Gericht gegen den Beamten wegen eines Dienstvergehens eine Warnung ausgesprochen. Es wäre jedoch unbillig, den Beamten insoweit mit den Kosten des Verfahrens zu belasten. Eine Warnung ist grundsätzlich im nichtförmlichen Disziplinarverfahren durch Disziplinarverfügung des Dienstvorgesetzten zu verhängen. Hierzu ist weder die Einleitung des förmlichen Disziplinarverfahrens noch etwa die Einreichung einer Anschuldigungsschrift bei Gericht erforderlich. Es wäre im vorliegenden Fall daher unbillig, den Beamten mit Kosten zu belasten, die ihm durch nicht erforderliche und seitens des Dienstherrn ohne weiteres vermeidbare Verfahrensabschnitte entstanden sind.

Entscheidungen

BUNDESARBEITSGERICHT Urteil vom 27.4.2006, 2 AZR 386/05

Ordentliche Unkündbarkeit - private Internetnutzung

Leitsätze

Bei der Prüfung der Frage, ob ein wichtiger Grund zur fristlosen Kündigung eines ordentlich unkündbaren Arbeitnehmers vorliegt, geht es allein um die Abwägung, ob dem Arbeitgeber die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der "fiktiven" Kündigungsfrist noch zugemutet werden kann.

Tenor

Auf die Revision der Beklagten wird das Urteil des Landesarbeitsgerichts Rheinland-Pfalz vom 9. Mai 2005 - 7 Sa 68/05 - aufgehoben.

Die Sache wird zur neuen Verhandlung und Entscheidung - auch über die Kosten der Revision - an das Landesarbeitsgericht zurückverwiesen.

Tatbestand

1 Die Parteien streiten über die Wirksamkeit einer Kündigung der Beklagten vom 29. Juni 2004.

2 Der am 8. August 1951 geborene Kläger (verheiratet, ein Kind) ist seit dem 10. Juli 1972 bei der Beklagten bei dem Bundesamt für Wehrtechnik und Beschaffung (BWB) beschäftigt. Seine Bruttomonatsvergütung betrug zuletzt 3.047,00 Euro. Auf das Arbeitsverhältnis der Parteien findet der BAT Anwendung.

3 Dem Kläger steht an seinem Arbeitsplatz ein PC mit Internetzugang zur Verfügung. Der Internetzugang darf nach der einschlägigen Dienstvorschrift nicht zu privaten Zwecken genutzt werden. Auf diese Regelung weist die Beklagte alle Internetnutzer in regelmäßigen Abständen von zwei Jahren hin. Der Kläger hat die Kenntnisnahme zuletzt im Dezember 2003 mit seiner Unterschrift bestätigt. Die Sicherheitsbelehrung enthält auch einen ausdrücklichen Hinweis auf arbeitsrechtliche Konsequenzen im Falle des Verstoßes.

4 Am 13. Mai 2004 wurde der PC des Klägers beschlagnahmt. Am 14. Mai 2004 wurde der Präsident des BWB darüber informiert, von dem PC des Klägers aus sei am 11. Mai 2004 eine Internetseite aufgerufen worden, auf der Sex mit Tieren dargestellt wird. Die Beklagte schaltete nach Prüfung des PC des Klägers die Kriminalpolizei ein. Gegen den Kläger wurde ein Ermittlungsverfahren wegen Verbreitung, Erwerb und Besitz kinderpornografischer Schriften eingeleitet. Dieses ist zwischenzeitlich eingestellt worden.

5 Am 4. und am 7. Juni 2004 wurde der Kläger zu dem Vorwurf angehört, er habe vom 8. März bis 13. Mai 2004 während der Dienstzeit rund 50 Stunden verbotswidrig den diensteigenen Internetzugang privat genutzt und dabei vorrangig pornografische Seiten besucht. Mit Schreiben vom 7. Juni 2004 wurde der Personalrat zur beabsichtigten außerordentlichen Kündigung des Klägers angehört. Mit Schreiben vom 9. Juni 2004 teilte der Personalrat mit, er stimme der außerordentlichen Kündigung des Klägers nicht zu. Am 9. Juni 2004 übermittelte der Kläger der Beklagten seinen Antrag auf Anerkennung als Schwerbehinderter. Mit Bescheid vom 20. September 2004 wurde ein Grad der Behinderung von 30 anerkannt. Am 9. Juni 2004 wurde die Vertrauensfrau der Schwerbehinderten beteiligt. Ihre

Stellungnahme erfolgte mit Schreiben vom 11. Juni 2004. Am 11. Juni 2004 bat die Beklagte das Integrationsamt um Zustimmung zur Kündigung. Diese wurde mit Datum vom 24. Juni 2004 erteilt. Mit Schreiben vom 29. Juni 2004, dem Kläger am gleichen Tage zugegangen, hat die Beklagte das Arbeitsverhältnis mit dem Kläger daraufhin außerordentlich gekündigt.

6 Dagegen wendet sich der Kläger mit seiner Klage. Er hat bestritten, im Umfang von 50 Stunden zu privaten Zwecken im Internet gesurft zu haben. Er habe zu keinem Zeitpunkt Dateien heruntergeladen, er habe sich vielmehr nur Dateien im Internet angeschaut. Zu keinem Zeitpunkt habe er Seiten mit kinderpornografischem Inhalt aufgerufen. Da den Logdateien konkrete Dateinamen nicht zu entnehmen seien, könne er nicht detailliert Stellung nehmen. Es sei auch zu berücksichtigen, dass 394 Minuten auf die 15-minütige Frühstückspause und die 45-minütige Mittagspause entfielen. Außerdem habe er sein Passwort auf dem PC abgespeichert und den Raum nicht abgeschlossen, wenn er seinen Arbeitsplatz nur kurz verlassen habe. Das Personalteam sei zudem zur Auswertung der Dateien nach der einschlägigen Dienstvorschrift nicht berechtigt gewesen.

7 Im Hinblick auf seine langjährige Betriebszugehörigkeit, während derer das Arbeitsverhältnis beanstandungsfrei verlaufen sei, sei eine außerordentliche Kündigung nicht gerechtfertigt. Noch im Jahr 2003 sei ihm auf Grund seiner positiven Leistungen eine Leistungsprämie in Höhe von 2.000 Euro gewährt worden. Es handele sich weder um eine schwerwiegende, noch um eine hartnäckige Pflichtverletzung, so dass der Ausspruch einer Abmahnung nicht entbehrlich gewesen sei. Es liege auch kein das Ansehen der Beklagten schädigendes Verhalten vor. Es sei ihm nicht anzulasten, wenn die Beklagte ohne jeden vernünftigen Anlass die Kriminalpolizei einschalte. Die betriebsinternen Ermittlungen hätten der Schweigepflicht unterlegen. Es sei nicht davon auszugehen, dass eine Abmahnung fruchtlos gewesen wäre. Denn er habe sich an die Fachdienste für Arbeit und Integration Stiftung B gewandt. Er habe auch die Klärung seiner privaten Probleme in Angriff genommen. Die Beklagte beschäftige im Übrigen einen Beamten weiter, der in ähnlicher Weise Verfehlungen begangen habe.

8 Die Zwei-Wochen-Frist des § 626 Abs. 2 BGB sei nicht eingehalten worden. Mangels anerkannter oder offensichtlicher Schwerbehinderung sei die Einholung der Zustimmung des Integrationsamtes gar nicht erforderlich gewesen. Es sei ihm auch nicht verwehrt, sich auf die Nichteinhaltung der Zwei-Wochen-Frist zu berufen. Es wäre der Beklagten unbenommen gewesen, eine Kündigung vor Zustimmung des Integrationsamtes auszusprechen. Es werde auch bestritten, dass die Auswertung des Sachverhalts erst am 3. Juni 2004 erfolgt sei.

9 Der Kläger hat beantragt

festzustellen, dass das Arbeitsverhältnis zwischen den Parteien durch die außerordentliche Kündigung vom 29. Juni 2004, ihm zugegangen am 29. Juni 2004, nicht aufgelöst worden ist.

10 Die Beklagte hat Klageabweisung beantragt und vorgetragen, es sei ihr nicht zuzumuten, das Arbeitsverhältnis mit dem Kläger weiter fortzusetzen. Der Kläger habe in dem Zeitraum 8. März 2004 bis 13. Mai 2004 fast täglich, insgesamt in einem Umfang von ca. 50 Stunden, das Internet während seiner Arbeitszeit privat, insbesondere zum Besuch pornografischer Seiten genutzt. Es seien nur die Internetseiten berücksichtigt worden, die sich ohne Zweifel einer alleinigen privaten Nutzung zuordnen ließen. Es seien auch 11 temporäre Dateien mit kinderpornografischen Darstellungen auf dem PC des Klägers vorhanden gewesen. Da man jedoch nicht habe klären können, ob diese Dateien bewusst durch den Kläger angelegt worden seien, sei eine eventuelle Straftat bei der Kündigung nicht berücksichtigt worden. Der Kläger habe die ihm vorgeworfenen Pflichtverletzungen zunächst in einem persönlichen Gespräch mit der personalbearbeitenden Teamleiterin am 4. Juni 2004 bestritten, am 7. Juni 2004 dann jedoch eingeräumt. Die Dienstvereinbarung über die Arbeitszeit sehe keine Frühstückspause vor. Die Arbeitszeit könne erst ab 11.30 Uhr für die Mittagspause unterbrochen werden. Selbst wenn man die Mittagspause von den ermittelten 51 Stunden und 25 Minuten abziehen würde, verblieben 49 Stunden und 34 Minuten. Bei der Ermittlung des Umfangs der privaten Internetnutzung sei sie gemäß der einschlägigen Dienstvorschrift vorgegangen. Zunächst seien die Ermittlungen durch den IT-Sicherheitsbeauftragten zusammen mit dem zuständigen Referenten vorgenommen worden. Die Erkenntnisse seien dann dem dafür zuständigen Personalführungsteam zur Auswertung bezüglich der arbeitsrechtlichen Konsequenzen zur Verfügung gestellt worden.

11 Insgesamt sei ein wichtiger Grund gegeben. Es drohe für sie die konkrete Gefahr einer Rufschädigung. Zum einen hinterlasse jede Nutzung des Internets eine Spur, die es sachkundigen Dritten möglich mache festzustellen, von welchem Internetzugang aus auf eine bestimmte Homepage zugegriffen worden sei. Durch das Aufrufen bestimmter Webpages könne das Ansehen desjenigen, der den Internetzugang zur Verfügung stelle, erheblich leiden. Zum anderen hätten die staatsanwaltschaftlichen Ermittlungen tatsächlich stattgefunden. Die Gefahr der Rufschädigung sei spätestens zum Zeitpunkt der Aufnahme der

Ermittlungen durch die Kriminalpolizei konkret geworden. Der Kläger habe durch das Aufrufen bestimmter Internetseiten zumindest den automatischen Download ausgelöst, und der Verdacht einer Straftat gemäß § 184 StGB habe bestanden. Im Falle des Verdachts einer während der Dienstzeit begangenen Straftat sei sie als Bundesbehörde verpflichtet, den Sachverhalt den zuständigen Stellen entsprechend anzuzeigen. Zahlreiche Personen seien in die Aufklärung des Sachverhalts eingebunden gewesen. Es bedürfe daher nicht erst des Forums einer Hauptverhandlung, um die unstreitigen Vorfälle zu verbreiten und eine konkrete Gefahr der Rufschädigung für sie zu schaffen. Hinzu komme die in jedem Fall bereits jetzt gegebene Schädigung des Ansehens der Verwaltung innerhalb der Behörde selbst. Das Verhalten des Klägers sei geeignet, das Ansehen der Beklagten in der Öffentlichkeit erheblich zu beschädigen. Sie sei eine Bundesbehörde und Teil der zivilen Bundeswehrverwaltung. Sie habe insoweit eine Vorbildfunktion zu erfüllen. Auch das Verhalten des Klägers nach Ausspruch der Kündigung sei zu berücksichtigen. Er habe sich nicht einsichtig gezeigt und damit jegliche Basis für ein zukünftiges Vertrauensverhältnis entzogen.

12 Auch der Hinweis auf den vermeintlich vergleichbaren Fall eines Beamten rechtfertige kein anderes Ergebnis. Das Bundesdisziplinargesetz sehe andere, abgestufte Maßnahmen vor. Zudem habe es sich dort nicht um einen Sachverhalt gehandelt, der die Einschaltung der Kriminalpolizei notwendig gemacht habe.

13 Das Arbeitsgericht hat der Klage stattgegeben. Die Berufung der Beklagten blieb erfolglos. Mit der vom Landesarbeitsgericht zugelassenen Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter.

Entscheidungsgründe

14 Die Revision ist begründet.

15 A. Das Landesarbeitsgericht hat angenommen, ein wichtiger Grund zur fristlosen Kündigung liege nicht vor. Die fortgesetzten Pflichtverletzungen des Klägers durch seine private Internetnutzung rechtfertigten zwar an sich eine außerordentliche Kündigung. Der Kläger habe gegen das ausdrückliche und ihm auch bekannte Verbot der Privatnutzung verstoßen. Die Beklagte habe jedoch nicht dargelegt, dass der Kläger daneben seine Arbeitspflicht zusätzlich dadurch verletzt habe, dass er die ihm übertragenen Aufgaben nicht, nicht ordnungsgemäß oder nicht in der regulären Arbeitszeit erledigt habe. Eine Abmahnung sei angesichts des fast täglichen Verstoßes des Klägers gegen das ausdrückliche Verbot, das Internet zu privaten Zwecken zu nutzen, entbehrlich gewesen. Es handele sich um einen hartnäckigen und uneinsichtigen Verstoß gegen seine Vertragspflichten. Dabei sei auch zu berücksichtigen, dass sich der Kläger überwiegend pornografische Darstellungen angesehen habe. Dieser Umstand allein begründe allerdings nicht bereits einen zusätzlichen, gegen den Kläger zu berücksichtigenden Umstand im Rahmen der Interessenabwägung. Es seien der Beklagten keine zusätzlichen Kosten durch die private Internetnutzung entstanden. Unter Zugrundelegung des besonders strengen Maßstabes der tariflich zugesicherten Dauerstellung und insbesondere der langen unbeanstandeten Tätigkeit des Klägers sei davon auszugehen, dass der Beklagten die Weiterbeschäftigung des Klägers bis zum Ablauf der ordentlichen Beendigung zumutbar wäre. Die mit dem Auffinden der temporären Dateien mit kinderpornografischen Darstellungen unter Umständen verbundene Gefahr der Rufschädigung der Beklagten sei als gering einzustufen. Die Beklagte habe auch selbst die Gefahr einer Rufschädigung durch Einschaltung der Kriminalpolizei ausgelöst. Eine abstrakte Gefährdung des Ansehens der Beklagten reiche insoweit jedenfalls nicht aus.

16 B. Dem folgt der Senat nicht. Die Revision der Beklagten führt zur Aufhebung des Berufungsurteils und zur Zurückverweisung des Rechtsstreits an das Landesarbeitsgericht (§ 563 Abs. 1 ZPO). Die Revision rügt zu Recht eine fehlerhafte Anwendung des § 626 Abs. 1 BGB (§ 54 Abs. 1 BAT). Die vom Landesarbeitsgericht gegebene Begründung trägt nicht das Ergebnis, die Kündigung der Beklagten habe das Arbeitsverhältnis der Parteien nicht aufgelöst.

17

I. Gemäß § 626 Abs. 1 BGB kann ein Arbeitsverhältnis aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist gekündigt werden, wenn Tatsachen vorliegen, auf Grund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der Kündigungsfrist nicht zugemutet werden kann. Da der in § 626 Abs. 1 BGB verwendete Begriff des wichtigen Grundes ein unbestimmter Rechtsbegriff ist, kann seine Anwendung durch die Tatsachengerichte im Revisionsverfahren nur darauf überprüft werden, ob das Berufungsgericht den Rechtsbegriff selbst verkannt hat, ob es bei der Unterordnung des Sachverhalts unter die Rechtsnorm Denkgesetze oder allgemeine Erfahrungssätze

verletzt und ob es alle vernünftigerweise in Betracht kommenden Umstände, die für oder gegen die außerordentliche Kündigung sprechen, widerspruchsfrei beachtet hat *(st. Rspr. des Senats, vgl. zuletzt: BAG 25. März 2004 - 2 AZR 341/03 - AP BGB § 626 Nr. 189 = EzA BGB 2002 § 626 Nr. 6)* . Ebenfalls ist die Prüfung, ob auf Grund des Verhältnismäßigkeitsgrundsatzes vor Ausspruch einer Kündigung eine Abmahnung erforderlich ist, weitgehend Aufgabe der Tatsacheninstanz und unterliegt nur einer eingeschränkten revisionsrechtlichen Prüfung *(vgl. beispw. BAG 15. November 2001 - 2 AZR 605/00 - BAGE 99, 331)* .

18 II. Auch diesem eingeschränkten Prüfungsmaßstab hält das Berufungsurteil nicht stand. Das Landesarbeitsgericht hat bei der Beurteilung des wichtigen Grundes nicht alle fallrelevanten Umstände berücksichtigt.

19 1. Im Ausgangspunkt zutreffend geht das Landesarbeitsgericht von einer zweistufigen Prüfung des wichtigen Grundes aus *(vgl. beispw. Senat 17. Mai 1984 - 2 AZR 3/83 - AP BGB § 626 Verdacht strafbarer Handlung Nr. 14 = EzA BGB § 626 nF Nr. 90; 2. März 1989 - 2 AZR 280/88 - AP BGB § 626 Nr. 101 = EzA BGB § 626 nF Nr. 118; 14. September 1994 - 2 AZR 164/94 - BAGE 78, 18)* . Im Rahmen von § 626 Abs. 1 BGB ist zunächst zu prüfen, ob ein bestimmter Sachverhalt ohne die besonderen Umstände des Einzelfalls als wichtiger Kündigungsgrund an sich geeignet ist. Liegt ein solcher Sachverhalt vor, bedarf es der weiteren Prüfung, ob die Fortsetzung des Arbeitsverhältnisses unter Berücksichtigung der konkreten Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile zumutbar ist oder nicht.

20 2. Schon bei der Prüfung des wichtigen Grundes “an sich” hat das Landesarbeitsgericht nicht alle fallrelevanten Aspekte berücksichtigt.

21 a) Das Landesarbeitsgericht geht zwar zutreffend davon aus, dass ein Arbeitnehmer ganz erheblich gegen seine arbeitsvertraglichen Pflichten verstößt, wenn er ein ausdrückliches und fortlaufend wiederholtes Verbot des Arbeitgebers missachtet, das Internet privat zu nutzen und innerhalb von mehr als zwei Monaten fast täglich, insgesamt in erheblichem Umfang privat im Internet surft. Ein solch hartnäckiger und uneinsichtiger Verstoß gegen die Weisung des Arbeitgebers, nicht während der Arbeitszeit mit den Arbeitsmitteln private Dinge zu treiben, rechtfertigt, wie das Landesarbeitsgericht zutreffend annimmt, regelmäßig auch eine fristlose Kündigung ohne vorherige Abmahnung. Es greift jedoch zu kurz, wenn das Landesarbeitsgericht unter den gegebenen Umständen bei der Prüfung des wichtigen Grundes “an sich” entscheidend nur auf diesen Pflichtverstoß des Klägers abstellt.

22 b) Nach der Senatsrechtsprechung *(7. Juli 2005 - 2 AZR 581/04 - EzA BGB 2002 § 626 Nr. 10, auch zur Veröffentlichung in der Amtlichen Sammlung vorgesehen; 12. Januar 2006 - 2 AZR 179/05 -)* kommt als kündigungsrelevante Verletzung arbeitsvertraglicher Pflichten bei einer privaten Nutzung des Internets ua. in Betracht:

- das Herunterladen einer erheblichen Menge von Daten aus dem Internet auf betriebliche Datensysteme (“unbefugter download”), insbesondere wenn damit einerseits die Gefahr möglicher Vireninfizierungen oder anderer Störungen des - betrieblichen - Betriebssystems verbunden sein können oder andererseits von solchen Daten, bei deren Rückverfolgung es zu möglichen Rufschädigungen des Arbeitgebers kommen kann, beispielsweise weil strafbare oder pornografische Darstellungen heruntergeladen werden (*Hanau/Hoeren Private Internetnutzung durch Arbeitnehmer, S. 31; Mengel NZA 2005, 752, 753*);

  die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internetanschlusses als solche, weil durch sie dem Arbeitgeber möglicherweise - zusätzliche - Kosten entstehen können und der Arbeitnehmer jedenfalls die Betriebsmittel - unberechtigterweise - in Anspruch genommen hat;
- die private Nutzung des vom Arbeitgeber zur Verfügung gestellten Internets *während* der Arbeitszeit, weil der Arbeitnehmer während des Surfens im Internet zu privaten Zwecken seine arbeitsvertraglich geschuldete Arbeitsleistung nicht erbringt und dadurch seine Arbeitspflicht verletzt (*Kramer NZA 2004, 457, 459; Mengel NZA 2005, 752, 753*).

23 Das Landesarbeitsgericht hat sich hier schwerpunktmäßig nur mit der beharrlichen Missachtung des Verbots einer privaten Internetnutzung auseinander gesetzt und andere Pflichtverletzungen des Klägers nicht hinreichend gewichtet.

24 c) Das Landesarbeitsgericht hat insbesondere dem Umstand, dass der Kläger das Internet *während der Arbeitszeit* privat genutzt und damit seine arbeitsvertragliche Leistungspflicht verletzt hat, keine hinreichende Beachtung geschenkt.

25 Bei einer privaten Internetnutzung während der Arbeitszeit verletzt der Arbeitnehmer grundsätzlich seine (Hauptleistungs-) Pflicht zur Arbeit *(BAG 7. Juli 2005 - 2 AZR 581/04 - EzA BGB 2002 § 626 Nr. 10; Balke/Müller DB 1997, 326; Beckschulze DB 2003, 2777, 2781; Kramer NZA 2004, 457, 461; Mengel NZA 2005, 752, 753)* . Die private Nutzung des Internets darf die Erbringung der arbeitsvertraglich geschuldeten Arbeitsleistung nicht erheblich beeinträchtigen *(Däubler Internet und Arbeitsrecht 3. Aufl. Rn. 189; Hanau/Hoeren Private Internetnutzung durch Arbeitnehmer S. 29; Kramer NZA 2004, 457, 460)* . Die Pflichtverletzung wiegt dabei um so schwerer, je mehr der Arbeitnehmer bei der privaten Nutzung des Internets seine Arbeitspflicht in zeitlicher und inhaltlicher Hinsicht vernachlässigt.

26 Unstreitig hat der Kläger mehr als zwei Monate lang fast täglich das Internet in einem Umfang zwischen ca. 15 Minuten und knapp 3 Stunden verbotswidrig privat genutzt. In ca. zehn Wochen betrug die Zeit der privaten Internetnutzung mehr als eine Woche. Damit hat er seine Arbeitspflicht ganz erheblich verletzt, selbst wenn man mögliche Pausenzeiten berücksichtigt. Zu Unrecht stellt das Landesarbeitsgericht in diesem Zusammenhang darauf ab, es gebe keine Anhaltspunkte dafür, dass der Kläger nicht ordnungsgemäß gearbeitet habe. Die Beklagte hat hinreichend dargelegt, dass sich der Kläger die Zeiten, die er sich verbotswidrig ohne Kenntnis seines Arbeitgebers am Arbeitsplatz mit privaten Dingen beschäftigt hat, als Arbeitszeit hat bezahlen lassen. Anhaltspunkte dafür, dass ihm die Beklagte nicht in ausreichendem Umfang Arbeiten zugewiesen hat, hat der Kläger nicht vorgetragen. Unter diesen Umständen gehörte es nicht zur Darlegungslast der Beklagten, im Einzelnen vorzutragen, ob und inwiefern auch die Arbeitsleistung des Klägers unter seinen Privatbeschäftigungen während der Dienstzeit gelitten hat.

27 d) Es spricht auch nicht, wie das Landesarbeitsgericht wohl meint, zu Gunsten des Klägers, dass er der Beklagten durch die private Internetnutzung offenbar keine zusätzlichen Kosten verursacht hat. Der Pflichtverstoß besteht insoweit schon darin, dass der Kläger in großem Umfang entgegen einem ausdrücklichen und ihm gegenüber noch kurz zuvor wiederholten Verbot seine Arbeitsmittel dazu benutzt hat, privaten Tätigkeiten nachzugehen.

28 e) Auch die Ausführungen des Landesarbeitsgerichts zu einer möglichen Rufschädigung der Beklagten halten einer revisionsrechtlichen Überprüfung nicht stand. Die Gefahr einer Rufschädigung der Beklagten entstand bei der Art der Privatnutzung des Internets durch den Kläger allein dadurch, dass der Kläger umfangreich fast täglich die verschiedensten Internetseiten aufrief, um sich mit Pornografie zu beschäftigen. Der Senat hat schon im Urteil vom 7. Juli 2005 *(- 2 AZR 581/04 - EzA BGB 2002 § 626 Nr. 10)* darauf hingewiesen, dass allein die Befassung mit pornografischen Darstellungen die Gefahr einer Rückverfolgung an den Nutzer mit sich bringen und damit den Eindruck erwecken kann, eine Behörde, hier des Bundesministers der Verteidigung, befasse sich anstatt mit ihren Dienstaufgaben beispielsweise mit Pornografie.

29 Zu Unrecht geht das Landesarbeitsgericht davon aus, wenn ein staatsanwaltschaftliches Ermittlungsverfahren gegen den betreffenden Arbeitnehmer eingestellt worden sei, spiele es keine Rolle, welche Internetseiten angesehen bzw. heruntergeladen worden seien. Gerade die vom Kläger angesehenen und nach Behauptung der Beklagten heruntergeladenen Seiten pornografischen Inhalts stellten eine konkrete, als zusätzlichen Pflichtverstoß zu wertende Pflichtverletzung des Klägers dar. Auf die bloß strafrechtliche Bewertung des entsprechenden Pflichtverstoßes des Klägers durch die Staatsanwaltschaft kommt es entgegen der Ansicht des Landesarbeitsgerichts nach § 626 Abs. 1 BGB entscheidend nicht an.

30 f) Neben dieser eher abstrakten Gefahr einer Rufschädigung halten auch die Ausführungen des Landesarbeitsgerichts zu konkreteren Gefährdungen einer rechtlichen Überprüfung nicht stand. Die Gefahr, dass allein durch die Ermittlungen im Hause und das eingeleitete Strafverfahren die Verfehlungen des Klägers einem größeren Personenkreis zur Kenntnis gebracht werden mussten und eine verbreitete Kenntnis dieser Ermittlungen kaum zu vermeiden war, lag auf der Hand. Der bloße Hinweis auf die Schweigepflicht der ermittelnden Mitarbeiter reicht insoweit nicht aus, diese Gefahr zu zerstreuen. Außerdem hat der Kläger nach seinem eigenen Vorbringen bei seinem Dienst-PC die angeordneten Sicherheitsmaßnahmen umgangen, das Passwort auf dem Computer gespeichert und bei kürzeren Abwesenheitszeiten das Zimmer offen gelassen. Er geht selbst davon aus, dass dadurch der Zugriff fremder Personen auf seine Dateien und damit auf die gespeicherten Pornodateien möglich war. Schließlich kann es der Beklagten auch nicht, wovon offenbar das Landesarbeitsgericht ausgeht, zum Vorwurf gemacht werden, dass sie angesichts des Verdachtes, dass auf dem PC des Klägers kinderpornografische Seiten abgespeichert waren, durch ihre Anzeige ein staatsanwaltschaftliches Ermittlungsverfahren veranlasst und damit möglicherweise einer “Vertuschung” der Angelegenheit entgegengewirkt hat. Von einer Bundesbehörde, die durch eine gravierende Pflichtverletzung eines ihrer Arbeitnehmer erheblich geschädigt worden ist, kann nicht verlangt werden, dass sie von ihrer Pflicht,

derartige Vorfälle zur Anzeige zu bringen, nur absieht, um eine mögliche Schädigung ihres eigenen Rufs zu verhindern.

31 g) Nicht eingegangen ist das Landesarbeitsgericht zudem auf den Sicherheitsaspekt. Als Behörde, die Sicherheitsvorschriften unterliegt, musste die Beklagte ein besonderes Interesse daran haben, dass nicht sie oder einer ihrer Arbeitnehmer mit Dingen in Verbindung gebracht wurde, die den Verdacht nahe legten, sie seien strafrechtlich relevant.

32 h) Unberücksichtigt geblieben ist schließlich, dass dem Kläger nach dem zur Zeit der Kündigung geltenden § 8 Abs. 1 Satz 1 BAT gegenüber einem normalen Angestellten in der Privatwirtschaft gesteigerte Verhaltenspflichten oblagen. Der Angestellte hat sich nach dieser Vorschrift so zu verhalten, wie es von Angehörigen des öffentlichen Dienstes erwartet wird. Von einem Angestellten des Bundes ist nach § 8 Abs. 1 BAT zu erwarten, dass er sich nicht monatelang fast täglich zwischen ca. einer Viertelstunde und knapp drei Stunden mit Pornografie im Internet beschäftigt, anstatt seine Dienstpflichten zu erfüllen. Werden solche Verfehlungen bekannt und schreitet der öffentliche Dienstherr hiergegen nicht ein, so fällt dies auf die Behörde und damit auf den gesamten öffentlichen Dienst zurück. Wenn der Eindruck entstehen sollte, Mitarbeiter in zivilen Dienststellen der Bundeswehr beschäftigten sich anstatt mit Dienstaufgaben zu einem erheblichen Teil ihrer Arbeitszeit mit dem Betrachten von Pornoseiten im Internet, so ist ein solcher Eindruck dem Ansehen der Bundeswehr in der Öffentlichkeit insgesamt höchst abträglich *(vgl. BVerwG 8. November 2001 - 2 WD 29/01 - Buchholz 236, 1 § 17 SG Nr. 36)* .

33 3. Was die Interessenabwägung des Landesarbeitsgerichts anbelangt, so geht das Landesarbeitsgericht zu stark von dem Prüfungsmaßstab aus, den die Rechtsprechung zur außerordentlichen Kündigung mit notwendiger Auslauffrist entwickelt hat. Geht es um die Frage, ob dem Arbeitgeber die Weiterbeschäftigung des Arbeitnehmers notfalls bis zu dessen Pensionierung zumutbar ist oder nicht, kann die ordentliche Unkündbarkeit des Arbeitnehmers bei der Interessenabwägung dort in der Tat sowohl zu Gunsten als auch zu Lasten des Arbeitnehmers ins Gewicht fallen. Vorliegend geht es jedoch lediglich um eine fristlose Kündigung. Eine Umdeutung in eine außerordentliche Kündigung mit notwendiger Auslauffrist kommt schon mangels Durchführung des entsprechenden Beteiligungsverfahrens der Personalvertretung nicht in Betracht.

34 a) Bei der Prüfung der Frage, ob ein wichtiger Grund zur *fristlosen* Kündigung des Arbeitnehmers vorliegt, geht es allein um die Abwägung, ob die Fortsetzung des Arbeitsverhältnisses bis zum Ablauf der bei einem ordentlich unkündbaren Arbeitnehmer “fiktiven” Kündigungsfrist dem Arbeitgeber noch zugemutet werden kann. Bei dieser Prüfung besteht kein hinreichender Anlass, neben dem Alter und der Beschäftigungsdauer die ordentliche Unkündbarkeit des Arbeitnehmers erneut zu dessen Gunsten zu berücksichtigen und damit den ordentlich unkündbaren Arbeitnehmer besser zu stellen als einen Arbeitnehmer ohne diesen Sonderkündigungsschutz bei entsprechenden Einzelfallumständen und beiderseitigen Interessen *(so im Ansatz schon BAG 21. Januar 1999 - 2 AZR 665/98 - BAGE 90, 367)* .

35 b) § 53 Abs. 3 BAT schließt ausdrücklich nur die ordentliche Kündigung aus. Die außerordentliche Kündigung wird in § 54 BAT unter denselben Voraussetzungen zugelassen wie die außerordentliche Kündigung aller anderen Arbeitnehmer. § 55 BAT enthält zwar für unkündbare Arbeitnehmer Ausnahmeregelungen. Diese gelten aber ausdrücklich nur für dringende betriebliche Erfordernisse und bestimmte personenbedingte Kündigungsgründe. Die Tarifregelung enthält damit keinen Anhaltspunkt für einen Willen der Tarifpartner, selbst beim Vorliegen eines verhaltensbedingten wichtigen Grundes zur außerordentlichen fristlosen Kündigung den unkündbaren Arbeitnehmer besser zu behandeln als jeden anderen Arbeitnehmer *(vgl. BAG 10. Oktober 2002 - 2 AZR 418/01 - EzA BGB 2002 § 626 Unkündbarkeit Nr. 1)* .

36 c) Die Interessenabwägung hat sich damit im vorliegenden Fall entgegen der Auffassung des Landesarbeitsgerichts allein daran zu orientieren, ob bei einem vergleichbaren Arbeitnehmer ohne den Sonderkündigungsschutz nach § 53 Abs. 3, § 55 BAT unter denselben Umständen und bei entsprechender Interessenlage ein wichtiger Grund zur außerordentlichen Kündigung ohne Einhaltung der ordentlichen Kündigungsfrist anzunehmen wäre.

37 III. Der Rechtsstreit ist noch nicht entscheidungsreif.

38 Zu Teilen des entscheidungserheblichen Sachverhalts fehlen hinreichende tatsächliche Feststellungen des Berufungsgerichts. So ist insbesondere bislang ungeklärt, in welchem Umfang sich der Kläger während seiner Arbeitszeit mit Pornografie befasst hat und welche konkreten Dateien etwa kinder- oder tierpornografischen Inhalts der Kläger willentlich oder unwillentlich auf seinen Dienstcomputer heruntergeladen hat. Dies wird nach der Zurückverweisung nachzuholen sein.

39 Auch eine an dem zutreffenden Maßstab orientierte Interessenabwägung kann der Senat ohne Eingriff in den Beurteilungsspielraum der Tatsacheninstanz nicht vornehmen. Sollte sich das Vorbringen der Beklagten allerdings bestätigen, dass der Kläger in so erheblichem Umfang wie behauptet seine Arbeit vernachlässigt und auf seinem Dienstcomputer Dateien pornografischen Inhalts heruntergeladen hat, liegt nach den bisherigen Feststellungen des Landesarbeitsgerichts die Wertung nahe, dass die Interessen der Beklagten, sich vom Kläger zu trennen, das Bestandsschutzinteresse des Klägers überwiegen. Anders könnte dies allerdings zu beurteilen sein, wenn, wie der Kläger geltend macht, sein Fehlverhalten Krankheitswert hatte.

40 Liegt ein wichtiger Grund zur fristlosen Kündigung iSv. § 54 Abs. 1 BAT iVm. § 626 Abs. 1 BGB vor, so wird das Landesarbeitsgericht weiter zu prüfen haben, ob die Kündigung nach § 54 Abs. 2 BAT rechtzeitig erfolgt ist. Dabei wird es, da sich der Kläger nach dem bisherigen Aktenstand nach Treu und Glauben kaum auf die Verzögerung durch die Mitteilung von seinem Antrag auf Anerkennung als Schwerbehinderter wird berufen können, vor allem auf die Feststellung ankommen, zu welchem Zeitpunkt die Ermittlungen der Beklagten abgeschlossen waren.

Rost Bröhl Schmitz-Scholemann

Pitsch Sieg

Bayerisches Staatsministerium des Innern
Zentrale IuK-Leitstelle

BayITR-05

Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung

Version 1.0

Inhaltliche Ausgestaltung:

Diese Richtlinie wurde unter Federführung der Zentralen IuK-Leitstelle im Bayerischen Staatsministerium des Innern erarbeitet und im IuK-Fachausschuss abgestimmt.

Stand: 1. Juni 2006

Bezugsstelle:

Bayerischen Staatsministerium
des Innern
Zentrale IuK-Leitstelle
Odeonsplatz 3

80539 München

oder http://www.bybn.de/

Richtlinie über die Nutzung von Internet und E-Mail
in der bayerischen Staatsverwaltung
(BayITR-05)

(Stand: 1. Juni 2006)

Gestützt auf Nummer 5.2 der Richtlinie für den koordinierten Einsatz der Informations- und Kommunikationstechnik (IuK) in der bayerischen Staatsverwaltung (IuK-Koordinierungsrichtlinie – IuK-KoordR) vom 15. Juni 2004 (AllMBl S. 231), erlässt die Zentrale IuK-Leitstelle im Staatsministerium des Innern folgende Grundsätze für die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung.

1 Vorbemerkung

Die Nutzung von Angeboten im World-Wide-Web (WWW-Dienst) sowie das Senden und Empfangen von E-Mails (E-Mail-Dienst) gehört mittlerweile zu den nicht mehr hinweg zu denkenden Arbeitsmitteln in der täglichen Verwaltungspraxis. Im Rahmen der dienstlichen Aufgabenerfüllung dienen sie insbesondere der Förderung effizienter, interner und externer Kommunikationsbeziehungen sowie einer breiten und beschleunigten Informationsbeschaffung. Ohne diese elektronischen Kommunikationsdienste können die Aufgaben der Staatsverwaltung vielfach nicht mehr sach- und termingerecht erledigt werden. Angesichts der allgemeinen Gefahren im Zusammenhang mit der Nutzung elektronischer Kommunikationsdienste sind allerdings auch Kontrollen nötig, um einem möglichen Missbrauch nachgehen zu können, ohne dass gleichzeitig die schutzwürdigen Interessen der Nutzer verletzt werden. Um die Nutzung des WWW-Dienstes und des E-Mail-Dienstes auch für private Zwecke nicht generell und umfassend auszuschließen, ist daher dafür Sorge zu tragen, dass diese Rahmenvorgaben im Sinne eines Grundschutzes der Behörden ressortübergreifend beachtet werden.

2 Geltungsbereich

Diese Richtlinie gilt für alle Behörden, Gerichte und Hochschulverwaltungen des Freistaats Bayern sowie im Hinblick auf die an der zentralen Firewall erfolgenden Protokollierungen für alle Nutzer des Bayerischen Behördennetzes. Die besonderen Rechtsstellungen des Landtagsamts, des Obersten Rechnungshofs, des Landesbeauftragten für den Datenschutz sowie der Wissenschaft, Forschung, Lehre und Kunst werden hiervon nicht berührt.

3 Nutzungsregeln

(1) Der dienstlich bereitgestellte Internetzugang darf zur Nutzung von Angeboten im World-Wide-Web (WWW-Dienst) sowie zum Senden und Empfangen von E-Mails (E-Mail-Dienst) nur für dienstliche Zwecke verwendet werden.

(2) Abweichend von Absatz 1 können die obersten Dienstbehörden oder die von ihnen ermächtigten Behörden die Nutzung des WWW-Dienstes auch für private Zwecke (Privatnutzung) für einzelne Behörden oder Teile davon erlauben, sofern sie diese von der Einhaltung nachfolgender Nutzungsbedingungen abhängig machen:

- Die Beschäftigten, die den Internetzugang privat nutzen wollen, haben eine eigenhändig unterzeichnete Einwilligungserklärung gemäß dem Muster in der Anlage 1 abzugeben; diese ist zum Personalakt zu nehmen.
- Die Privatnutzung ist auf einen geringfügigen Umfang zu beschränken. Hiervon umfasst ist auch die Speicherung privater Daten und Downloads, sofern nicht die Sicherheit der IT-Systeme gefährdet ist.
- Die Privatnutzung darf nicht zur Verfolgung gewerblicher oder geschäftsmäßiger Interessen erfolgen; die Privatnutzung für Rechtsgeschäfte des täglichen Lebens kann zugelassen werden.
- Die Privatnutzung darf nicht zu Zwecken erfolgen, die die Interessen oder das Ansehen einer Behörde oder des Freistaats Bayern in der Öffentlichkeit oder die Sicherheit des Behördennetzes beeinträchtigen können. Insbesondere haben

- der Abruf kostenpflichtiger Internetseiten,
- das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen,
- Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver)

zu unterbleiben.

(3) Die Privatnutzung darf ferner nur gestattet werden, solange und soweit die uneingeschränkte Verfügbarkeit der betroffenen IT-Systeme für dienstliche Zwecke vorrangig gewährleistet bleibt und keine haushaltsrechtlichen Belange entgegenstehen.

(4) Wird die Privatnutzung des Internet erlaubt, so stellt dies eine freiwillige Leistung des Dienstherrn dar. Aus der Gestattung der Privatnutzung kann kein Rechtsanspruch der Beschäftigten hergeleitet werden. Die Gestattung der Privatnutzung kann jederzeit durch einseitige Erklärung widerrufen werden.

(5) Für die Nutzung des dienstlich bereitgestellten E-Mail-Dienstes zu privaten Zwecken (Privatnutzung) gelten diese Bestimmungen entsprechend. Generell unzulässig ist die Verwendung des intern genutzten Anmeldenamens (Benutzerkennung) und Anmeldepasswortes im Internet und der dienstlichen E-Mail-Adresse in öffentlichen „Chat-Räumen" und ähnlichen öffentlichen Meinungsforen. Es ist sicherzustellen, dass die Interessen oder das Ansehen einer Behörde oder des Freistaats Bayern in der Öffentlichkeit oder die Sicherheit des Behördennetzes durch die Privatnutzung nicht beeinträchtigt werden. Die Privatnutzung von E-Mail-Diensten über private Webmail-Angebote ist im Rahmen der erlaubten Privatnutzung der Web-Dienste möglich.

4 Kontrollen

(1) Zur Überwachung der Einhaltung der Nutzungsregelungen zu dienstlichen und privaten Zwecken können unter Beachtung des Verhältnismäßigkeitsprinzips sowie der personalvertretungs- und datenschutzrechtlichen Vorschrif-

ten und Vereinbarungen Missbrauchskontrollen (Stichproben- und Verdachtskontrollen) durchgeführt werden. Die Bestimmungen der datenschutzrechtlichen Freigabe für die Protokollierung der Internetzugriffe an der zentralen Firewall des Bayerischen Behördennetzes beim Landesamt für Statistik und Datenverarbeitung sind zu beachten (IMS vom 22.02.2001).

(2) Die Behörden, die die Privatnutzung erlauben, tragen die Verantwortung für die Einhaltung der Regelungen dieser Richtlinie. Die persönliche Verantwortlichkeit der Beschäftigten bleibt hiervon unberührt.

(3) Werden Vorkommnisse bekannt, die geeignet sind, die Interessen oder das Ansehen des Freistaats Bayern zu beeinträchtigen, so hat die verantwortliche Stelle umgehend geeignete Maßnahmen zur Aufklärung der Vorkommnisse zu ergreifen und erforderlichenfalls unverzüglich für Abhilfe zu sorgen.

(4) Die Durchführung von Protokollierungsmaßnahmen unterliegt stets der Mitbestimmung der Personalvertretung. Es wird empfohlen, die Protokollierung, Auswertung und Durchführung von Kontrollen behördenintern im Wege einer Dienstvereinbarung zu regeln.

herunterzuladen oder Beschränkungen für die Abwicklung von Rechtsgeschäften des täglichen Lebens.>

Eine Trennung zwischen dienstlicher und privater Nutzung ist technisch nicht möglich. Die Privatnutzung kann daher nur den Beschäftigten erlaubt werden, die einwilligen, dass ihre gesamten Internetzugriffe (ggf. ergänzen um "sowie der gesamte E-Mail-Verkehr") protokolliert werden und dass – stichprobenartig oder im Einzelfall bei konkretem Verdacht einer missbräuchlichen Nutzung – überprüft werden kann, ob sich die Zugriffe auf die oben beschriebenen unzulässigen Inhalte beziehen. Die Beschäftigten müssen bei privater E-Mail-Nutzung auch damit einverstanden sein, dass virenverseuchte E-Mails und unerwünschte Werbung (Spam) wie dienstliche E-Mails behandelt werden und gegebenenfalls gelöscht werden. Bei eingehenden privaten E-Mails muss damit gerechnet werden, dass diese von anderen Bediensteten im Rahmen der Erledigung dienstlicher Aufgaben (z.B. Vertretung, Systemadministrator) zur Kenntnis genommen werden. Auf die Bestimmungen der datenschutzrechtlichen Freigabe für die Protokollierung der Internetzugriffe an der zentralen Firewall des Bayerischen Behördennetzes beim Landesamt für Statistik und Datenverarbeitung (IMS des StMI vom 22.02.2001) wird hingewiesen. Wer von der Möglichkeit der Privatnutzung in dem beschriebenen Umfang Gebrauch machen will, übersendet die folgende Einwilligungserklärung an das Sachgebiet ...
Dieses Schreiben ergeht mit Zustimmung des Personalrats (oder: Dieses Schreiben entspricht der Dienstvereinbarung mit dem Personalrat vom ...)."

II. Die eigenhändig unterzeichnete Einwilligungserklärung des Beschäftigten lautet wie folgt:

Einwilligungserklärung

„Ich möchte von dem Angebot meiner Dienststelle Gebrauch machen, Web-Dienste (WWW-Dienst, E-Mail-Dienst) (ggf.nur WWW-Dienst) in geringfügigem Umfang auch für private Zwecke zu nutzen, z.B. für die Internetrecherche. Mir

ist bekannt, dass jede Nutzung unzulässig ist, durch die gewerbliche oder geschäftsmäßige Interessen verfolgt werden oder die den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit schaden oder die Sicherheit des Behördennetzes beeinträchtigen kann. Dies gilt vor allem für das Abrufen oder Verbreiten von Inhalten, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenz- oder urheberrechtliche Bestimmungen verstoßen. Dies gilt weiter für das Abrufen oder Verbreiten von verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden, pornographischen, beleidigenden oder verleumderischen Inhalten.

<Ggf. ergänzen um weitere organisatorische Einschränkungen>

Ich willige ein, dass auch meine privaten – also nicht nur die dienstlichen – Internetzugriffe (ggf. ergänzen um "sowie der gesamte dienstliche und private E-Mail-Verkehr") protokolliert werden und dass die Protokolldaten stichprobenartig oder im Einzelfall bei konkretem Verdacht einer missbräuchlichen Nutzung überprüft werden können, um eine missbräuchliche Nutzung feststellen zu können. Ich willige ferner ein, dass meine privaten E-Mails hinsichtlich der Behandlung virenverseuchter E-Mails und unerwünschter Werbung (Spam) wie die dienstlichen E-Mails behandelt werden und gegebenenfalls gelöscht werden. Mir ist bekannt, dass meine Dienststelle die Gestattung der Privatnutzung jederzeit widerrufen kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen mit der Folge, dass ich ab Widerruf die Internetzugriffsmöglichkeit nicht mehr privat nutzen darf.

Diese Einwilligungserklärung wird in den Personalakt aufgenommen."

Alexander Roßnagel 20.11.2006

Vorhaltung von Einrichtungen zur TK-Überwachung in der Universität Kassel

Inwieweit kann die Universität Kassel TK-Zugänge für An-Institute oder Studierende von Weiterbildungsstudiengängen oder Partneruniversitäten anbieten, ohne Einrichtungen zur TK-Überwachung vorhalten und betreiben zu müssen? Vielfach sollen diese zum Beispiel auf Inhalte zugreifen können, die auf Inhaber eines UniK-Accounts beschränkt sind.

1. Telekommunikationsdienste für die Öffentlichkeit

Ausgangspunkt sind § 110 Abs. 1 Satz 1 TKG und § 3 Abs. 1 Satz 1 TKÜV. Nach diesen Vorschriften besteht die Pflicht, Einrichtungen zur TK-Überwachung vorzuhalten nur dann, wenn die Universität Kassel „Telekommunikationsdienste für die Öffentlichkeit" erbringt.

Für die Öffentlichkeit erbracht wird ein TK-Dienst, wenn er grundsätzlich für jeden aus einer unbeschränkten Anzahl möglicher Nutzer angeboten wird. Im neuen Telekommunikationsgesetz ist der Begriff „Telekommunikationsdienste für die Öffentlichkeit" nicht definiert. Im alten Telekommunikationsgesetz war der Begriff „Telekommunikationsdienstleistungen für die Öffentlichkeit" in § 3 Nr. 19 TKG wie folgt definiert: „das gewerbliche Angebot von Telekommunikation ... für beliebige natürliche und juristische Personen und nicht lediglich für die Teilnehmer geschlossener Benutzergruppen". Es ist davon auszugehen, dass der Gesetzgeber hinsichtlich des Begriffs der Öffentlichkeit im neuen Telekommunikationsgesetz keine Änderung einführen wollte.[1]

Kein Dienst für die Öffentlichkeit besteht somit, wenn nur eine beschränkte Anzahl von Teilnehmern ihn nutzen kann. Von einem eingeschränkten Teilnehmerkreis ist jedenfalls dann auszugehen, wenn der Kreis der Teilnehmer nach einem nachvollziehbaren Kriterium (zu einem bestimmten Zweck) beschränkt ist. Er muss nicht auf den Anbieter beschränkt sein. Insbesondere besteht eine geschlossene Benutzergruppe auch dann, wenn weitere juristische und natürliche Personen in den geschlossenen Teilnehmerkreis – zur Verfolgung eines gemeinsamen Ziels – aufgenommen werden.[2]

Für die Universität Kassel bedeutet dies, dass sie jedenfalls dann keine „Telekommunikationsdienste für die Öffentlichkeit" erbringt, wenn ihr Angebot von Telekommunikationsdiensten (satzungsgemäß und tatsächlich) auf Personen beschränkt ist, die bezogen auf die gesetzlichen Aufgaben der Hochschule objektiv in einem besonderen Verhältnis zu dieser stehen und auf den TK-Dienst angewiesen sind, um hinsichtlich dieser Aufgabe mit der Hochschule kommunizieren zu können.

---

1 Bock, Beck'scher TKG-Kommentar, 3. Aufl. München 2000, § 110 Rn. 9.

2 Schütz, in: Beck'scher TKG-Kommentar, 2. Aufl. München 2000, § 3 Rn. 22 für die geschlossenen Benutzergruppen in Konzernen und Unternehmenskooperationen.

Aufgaben der Hochschule sind

- Ausbildung (§§ 3, 16 ff. HHG – auch (internationale) Zusammenarbeit in Lehre und Studium)
- Weiterbildung (§§ 3, 21 HHG – in enger Kooperation mit der Praxis)
- Forschung (§§ 3, 35 ff. HHG – auch (internationale) Forschungskooperation) und
- Wissenstransfer (§ 3 HHG – in enger Kooperation mit der Praxis)

Dementsprechend sind neben den Mitgliedern und Angehörigen der Universität Kassel (§ 8 HHG) folgende Personengruppen sowohl von diesen Aufgaben erfasst als auch zahlenmäßig beschränkt:

- Ausbildung: Studierende in kooperierenden Studiengängen und Lehrveranstaltungen, Gasthörer, Gaststudierende, Lehrbeauftragte
- Weiterbildung: Studierende in Weiterbildungsstudiengängen der Universität Kassel oder in verselbständigten Weiterbildungsinstitutionen der Universität Kassel, Lehrbeauftragte
- Forschung: An-Institute der Universität Kassel, Gastwissenschaftler, Kooperationspartner aus anderen Forschungsinstituten oder von Praxispartnern
- Wissenstransfer: Institutionen des Wissenstransfers der Universität Kassel und die Teilnehmer an deren Veranstaltungen

In einigen Fällen kann es geboten sein, die Rechte der Zugelassenen auf bestimmte Dienste der Universität Kassel zu begrenzen (etwa E-Mail und E-Learning, aber kein Telefon). Grundsätzlich ist ein Angebot, das sich auf den beschriebenen Kreis von Nutzern beschränkt kein Angebot von Telekommunikationsdiensten für die Öffentlichkeit.

Als problematisch wird teilweise angesehen, Telekommunikationsdienst allen ehemaligen Studierenden anzubieten.[3] Diese Skepsis muss jedoch angesichts der ausdrücklichen Aufgabe in § 3 Abs. 5 HHG in Frage gestellt werden, zu ihren Absolventinnen und Absolventen in Verbindung zu bleiben und die Vereinigung Ehemaliger zu fördern.

Ein Angebot für die Öffentlichkeit wäre unstrittig zum Beispiel ein frei zugänglicher WLAN-Zugang zum Internet auf dem Universitätsgelände.

---

[3] So vorsichtig Helf (Bundesnetzagentur) nach einem Bericht von Hartenstein, Zwischen Überwachungsverordnung und Datenschutz, RZ-News der Universität Karlsruhe, November/Dezember 2005, 6.

2. Beschränkung der Vorhaltungspflicht

Selbst wenn eine Teil der Teilnehmer, die Telekommunikationsdienste der Universität Kassel nutzen, sind folgende Einschränkungen der Pflicht, Einrichtungen zur TK-Überwachung vorhalten zu müssen, zu beachten:

Bietet die Universität Kassel Telekommunikationsdienste sowohl für einen geschlossenen Benutzerkreis als auch für die Öffentlichkeit an, fallen nach § 3 Abs. 1 Satz 2 TKÜV nur die Dienstleistungen und Anschlüsse, die für die Öffentlichkeit angeboten werden, unter die Pflicht des § 110 TKG und der TKÜV.

Diese Pflicht besteht nach § 3 Abs. 2 Nr. 5 TKÜV nicht, wenn nicht mehr als 1000 Nutzungsberechtigte angeschlossen sind.

Sollte in Grenzfällen die Bundesnetzagentur die geschlossene Benutzergruppe als überschritten ansehen und sollte der Teilnehmerkreis diese überschreitenden Teilnehmer die Zahl von 1000 überschreiten, kann die Universität Kassel das Angebot an diese Teilnehmer auf eine Zahl von unter 1000 beschränken.

3. Zusammenfassung

Die Universität Kassel kann Telekommunikationsdienstleistungen an die unter 1. genannten Personen anbieten (und darüber hinaus an bis zu 1000 Teilnehmer aus der Öffentlichkeit), ohne der Pflicht zu unterliegen, Einrichtungen zur TK-Überwachung vorhalten und betreiben zu müssen.