



Datensicherheit und Haftung

E-Business und Internet im Unternehmen

Dr. Astrid Auer-Reinsdorff
Rechtsanwältin, Berlin



IT/TK-Risk-Management im Unternehmen

- Haftung / Verantwortlichkeit
- Mitarbeiter und Kooperationen
- Datenschutz
- Anbieterkennzeichnung / Impressum
- Verbraucherschutz
- Schutzrechte (Inhalte, Marken etc.)



IT/TK-Risiko-Management nach KonTraG*:

§ 91 Absatz 2 KonTraG:

„...der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

gilt entsprechend für andere Gesellschaftsformen, für die GmbH-Geschäftsführer über § 43 Absatz 2 GmbHG – „Sorgfalt eines ordentlichen Kaufmanns“

*Gesetz zur Kontrolle und der Transparenz im Unternehmensbereich, 27.04.1998



IT/TK-Risiko-Management für die GmbH:

§ 43 GmbHG:

„(1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.

(2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden. ... “



Regelkreis des IT/TK-Risk-Managements

- **Festlegung der Risikopolitik**
Sicherung der Unternehmensziele
Sicherung des Erfolgs des Unternehmens
Senkung der Risikokosten
- **Risikoidentifikation**
- **Risikobewertung**
- **Risikosteuerung und –kontrolle**
- **Notfallplan**



Schutzziele des IT/TK-Risk-Managements

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Zurechenbarkeit
- Vermeidung von Imageschäden



Verfügbarkeit der IT und der Daten

- Hardware
- Software
- Pflege und Support
- Datensicherung
- Zugriff
- IT-Grundschutz-Konzept (www.bsi.de)



Vertraulichkeit der Kommunikation

- Datenschutz / Datenschutzbeauftragter
- Geheimhaltungs-/
Vertraulichkeitsvereinbarungen
- Verschlüsselung
- Zugriffskontrolle
- Passwortmanagement



Gegenstand des Schutzes

- Datengeheimnis oder Geheimhaltung aufgrund vertraglicher Vereinbarung
- personenbezogene Daten - BDSG
- wettbewerbsrechtlicher Schutz der Geschäfts- / Betriebsgeheimnisse - § 17 Absatz 1 UWG
- Strafrechtlicher Schutz gegen die Weitergabe durch Geheimnisträger – § 203 StGB
- Schutz von Immaterialgüterrechten



Sicherheitslücken bei Email und WLAN

interne Dokumente / Konzepte etc. verlieren mit der Zugriffsmöglichkeit den Schutz als Geschäftsgeheimnisse

- kein strafrechtlicher Schutz
- geringer Schutz nach § 17 UWG
- kein Schutz durch Geheimhaltungsvereinbarung, da zugänglich
- durch Verbreitung evtl. Verlust von Verwertungsmöglichkeiten
- evtl. Verlust der für den Patent-/ Geschmacksmusterschutz erforderlichen „Neuheit“



Fünftehnter Abschnitt des Strafgesetzbuches (StGB) Verletzung des persönlichen Lebens- und Geheimbereichs

StGB § 201 Verletzung der Vertraulichkeit des Wortes

StGB § 201a Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

StGB § 202 Verletzung des Briefgeheimnisses

StGB § 202a Ausspähen von Daten

StGB § 203 Verletzung von Privatgeheimnissen

StGB § 204 Verwertung fremder Geheimnisse

StGB § 205 Strafantrag

StGB § 206 Verletzung des Post- oder Fernmeldegeheimnisses

StGB §§ 207 bis 210



StGB § 202a 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.**



StGB § 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

- 1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,**
- 2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,**
- 3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,**
- 4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist.**
 - 4a. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,**
- 5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder**
- 6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle**

anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.



StGB § 204 Verwertung fremder Geheimnisse

- (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.**

- (2) § 203 Abs. 4 gilt entsprechend.**



StGB § 205 Strafantrag

- (1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 201a bis 204 wird die Tat **nur auf Antrag** verfolgt.**
- (2) Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen des § 202a. Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß.**



StGB § 206 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.



UWG 2004 § 17 Verrat von Geschäfts- und Betriebsgeheimnissen

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.



UWG 2004 § 17 Verrat von Geschäfts- und Betriebsgeheimnissen

- (2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,**
- 1. sich ein Geschäfts- oder Betriebsgeheimnis durch**
 - a) Anwendung technischer Mittel,**
 - b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder**
 - c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist, unbefugt verschafft oder sichert oder**
 - 2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.**



UWG 2004 § 17 Verrat von Geschäfts- und Betriebsgeheimnissen

- (3) Der Versuch ist strafbar.**
- (4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter**
 - 1. gewerbsmäßig handelt,**
 - 2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder**
 - 3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.**
- (5) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.**
- (6) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.**



Sicherheitslücken bei Email und WLAN

interne Dokumente / Konzepte etc. büßen die ökonomische Verwertbarkeit ein

- keine oder eingeschränkte Kontrollmöglichkeit der Verbreitung und Nutzung durch Dritte
- Gefahr der Übernahme der Inhalte durch Dritte und Verbreitung unter deren Namen
- erschwerte Nachweisbarkeit der Urheberschaft



Sicherheitslücken bei Email und WLAN

Zugriff auf Kundendaten

- Schadensersatzpflicht gegenüber den Kunden wegen der Verpflichtung zur Datensicherung - § 9 BDSG
- Imageschaden
- Ordnungswidrigkeit nach § 7 BDSG



Bundesdatenschutzgesetz (BDSG)

§ 4 Zulässigkeit der Datenverarbeitung und -nutzung

- (1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.**
- (2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie 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 die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.**
- (3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2 Satz 2 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.**



BDSG § 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt 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.



BDSG § 6 Unabdingbare Rechte des Betroffenen

- (1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.
- (2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsbeauftragt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. Die in § 19 Abs.3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs.6.



BDSG § 8 Schadensersatz durch nicht-öffentliche Stellen

Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung geltend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.



BDSG § 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.



Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

- Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
- zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
- die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
- zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
- zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
- die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).



Sicherheitslücken bei Email und WLAN

Löschen von Daten / Know-how

- Vertragliche Haftung bei Daten Dritter
- Vermögensschaden
- Ggf. vertragliche Schadensersatzpflicht aus nicht ordnungsgemäßer Erfüllung (Verspätung; Unmöglichkeit etc.)



Sicherheitslücken bei Email und WLAN

Verwertung von urheberrechtlich geschützten Daten / Know-how etc.

- Schadensersatzpflicht bei Daten Dritter
- Vermögensschaden



Integrität und Zurechenbarkeit

- Elektronische Signatur
- Anbieterkennzeichnung (TDG)
- Redaktionelle Verantwortlichkeit (MDStV)



Anbieterkennzeichnung / Impressum

- Name / Firma
- Anschrift
- Kommunikationsdaten: Email und Telefon
- Umsatzsteueridentifikationsnummer (falls vorhanden)
- Geschäftsführer / Vorstand
- Handelsregisterdaten (HR-Nummer und Amtsgericht)
- [redaktionell Verantwortliche – MDStV]



Anbieterkennzeichnung / Impressum

- „Kontakt / Über Uns / Impressum / Unternehmen“
- leicht auffindbar auf der Site
- maximal zwei Klicks
- Druckversion (fakultativ)
- Urheberrechtsvermerk (fakultativ)



Verantwortlichkeit §§ 8 - 11 TDG

„§ 8 Teledienstegesetz:

I: Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, auch den allgemeinen Gesetzen verantwortlich.

II: Diensteanbieter im Sinne der §§ 9 bis 11 sind nicht verpflichtet, die von Ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieter nach den §§ 9 bis 11 unberührt. ...“



Verantwortlichkeit §§ 8 - 11 TDG

- § 9 Durchleitung von Informationen
- § 10 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen
- § 11 Speicherung von Informationen
- keine spezielle Regelung für Hyperlinks und Suchmaschinen



Haftung aufgrund der Internetarbeitsplätze

Rechtmissbräuchliche Nutzung:

- Empfangen/Versenden rechtswidriger Inhalte vom Arbeitsplatz aus
- Urheberrechtsverletzungen z.B. Teilnahme an Musiktaschbörsen
- Lizenzrechtsverletzungen z.B. Softwarekopien
- Computerstraftatbestände
Ausspähen von Daten § 202 a StGB
Datenveränderung § 303 a StGB
Computersabotage § 303 b StGB
- Vertragswidrige Nutzung von Daten, Informationen etc.



Haftung für die Kommunikation über Internetarbeitsplätze

- § 278 BGB – Haftung für Erfüllungsgehilfen
Einstandpflicht im Rahmen der Vertragserfüllung
- § 831 BGB – Haftung für Verrichtungsgehilfen
Exkulpationsmöglichkeit = dezentralisierter Entlastungsbeweis der sorgfältigen Auswahl und Überwachung des Mitarbeiters
- § 823 I BGB - Organisationsverschulden
Sicherheitsvorkehrungen wurden in vorwerfbarer Weise nicht getroffen
- § 31 BGB – Organhaftung
Haftung der verfassungsmäßig berufenen Vertreter
- § 830 BGB – Mittäterschaft / Beihilfe
z.B. Dulden von Rechtsverstößen mit ökonomischem Mehrwert
- Störerhaftung – Gewerbliche Schutzrechte
Unterlassungs-, Beseitigungs- und ggf. Schadensersatzansprüche
§ 101, 1 UrhG; § 14 VII MarkenG; § 13 IV UWG a.F.



Überwachung der Internetarbeitsplätze

Exkulpation, wenn planmäßige, unauffällige Überwachungen – mit unerwarteten Kontrollen – vorgesehen sind sowie Belehrungen über Gefahren und erforderliche Verhaltensmaßregeln erfolgen.

- IT-Policies, Dienstanweisungen, Betriebsvereinbarungen, arbeitsvertragliche Vereinbarungen
- Einsatz von Filtertechnologien



Überwachung <=> Private Nutzung ?

1. Ausschließlich dienstliche Nutzung
2. Nutzung auch zu privaten Zwecken erlaubt
3. Einrichtung einer separaten privaten Email-Adresse für die Mitarbeiter

Erlaubte private Nutzung => Anforderungen wegen des Schutzes des Fernmeldegeheimnisses (§ 85 TKG)
=> Erforderlichkeit der Einwilligung der Mitarbeiter



Haftung für die Weiterverbreitung von Viren durch E-Mails

In Betracht kommen neben vorsätzlichen Handlungen:

- deliktische Verkehrssicherungspflichten und Schadensersatz nach § 823 I BGB
- vertragliche Schutzpflichten nach § 242 BGB

des Unternehmers gegenüber dem Verbraucher.



Haftung für die Weiterverbreitung von Viren durch E-Mails

Bei der Beurteilung der Haftung sind im Sinne einer Interessensabwägung zu berücksichtigen:

- Berechtigte Erwartungen des E-Mail Empfängers (Vorteilsziehung durch den Versender, berechtigtes Vertrauen in verkehrsgerechtes Verhalten)
- Berechtigte Erwartungen des E-Mail Versenders (Vertrauensschutz hinsichtlich der Gefahrvermeidung durch Selbstschutz gemessen am Ausmaß der Gefahr und den technischen Möglichkeiten und dem finanziell Zumutbaren; Einschätzung des Schadensrisikos nur durch den Empfänger)
- Rechtmäßiges Alternativverhalten wegen Neuartigkeit des Virus, Trojanischen Pferd etc.



Elfter Teil Telekommunikationsgesetz (TKG) Fernmeldegeheimnis, Datenschutz, Sicherung

TKG § 85 Fernmeldegeheimnis

**TKG § 86 Abhörverbot, Geheimhaltungspflicht der
Betreiber von Empfangsanlagen**

TKG § 87 Technische Schutzmaßnahmen

**TKG § 88 Technische Umsetzung von
Überwachungsmaßnahmen**

TKG § 89 Datenschutz

**TKG § 91 Kontrolle und Durchsetzung von
Verpflichtungen**

TKG § 92 Auskunftspflicht

TKG § 93 Staatstelekommunikationsverbindungen



TKG § 85 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 verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. 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 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) ...**



TKG § 86 Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

Mit einer Funkanlage dürfen Nachrichten, die für die Funkanlage nicht bestimmt sind, nicht abgehört werden. Der Inhalt solcher 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 § 85 besteht, anderen nicht mitgeteilt werden. § 85 Abs. 4 gilt entsprechend. Das Recht, Funkaussendungen zu empfangen, die für die Allgemeinheit oder einen unbestimmten Personenkreis bestimmt sind, sowie das Abhören und die Weitergabe von Nachrichten auf Grund besonderer gesetzlicher Ermächtigung bleiben unberührt.



TKG § 87 Technische Schutzmaßnahmen

- (1) Wer Telekommunikationsanlagen betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dienen, hat bei den zu diesem Zwecke betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze**
- 1. des Fernmeldegeheimnisses und personenbezogener Daten,**
 - 2. der programmgesteuerten Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe,**
 - 3. gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen, und**
 - 4. von Telekommunikations- und Datenverarbeitungssystemen gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Dabei ist der Stand der technischen Entwicklung zu berücksichtigen. Die Regulierungsbehörde erstellt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik nach Anhörung von Verbraucherverbänden und von Wirtschaftsverbänden der Hersteller und Betreiber von Telekommunikationsanlagen einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen, um eine nach dem Stand der Technik und internationalen Maßstäben angemessene Standardsicherheit zu erreichen. Dem Bundesbeauftragten für den Datenschutz ist Gelegenheit zur Stellungnahme zu geben. Der Katalog wird von der Regulierungsbehörde im Bundesanzeiger veröffentlicht. Der für die Schutzmaßnahmen zu erbringende technische und wirtschaftliche Aufwand ist von der Bedeutung der zu schützenden Rechte und der zu sichernden Anlagen für die Allgemeinheit abhängig.**
- (2) Lizenzpflichtige Betreiber von Telekommunikationsanlagen haben einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen, aus dem hervorgeht, ...**



TKG § 88 Technische Umsetzung von Überwachungsmaßnahmen

- (1) Die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation sind von dem Betreiber der Telekommunikationsanlage auf eigene Kosten zu gestalten und vorzuhalten.**
- (2) Die technische Gestaltung dieser Einrichtungen bedarf bei Betreibern von Telekommunikationsanlagen, die gesetzlich verpflichtet sind, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, der Genehmigung der Regulierungsbehörde. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf,...**

www.regtp.de – Umsetzung im Unternehmen bis 31.12.2004



e-shop und Verbraucherschutz

- Produktbeschreibung
- Preisangabenverordnung
- Gestaltung des Bestellvorgangs
- Verwaltung der Kundendaten
- Widerrufs- oder Rückgaberecht



Welche Rechte können berührt sein ?

- Rechte der Urheber / Leistungsschutzberechtigten
- Rechte der Hersteller
- Bildnisrechte / Persönlichkeitsrechte
- Marken- und Namensrechte
- Titelrechte
- Wettbewerbsrecht
- Technische Schutzrechte
- Datenschutzrecht
- Verbraucherschutzrechte
- Strafrecht / Ordnungswidrigkeitenrecht ...



Security Day 2004

T-Com Geschäftskunden Center Berlin

28. September 2004



URHEBERRECHTSVERMERK:

Diese Datei / Präsentation wird zur Information auf der Website der Autorin zur reinen Information bereit gehalten. Der Download, die Vervielfältigung, Verbreitung oder andere Verwertung auch auszugsweise ist nicht gestattet. Zitate aus dieser Präsentation müssen unter Hinweis auf die Autorin Dr. Astrid Auer-Reinsdorff erfolgen.

© Dr. Auer-Reinsdorff, Berlin 09/2004

Vielen Dank für Ihre Aufmerksamkeit

Dr. Astrid Auer-Reinsdorff
www.dr-auer.de

Johannisstraße 20, 10117 Berlin-Mitte

Fon: 030 – 726 19 4014, Mail: kanzlei@dr-auer.de