Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Administratoren im Paragrafendschungel (IT-Recht für Admins)

Berlin, 26.06.2015

Referent: Michael Stolze LL.M. LL.M

Rechtsanwalt / Datenschutzbeauftragter (TÜV®)

Master of Laws – IT-Recht & Recht des Geistigen Eigentums (Hannover)

Master of Laws – Information and Communication Technology Law (Oslo)

Empfehlungen

Praxisrelevante Hilfsmittel

Veröffentlichungen der datenschutzrechtlichen Aufsichtsbehörden bzw. des sog. „Düsseldorfer Kreises“

http://www.datenschutz-berlin.de/content/veroeffentlichungen

Publikationen von BITKOM **www.bitkom.org**

Skript „Internetrecht“ von Prof. Hoeren

https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien

Generatoren Datenschutzerklärung / Impressum

IT-Recht

1. Vertragsrecht der Informationstechnologien, einschließlich der Gestaltung individueller Verträge und AGB,
2. Recht des elektronischen Geschäftsverkehrs, einschließlich der Gestaltung von Provider-Verträgen und Nutzungsbedingungen (Online-/Mobile Business),
3. Grundzüge des Immaterialgüterrechts im Bereich der Informationstechnologien, Bezüge zum Kennzeichenrecht, insbesondere Domainrecht,
4. Recht des Datenschutzes und der Sicherheit der Informationstechnologien einschließlich Verschlüsselungen und Signaturen sowie deren berufsspezifischer Besonderheiten,
5. Das Recht der Kommunikationsnetze und -dienste, insbesondere das Recht der Telekommunikation und deren Dienste,
6. Öffentliche Vergabe von Leistungen der Informationstechnologien (einschließlich e-Government) mit Bezügen zum europäischen und deutschen Kartellrecht,
7. Internationale Bezüge einschließlich Internationales Privatrecht,
8. Besonderheiten des Strafrechts im Bereich der Informationstechnologien
9. Besonderheiten der Verfahrens- und Prozessführung.

vgl. § 14k Fachanwaltsordnung zu den nachgewiesenen Kenntnissen für den Fachanwalt für IT-Recht

IT-Recht für Admins?

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

IT-Recht

1. Vertragsrecht der Informationstechnologien, einschließlich der Gestaltung individueller Verträge und AGB,
2. Recht des elektronischen Geschäftsverkehrs, einschließlich der Gestaltung von Provider-Verträgen und Nutzungsbedingungen (Online-/Mobile Business),
3. Grundzüge des Immaterialgüterrechts im Bereich der Informationstechnologien, Bezüge zum Kennzeichenrecht, insbesondere Domainrecht,
4. Recht des Datenschutzes und der Sicherheit der Informationstechnologien einschließlich Verschlüsselungen und Signaturen sowie deren berufsspezifischer Besonderheiten,
5. Das Recht der Kommunikationsnetze und -dienste, insbesondere das Recht der Telekommunikation und deren Dienste,
6. Öffentliche Vergabe von Leistungen der Informationstechnologien (einschließlich e-Government) mit Bezügen zum europäischen und deutschen Kartellrecht,
7. Internationale Bezüge einschließlich Internationales Privatrecht,
8. Besonderheiten des Strafrechts im Bereich der Informationstechnologien
9. Besonderheiten der Verfahrens- und Prozessführung

IT-Recht für Admins!

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Agenda

1. **Der Paragrafendschungel, unübersichtlich und gefährlich**
2. **Rechte aus Pflichten nach TMG**
3. **Urheberrecht**
4. **Straf- und haftungsrechtliche Risiken für Admins**

PAUSE

5. **IT-Sicherheitsgesetz**
6. **Datenschutz**
    1. **Grundlinien**
    2. **Verantwortung im Datenschutz**
    3. **TOM und ADV**
    4. **Einsicht in Endgeräte von Mitarbeitern**

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Rechte und Pflichten nach TMG

§§ 5,6 Impressumspflicht

§ 7 Provider grundsätzlich für seine eigenen Inhalte verantwortlich

§§ 8-10 Providerprivilegierung bei rein technischen Dienstleistungen

§15a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG „entsprechend“)

§ 13 Pflicht zur Datenschutzerklärung und Maßnahmen zum Schutz personenbezogener Daten vor der Kenntnisnahme durch Dritte

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

§ 13 TMG neu

Nach Absatz 6 wird folgender Absatz 7 eingefügt:

(7) Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien **durch technische und organisatorische Vorkehrungen sicherzustellen**, dass

1. kein **unerlaubter Zugriff** auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese
   a) gegen Verletzungen des Schutzes personenbezogener Daten und
   b) gegen Störungen, auch soweit sie durch **äußere Angriffe** bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. **Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.**

TMG und Wettbewerbsrecht

- § 13 TMG wird als das Marktverhalten regelnde Norm gemäß § 4 Nr. 11 UWG angesehen
  - OLG Hamburg WRP 2013, 1203ff; OLG Köln vom 14.08.2009, 6 U 70/09

- Die Normen des Telemediengesetzes berechtigen im Allgemeinen zur Abmahnung (BGH vom 20.07.2006, Az: I ZR 228/03)
  - Allerdings bezieht sich die bisherige Rechtsprechung auf die Informationspflichten zur Anbieterkennzeichner

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Urheberrecht

Erlaubt ist, was erlaubt ist – Keine Lücke bei der Rechtekette !

- **Vorsicht bei Bildern**
- **Vorsicht bei OSS**

Schöpferprinzip, aber bei Software § 69 b UrhG beachten !

Wenn gelöscht werden muss, dann richtig !

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Straf- und haftungsrechtliche Risiken für Admins

„Vorsicht Falle“

IT-Strafrecht

§ 202a StGB – Ausspähen von Daten

Unbefugtes Zugangsverschaffen zu besonders gesicherten Daten.

- Ein Verschaffen oder gar die Kenntnisnahme von Daten ist nicht erforderlich.
- Bedeutung bei: IT-Sicherheitsprüfungen (Penetrationstests, Test von Schwachstellen durch Exploits, internen Ermittlungen, wenn private Mailnutzung erlaubt.

- Auch Portscans und Pings?
- Wahrscheinlich strafrechtlich zulässig, mangels Zugang zu besonders gesicherten Daten

IT-Strafrecht

§ 202b StGB – Abfangen von Daten

Nach § 202b StGB macht sich strafbar, wer sich unter Anwendung von technischen Mitteln für ihn nicht bestimmten Daten aus einer nichtöffentlichen Datenübermittlung verschafft.

- Nur Daten während des Übertragungsvorgangs betroffen.
- Besonderer Schutz der Daten nicht erforderlich (z.B. Verschlüsselung)

Abwendungsbereich z.B.: Erfassung von Nettraffic, ausgenommen Verkehrsdaten beim Access-Provider)

IT-Strafrecht

§ 202c StGB – Vorbereiten des Ausspähens oder Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

(1) Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder

(2) Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

Herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Sog. „Hackerparagraf“

IT-Strafrecht

§ 202c StGB – Vorbereiten des Ausspähens oder Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

(1) Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder

(2) Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

Herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Sog. „Hackerparagraf“

IT-Strafrecht

§ 303a - Datenveränderung

(1) Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird [bestraft].

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

Strafrechtliche Verantwortung durch Unterlassung

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

BGH Urteil vom 17. Juli 2009 - 5 StR 394/08 (BSR) – Compliance Officer

- Der Leiter der Rechtsabteilung und Innenrevision hatte Kenntnis von überhöhten Gebührenabrechnungen gegenüber Kunden, war an der Entscheidung aber nicht beteiligt.
- Inhalt und Umfang der **Garantenpflicht** bestimmen sich aus dem konkreten Pflichtenkreis, den der Verantwortliche übernommen hat.
- Garantenpflicht wird daraus abgeleitet, dass bei einer Anstalt des öffentlichen Rechts der Gesetzesvollzug das eigentliche Kernstück ihrer Tätigkeit sei und der Leiter der Rechtsabteilung das „juristische Gewissen“ des Unternehmens gewesen sei.
- Möglichkeit der Unterbindung rechtswidrigen Verhaltens sei durch Unterrichtung des Vorstandsvorsitzenden oder des Aufsichtsratsvorsitzenden gegeben gewesen.

IT-Strafrecht

Maßnahmen zur Minimierung von Strafbarkeitsrisiken:

Dokumentation von Zustimmung und Einsatz des Berechtigten zum Nachweis der Befugnis (§§ 202a ff. StGB)

Kein dauerhafter Mitschnitt z.B. von Netztraffic , sondern nur anlassbezogen. Vorgang und Zustimmung dokumentieren (§ 202b StGB)

Dual-Use-Tools, die für die Systemwartung nicht erforderlich sind, sollten gelöscht werden. Einsatz dokumentieren und nur geschlossenen Benutzergruppen zum Download anbieten (wenn überhaupt), insbesondere bei eigenen Programmierleistungen.

Private Nutzung der dienstlichen Mail-Adresse verbieten (§ 206 StGB)

Verzicht auf Wahrung des Fernmeldegeheimnisses (§§ 88 TKG, Art. 10 GG) des Arbeitnehmers (bestenfalls zu Beginn des Dienstverhältnisses)

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Haftung Mitarbeiter in der Verantwortung

Grundsatz:

Jeder hat im Rahmen einer vertraglichen Beziehung dem anderen nur die Schäden zu ersetzen, die er auch zu vertreten hat (Stichwort Verschulden).

Gehaftet wird für

- vertragliche Pflichtverletzungen (§ 280 Abs. 1 BGB)
- unerlaubte Handlungen (§ 823 ff. BGB)

Bezogen auf den Arbeitsvertrag sind somit relevant

- Verstöße gegen arbeitsvertragliche Pflichten
- Verletzungen von absolut geschützten Rechten oder Schutzrechten

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Voraussetzungen der Haftung eines Arbeitnehmers

Es müssen stets vorliegen:

- Verletzungshandlung
- Schaden
- Kausalität
- Verschulden

- Tatsächlich auch im Arbeitsverhältnis?

Haftungsbeschränkung im Arbeitsverhältnis

Der Arbeitnehmer haftet nur begrenzt gegenüber dem Arbeitgeber.

Die Haftung ist abhängig vom

Grad des Verschuldens

- keine Haftung bei leichter Fahrlässigkeit
- quotale Haftung bei mittlerer Fahrlässigkeit
- volle Haftung bei Vorsatz des Arbeitnehmer bzgl. Pflichtverstoß und Schaden (Urt. des BAG vom 18.04.2002)

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

PAUSE

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

„IT-Sicherheitsgesetz“

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – IT-SiG)

Verabschiedet vom Bundestag am 12.06.2015.

Der Bundesrat wird am 10. 07. 2015 noch einmal beraten.

Überblick über die rechtlichen Neuerungen

- IT-Sicherheitsgesetz ist ein Artikel-Gesetz
- Folgende Gesetze werden geändert:
  - BSI-Gesetz
  - Telemediengesetz
  - Telekommunikationsgesetz
  - …

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Ausgangslage 1/2

Statistisches Bundesamt 2013

- 87% aller deutschen Unternehmen nutzt einen Internetzugang
- 37% der deutschen Unternehmen nutzen soziale Medien für die Interaktion mit Privatkunden

- 40% der Unternehmen setzen Cloud-Dienste ein (BITKOM 2014)
- Bund gibt jährlich etwa 3 Milliarden EUR für IT aus (BMI 2014)

Ziel des Gesetzes

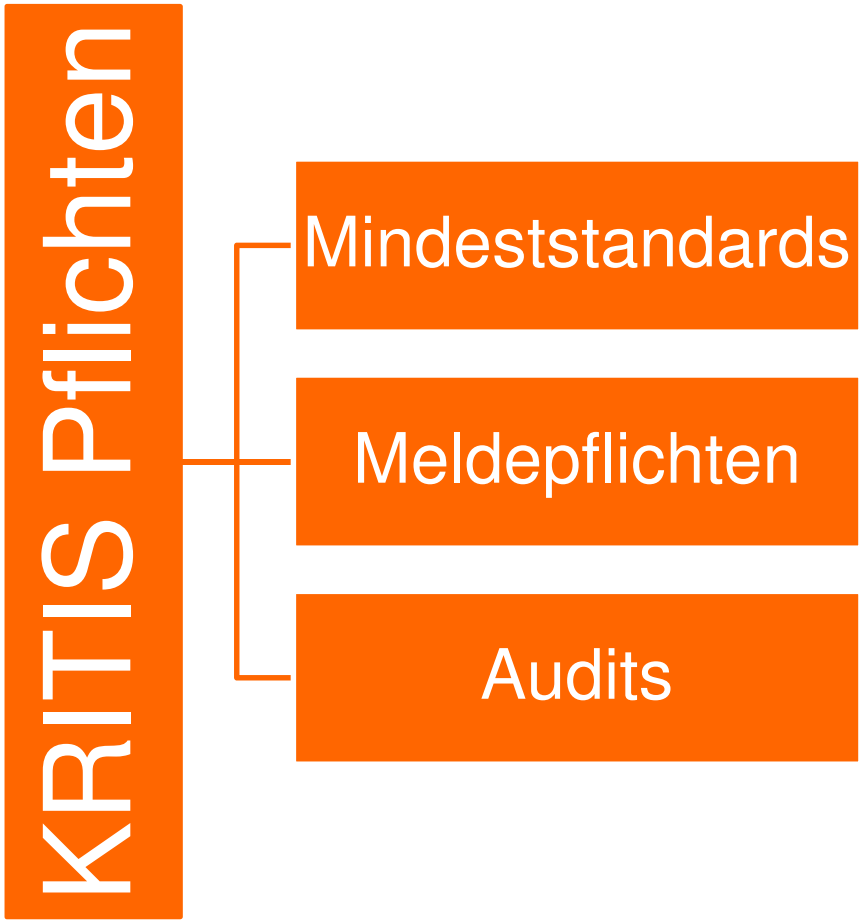
- Sicherheit informationstechnischer Systeme in Deutschland vorantreiben
- Aktuellen und zukünftigen Gefährdungen wirksam begegnen
- Verstärkter Schutz der Bürger im Internet
- Stärkung des BSI und des BKA

- Hohes Sicherheitsniveau bei „Kritischen Infrastrukturen“ (KRITIS) soll erreicht werden

- „Umsetzung“ der sog. Cybersicherheitsrichtlinie

Kritik am Gesetz

- Netzpolitk.org: „Es wird ein IT-Sicherheitsimulationsgesetz verabschiedet werden."
- Gesetz nicht verfassungsgemäß
- BSI nach wie vor dem BMI untergeordnet
- „Doppelrolle" des BSI
- Öffentliche Hand der Länder wird nicht berücksichtigt
- Schwerpunkt liegt auf Meldepflicht, proaktives Handeln nur begrenzt möglich
- Anforderungen zu unbestimmt
- Tatbestände für Ordnungswidrigkeiten zu unbestimmt
- Kosten für Wirtschaft rund 1,1 Milliarden EUR pro Jahr (KPMG)
- Explizite Aussagen zur Sicherheit der Bürgerinnen und Bürger fehlen (nur mittelbares Ziel)
- Datenschutz noch unzureichend geregelt



§ 2 BSIG n.F.

Begriff der Kritischen Infrastruktur (KRITIS)

(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen **oder Teile davon**, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören **und**
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

Kriterien für KRITIS laut Gesetzesbegründung

Einteilung der Kritischen Infrastrukturen nach den Kriterien ualität und Quantität

- Qualität
  - Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung durch einen Ausfall unmittelbar oder mittelbar beeinträchtigt
- Quantität
  - Soll den Versorgungsgrad der jeweiligen Einrichtungen, Anlagen oder Teile davon erfassen. Zu untersuchen ist in diesem Zusammenhang, ob die Auswirkungen eines Ausfalls bzw. einer Beeinträchtigung der jeweiligen Einrichtungen, Anlagen oder Teile davon für die Versorgung einer entsprechend großen Zahl an Personen (Schwellenwert) mit einer kritischen Dienstleistung unmittelbar oder mittelbar wesentlich sind, das heißt aus gesamtgesellschaftlicher Sicht eine stark negative Wirkung hätten
  - Ziel: branchenspezifische Schwellenwerte

BT-Drs 18/4096 Seite 23, 24

Ausgestaltung des Meldeverfahrens

- Erst Meldeverfahren, dann innerhalb von 6 Monaten nach Rechtsverordnung Kontaktstelle einrichten (Bußgeld).

- Meldung soll über Kontaktstelle erfolgen, obwohl diese nach § 8b Abs. 3 erst 6 Monate nach Inkrafttreten der Rechtsverordnung zu benennen ist.
  - 24/7 Erreichbarkeit der Kontaktstelle

- „unverzüglich“
  - Nach der Legaldefinition des § 121 Abs. 1 BGB bedeutet unverzüglich „ohne schuldhaftes Zögern“. Unverzüglich erfolgt eine Handlung nur, wenn sie innerhalb einer nach den Umständen des Einzelfalls zu bemessenden Prüfungs- und Überlegungszeit vorgenommen wird. Es kommt also auf den Einzelfall an, wie lange der Zeitraum der Bedenkzeit sein kann. Als Obergrenze für ein unverzügliches Handeln wird durch die Rechtsprechung in der Regel ein Zeitraum von zwei Wochen angesehen.

Ausgangslage aus Sicht des Gesetzgebers

Aktuellen Schätzungen:

- Maximal 2.000 meldepflichtige Betreiber Kritischer Infrastrukturen
- Pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr
- IT-Sicherheitsvorfälle müssen ohnehin untersucht, bewältigt und dokumentiert werden. Mehraufwand an Bürokratiekosten nur über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgehend.
- Bearbeitung einer Meldung kostet 660 Euro (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro).

§ 8b Abs. 4 BSIG - Gesetzesbegründung

Definition „Störung“

Wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.

Insbesondere:

- Sicherheitslücken
- Schadprogrammen
- Erfolgte, versuchte oder erfolgreich abgewehrte Angriffen auf die IT-Sicherheit außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (zum Beispiel nach Softwareupdates oder ein Ausfall der Serverkühlung).

Heißt konkret?

§ 8b Abs. 4 BSIG - Gesetzesbegründung

Nennung des Namens des Betreibers

- Soweit die Störung **nicht** zu einem tatsächlichen Ausfall oder einer Beeinträchtigung führt, ist die namentliche Nennung des Betreibers **nicht erforderlich**.
- Die Meldung kann in diesem Fall pseudonymisiert erfolgen (über die Kontaktstelle).

- Eine Nennung des Namens des Betreibers **ist erforderlich** bei bedeutenden Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die bereits konkret zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt haben.

Heißt konkret?

Innerbetriebliche Organisation des Meldeverfahrens

Welche innerbetrieblichen / -behördlichen

Maßnahmen sind zu ergreifen?

Etablierung eines ISMS

ISMS = *Information Security Management System*

Etablierung einer IT-Sicherheitsorganisation:

- IT-Sicherheitsbeauftragter (ITSB)
- Datenschutzbeauftragter (DSB)
- Informationssicherheitsmanagement-Team (IS-Team)
  - ITSB
  - DSB
  - CIO/Unternehmensentwicklung
  - Betriebsrat/Personalrat
  - Bereichsleiter IT
  - Zentrales Risikomanagement
  - Compliance Officer

ISMS-Dokumentation

1. Richtlinien für Anwender, z.B.:
   - Allgemeine Arbeitsanweisung IT-Abteilung
   - Betriebsvereinbarung Email und Internet
   - Betriebsvereinbarung IT-Sicherheitsrichtlinie für Anwender
   - Remote Access Sicherheitsrichtlinie
   - Dienstanweisung zum Umgang mit mobilen
   - Datenträgern
   - Social Media Guideline

2. Notfallmanagement, z.B.:
   - Notfallvorsorgekonzept
   - Notfallhandbuch

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Datenschutzrecht

Anwendungsbereich

Gesetzlicher Regelungsrahmen

- Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens)
- Art. 8 Grundrechtscharta EU (Schutz personenbezogener Daten)
- Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG (Informationelle Selbstbestimmung)
- Bundesdatenschutzgesetz (BDSG), Landesdatenschutzgesetze
- Dienst- und Betriebsvereinbarungen

- Bald Datenschutzgrundverordnung ?

Datenschutzrecht

§ 1 BDSG

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung **personenbezogener Daten** durch [Bundesbehörden und Unternehmen]

3. […] es sei denn […] ausschließlich für persönliche oder familiäre Tätigkeiten.

Datenschutzrecht

§ 3 BDSG

(1) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene).

[…]

(9) **Besondere Arten personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

.

Datenschutzrecht

§ 3 BDSG

(1) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene).

[…]

(9) **Besondere Arten personenbezogener Daten** sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Definition der personenbezogenen Daten problematisch in Zeiten von BIG DATA?

Datenschutzrecht

§ 1 BDSG

(2) Dieses Gesetz gilt für die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten […].

§ 3 BDSG

(3) **Erheben** ist das Beschaffen von Daten über den Betroffenen.

(4) **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.

(5) **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Grundprinzipien des Datenschutzrechts

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Grundprinzipien des Datenschutzes

- **Verbot mit Erlaubnisvorbehalt**
- **Zweckbindungsgrundsatz**
- **Erforderlichkeitsgrundsatz**
- **Datensparsamkeit**

vgl. auch sog. Volkszählungsurteil des Bundesverfassungsgericht (BVerfGE, 61, 1)

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Verantwortung im Datenschutz

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Verantwortung im Datenschutz

- **Geschäftsführung**
  Sie trägt die Verantwortung für den Datenschutz nach innen und außen.
- **Führungskraft**
  Sie sorgt für die Um-setzung und Kontrolle der Einhaltung gesetzlicher und interner betrieblicher Regelungen.
- **Mitarbeiter**
  Sie sind u. a. für den Schutz pbD Daten vor unbefugtem Zugriff und un-zulässiger Weiter-gabe zuständig.
- **Betriebsrat**
  Als Vertretung der Mitarbeiter wirkt er im Rahmen der Mit-bestimmung auf einen mitarbeiterorientierten Datenschutz hin.
- **Datenschutzbeauftragter**
  Er wirkt auf die Einhaltung des Datenschutzes hin vgl. § 4f. ff. BDSG.

Datenschutzrecht

§ 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.

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Auftragsdatenverarbeitung

Datenschutzrecht

§ 11 BDSG Auftragsdatenverarbeitung

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften [des] Datenschutzes verantwortlich. […]

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

Nr. 3: die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen […]

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Datenschutzrecht

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, 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 BDSG

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle

Vorsicht mit US-amerikanischen Diensteanbietern

Andere Datenschutzkultur

Andere Gesetzeslage: Herausgabe von E-Mail-Daten auf Microsoftservern in Irland?

Gmail-Man:

Episode 1 (http://vimeo.com/49048679)

Episode 2 (http://vimeo.com/76994635)

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Spezialfall: Einsicht von IT-Endgeräten von Mitarbeitern

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Einsicht in IT-Endgeräte von Mitarbeitern

Das (juristische) Problem:

Spannungsfeld verschiedener Interessen (Reibungsloser Ablauf Mitarbeiterwechsel, Urheberrechte, (postmortales) Persönlichkeitsrecht, Datenschutz, Personalvertretung, Post- und Briefgeheimnis, Archivierungspflichten…

Das (praktische) Problem:

Mitarbeiterwechsel nach Kündigung, Ausscheiden des Mitarbeiters durch schwere Krankheit oder Tod, Auseinandersetzung mit möglichen Erben oder Vertrauenspersonen, viele Beteiligte auch in der Dienststelle (Personalvertretung, Datenschutzbeauftragter, IT)

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Einsicht in IT-Endgeräte von Mitarbeitern

Handlungsempfehlungen, um Risiken zu minimieren:

1. **Problemstellung in IT-Sicherheits- und Berechtigungskonzept berücksichtigen**
    1. Regelung zur privaten Nutzung
    2. Aufklärung über mögliche Kontrollen
    3. Pflicht zur Kennzeichnung oder regelmäßigen Löschung

2. **Bestandsaufnahme**
    1. Wie ist der Mitarbeiter in der Dienstelle eingebunden?
    2. Um was für Daten geht es?
    3. Wurden dienstliche Endgeräte zur Verfügung gestellt?

Einsicht in IT-Endgeräte von Mitarbeitern

3. **Prozessbeschreibung und entsprechende Durchführung**
    1. Abteilungsspezifische Prozesse festlegen (Rolle der IT, Personalvertretung, bDSB)
    2. Prozesse mit einander verknüpfen
    3. Wenn Mitarbeiter möglich Prozess früh genug beginnen und ausscheidenden Mitarbeiter auffordern, private Inhalte zu entfernen, Zugang zu Mail-Postfach zu ermöglichen, automatische Weiterleitung mit alternativen Kontakt einrichten (sofort)
    4. Löschung privater Inhalte schriftlich bestätigen lassen, vielleicht auch von der IT
    5. Wenn Mitarbeiter sich weigert, dann Hinweis, dass Vertretungsregelung greift und Vertreter Zugang zum Postfach hat.
    6. In kritischen Fällen, Löschung unter Aufsicht der Personalvertretung und des behördlichen Datenschutzbeauftragten

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

Haben Sie noch Fragen?

Feil Rechtsanwaltsgesellschaft mbH
recht-freundlich.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT !

Michael Stolze, LL.M. LL.M.

Rechtsanwalt / Datenschutzbeauftragter (TÜV®)
Master of Laws – IT-Recht & Recht des Geistigen Eigentums (Hannover)
Master of Laws – Information and Communication Technology Law (Oslo)

Feil Rechtsanwaltsgesellschaft mbH
Döhrbruch 62 · 30559 Hannover

Tel 0511 / 473906-0
Fax 0511 / 473906-7

stolze@recht-freundlich.de