# Belehrung zur Verpflichtung auf das Datengeheimnis gem. §5 BDSG

- Grundbelehrung -

Anja Hirschel

PIRATEN PARTEI
Ulm (und um Ulm herum)

# Übersicht

- Was ist Datenschutz?
- Begriffe im Datenschutz
- Geltungsbereich des Datenschutzes
- Kontrollorgane
- Datenschutzverpflichtung
- Forderungen des Datenschutzes
- Datensicherheit
- Informationssicherheit
- Protokollierung
- Löschen von Daten (Fristen, Umsetzung, Crash)
- Aktuelle Bedrohungen des Datenschutzes

# Was ist Datenschutz?

*„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“*

*(§ 1 Abs. 1 BDSG)*

- Datenschutz ist der Schutz des Persönlichkeitsrechts
- Daten-Sicherheit ist nur Teil des Datenschutzes!

# Begriffe im Datenschutz

Im ersten Abschnitt des BDSG zu finden

- Umgang mit Daten § 3,4,5 BDSG
  Nutzen und Verwenden von Daten:
  das Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen.
- einfache Daten: Name, Adresse u.ä.
- Persönlichkeitsdaten: Einkommen, Familienverhältnisse u.ä.
- Besondere / sensible Daten: politische Meinung, Religion, Gesundheit
- personenbezogene Daten §3(1) BDSG
  Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

# Begriffe im Datenschutz

Erlaubnis-Tatbestände zum Umgang mit Daten („5er-Regel“)

- Rechtsvorschrift (z.B. Meldepflichten)
- Allgemein zugängliche Daten (z.B. Telefonbuch, Internet)
- Im Rahmen eines Vertragsverhältnisses
- Abwägung Nutzungsinteresse ←→ Geheimhaltungsinteresse
- Einwilligung des Betroffenen § 4a BDSG

- Listenprivileg § 28 (3) BDSG
  Weitergabe von Sammlungen mit einfachen Daten für Marketingzwecke erlaubt solange Betroffener nicht widerspricht.

# Geltungsbereich des Datenschutzes

- BDSG
  öffentliche Einrichtungen des Bundes §2 BDSG
  alle nicht öffentlichen Unternehmen §1 Abs.2 Nr.3 BDSG

  Wenn personenbezogene Daten verwendet werden.
  Nicht bei persönlicher Tätigkeit z.B. privates Adressbuch §1 Abs.1 Nr.3 BDSG

- LDSG (zusätzlich zum BDSG)
  öffentliche Einrichtungen des Landes

- Besondere Rechtsvorschriften haben immer Vorrang bei der Anwendung z.B. Sozialgesetzbuch, Telemediengesetz

# Kontrollorgane

- BfDI
  Bundesbeauftragter für Datenschutz und Informationsfreiheit
  Für öffentliche Einrichtungen des Bundes

- Landesdatenschutzbeauftragter
  Für öffentliche Einrichtungen des Landes

- Innenministerium
  Für nicht-öffentliche Unternehmen

# Datenschutzverpflichtung

- Jeder, der mit persönlichen Daten der Mitglieder oder Dritter in Berührung kommt, ist vorher durch die verantwortliche Stelle auf das Datengeheimnis zu verpflichten. Daher ist eine sogenannte Datenschutzverpflichtung nach erfolgter Belehrung zu unterschreiben.
- Diese Verpflichtung unterliegt einer jährlichen Belehrung durch die verantwortliche Stelle idR. durch den DSB. Wird die Belehrung nicht nachgewiesen, erlöschen alle Zugriffsrechte automatisch.
- Die Datenschutzverpflichtung wirkt über das Ausscheiden hinaus.

# Forderungen des Datenschutzes

- Sicherheit
  Schutz der Daten (Zugriff, Weitergabe, Speicherdauer)
- Transparenz
  Heimliche oder offene Datenerhebung?
  Profilbildung, Verhaltens- und Leistungskontrolle geplant?
- Zweckbindung
  Wofür werden die Daten erhoben?
- Ordnungsmäßigkeit
  Dürfen die Daten erhoben werden? („5er-Regel“)
- Beweisbarkeit
  Sind Einwilligungen schriftlich erteilt?
  Können Maßnahmen belegt werden (Verfahrensverzeichnis u.ä.)

# Forderungen des Datenschutzes

Bei der Definition schutzwürdiger Daten entstehen einige Fragen, die im Vorfeld geklärt werden müssen:

- Welche Daten sind vorhanden?
- Welche Daten sind zu schützen?
- Wer arbeitet mit diesen Daten oder hat Zugriff darauf?
- Was wird mit den Daten gemacht?
- Wer entscheidet über die Daten?

# Forderungen des Datenschutzes

Bei der Durchsicht ist auf Daten mit Verarbeitungsbeschränkungen nach §3 Abs. 9 BDSG zu achten:

- Angaben über ethnische Herkunft
- Politische Meinungen
- Religiöse oder philosophische Überzeugungen
- Parteizugehörigkeit
- Gesundheit
- Sexualleben

# Datensicherheit

IT-Sicherheit ist erforderlich, um Datenschutz technisch und organisatorisch zu gewährleisten.

Das BDSG erwähnt Maßnahmen der IT- Sicherheit in §31:

*„Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutz-kontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.“*

→ Der Datenschutz erlaubt daher die Speicherung aus Gründen der IT-Sicherheit

# Datensicherheit

- Gesamtheit aller Regelungen und Maßnahmen zur Herstellung und Erhaltung der Datensicherheit, die erforderlich sind, um einen wirksamen Datenschutz zu gewährleisten.
- Damit: Teil des Datenschutzes
- Anforderungen: §9 BDSG IT Grundschutz + Anlage
  Zutrittskontrolle
  Zugangskontrolle
  Zugriffskontrolle
  Weitergabekontrolle
  Eingabekontrolle
  Auftragskontrolle
  Verfügbarkeitskontrolle
  Datentrennung

# Datensicherheit

- Zusätzliche Schutzmaßnahmen gelten bei besonders schützenswerten Daten nach § 3 (9) BDSG

- Standards:
  IT Grundschutzzertifikat ISO 27001
  BSI-Standard 100-2 Vorgehensweisen zum IT-Grundschutz
  BSI-Standard 100-3 Risikoanlaysen zum IT-Schutz („Vorabkontrolle“)

# Datensicherheit - Backup

Backupsysteme schützen vor Datenverlust und sichern eine schnelle Verfügbarkeit im Falle eines Defekts. Ein gutes Backupsystem sollte folgende Punkte beachten:

- Es sollte auf verschiedenen Medien gesichert werden.
- Die Daten sollten verifiziert werden
- Die Medien sollten an verschiedenen Orten gelagert werden (nicht im Serverschrank, nicht im Schreibtisch, nicht zuhause).
- Die Daten sollten schnell und sicher wiederherstellbar
- Regelmäßige Prüfung auf Wiederherstellbarkeit der Backups.
- Feste Termine für Backups

# Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Werten unabhängig von Ihrer Form.

Daten sind alle schriftliche, bildliche und gesprochene Informationen.

## Vertraulichkeit:

Unberechtigten Personen, Einheiten oder Prozessen dürfen Informationen nicht verfügbar oder zugänglich gemacht werden.

## Integrität:

Werte müssen richtig und vollständig sein.

## Verfügbarkeit:

Daten einer berechtigten Einheit auf Anforderung zugänglich und nutzbar machen.

# Informationssicherheit

## Personelle Sicherheit

Sicherstellung, dass Angestellte, Auftragnehmer, Dritte ihre Verantwortlichkeiten verstehen und für die Aufgaben geeignet sind.
Diebstahl, Betrug- und Missbrauchsrisiko verringen.

Regelmäßige Überprüfung und Schulung, Disziplinarverfahren.

Verantwortlichkeit für Änderungen festlegen.
(Zugriffsrechte / Rückgabe Computer).

# Informationssicherheit

## Datenumgang

Keine Datenträger offen herum liegen lassen

Auf Laptops keine Links mit gespeicherten Passwörtern und Ordner auf dem Desktop

Keine unverschlüsselten Datenträger wie USB-Sticks

# Protokollierung

Bei der Benutzung von IT-Systemen in Abhängigkeit von der Sensibilität

- Wer hat wann mit welchen Mitteln zugegriffen, Daten eingegeben, verändert oder gelöscht?
- Wer hatte von wann bis wann welche Zugriffsrechte?

Anforderungen

- Die Protokolldateien müssen Beweisfest und Revisionssicher sein
- Keine Verhaltens- und Leistungskontrollen!
- Datensparsamkeit: Komplett- oder Blockprotokoll?
- Kontrolle: automatisiert oder in Stichproben
- Aufbewahrung: max. 1 Jahr, nach Möglichkeit weniger

# Protokollierung

Revisionssicherheit und Beweisfestigkeit

- Eintragung des exakten Zeitpunktes einer Aktion (Zeitstempel)
- Eintragung des tatsächlichen Nutzers (separater Authentisierungsvorgang
- Eintragung der tatsächlich durchgeführten, versuchten Operation
- Überprüfung der Protokollierung durch die QS

Standard-Analyse von Protokollen, Logs:

- unerlaubte Änderungen / Löschungen und Systemzugriffe
- Abbildung von Angriffszenarien
- usw.

Weiterführende Analysen

- Sind nur erlaubt wenn der Anfangsverdacht einer Straftat besteht

# Löschen von Daten

- Die allg. Löschregeln, Löschpflicht siehe § 20 (2) BDSG
- Löschen wenn Daten unzulässig erhoben wurden
- Kenntnis zur Erfüllung der Aufgaben nicht mehr nötig (Löschbestätigung)

Faustregel:

- Erfahrungsgemäß sollte ein Jahr nicht überschritten werden, besser nur 6 Monate.

Ausnahme:

- Backup-Dateien
- Spezial Regelungen (Mediziner, Personaldaten usw.)
- Gesetzliche Vorgaben (z.B. Finanzdaten)

# Löschen von Daten

Sicheres Entsorgung von Daten:

- Papierschredder mit Partikelschnitt der passenden Sicherheitsklasse
- Auch CDs, DVDs, USB-Sticks, Speicherchips usw. fachgerecht entsorgen
- Entsorgung im Auftrag möglich, aber Verantwortlichkeit bleibt bestehen

Physikalisches Löschen

- mechanisch: Zerkleinerung des Datenträgers
- thermisch: Temperatur über 750°C, Einschmelzen
- magnetisch: mit speziellen Degausser-Geräten nach DIN 33858

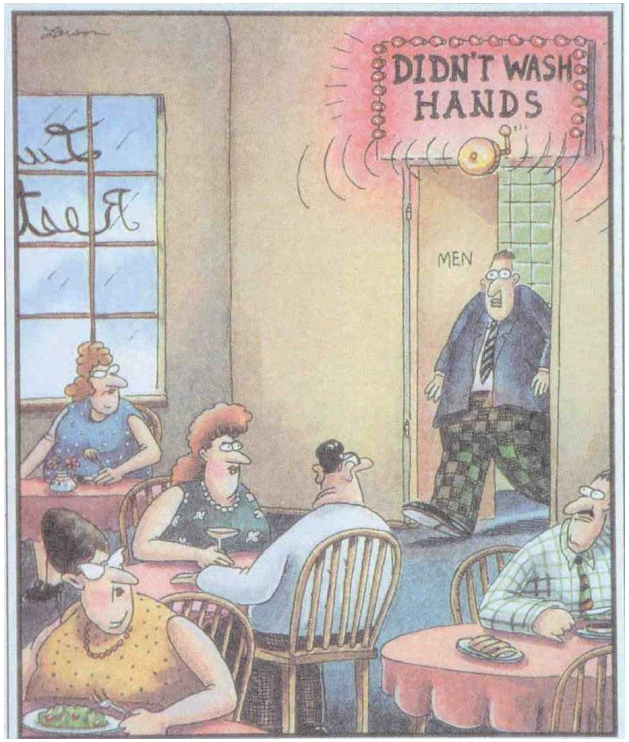
Löschen durch Überschreiben

- Hohe Überschreibrate (33-35 mal) mit Zufallszahlen bietet hohe Schutz selbst bei Laboranalyse der Datenträger.
- Heute gängige und sichere Verfahren: Gutman und Pfitzner
  z.B. SafeErase (kostenpflichtig) oder Wipe (GNU-Lizenz)
- Vorsicht bei SSD-Festplatten da Speicher nicht komplett im Zugriff

# Löschen von Daten

- Im Falle eines Plattencrashs wird die beschädigte Festplatte / die Speicherkarte oft bedenkenlos eingeschickt.
- Gefahr: Sämtliche Daten können ausspioniert werden
- Je nach Vertragsbedingungen wird ein neues Speichermedium zurück geschickt, das alte nach Reparatur anderweitig verbaut. Eine Garantie für vorheriges sicheres Löschen der Daten ist dabei nicht gegeben!
- Deshalb wenn möglich gecrashte Speichermedien nicht einschicken.
- Vor der Zerstörung das Speichermedium fotokopieren um die Seriennummer u.a. später nachweisen zu können. Kann auch als Nachweis nach einer Reparatur dienen, ob es sich um dasselbe Speichermedium handelt.

# Aktuelle Bedrohungen




- Der Grundgedanke des Datenschutzes ist es, jeden einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrechts beeinträchtigt wird

- Besonders durch Technikeinsatz nimmt nicht nur die Zahl der personen-bezogenen Daten zu, sondern auch deren Sensibilität.

# Aktuelle Bedrohungen

- Blogs
  Peinliche Darstellungen und Bilder für alle sichtbar (auch zukünftige Chefs)

- Communities (z.B.Studi-VZ, Team-Ulm, Localisten)
  als öffentlich zugänglicher Datenspeicher (5er-Regel greift hier!)

- Online-Pranger:

  *Unser geliebter Arbeitskollege Roland F. (27 Jahre aus Bad Tölz) hatte heuten seinen letzten Arbeitstag bei uns! Ich habe noch nie einen ekelhafteren, hässlicheren, widerlicheren Typen in diesem unserem Universum gesehen. […] Ausserdem ist er ein perverses Arschloch.[…] Lieber Roland F., schlechtester Krankenpfleger der Welt, wir wünschen Dir für Deinen weiteren Weg alles erdenklich Schlechte! Gott sei Dank haben wir Dich heute rausgeschmissen, so dass wir deine blöde Visage nie wieder sehen müssen.*

  *Deine Arbeitskolleginnen IH und BO*

  *P.S: Danke an Gerd, der dies ermöglicht hat!*

  *www.rache-ist-suess.de*

# Aktuelle Bedrohungen

# Schutz vor Ausspähung

- Verschlüsselung der Kommunikation (Mail und Telefonie)
- Verschlüsselung der Hardware
- Gesicherte Verbindungen ins Internet (VPN)
- Keine privaten PGS-Schlüssel auf vielen mobilen Datenträgern
- Vorsicht vor der Raumüberwachung durch Handys
- Passwortschutz bei allen mobile Devices aktivieren
- Auslesen der International Mobile Station Equipment Identity (IMEI)
- MSI-Catcher sind Geräte, mit denen die auf der Mobilfunk-Karte eines gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann. Auch das Mithören von Mobilfunk-Telefonaten ist möglich.
- Netzzugriffe auch über IP Telefone möglich

# Tools für Mails

z.B. für Mozilla Thunderbird

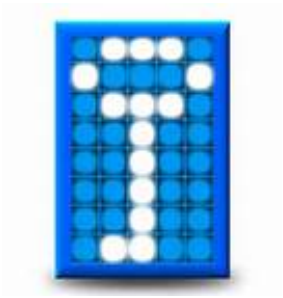
Zusätzlich die Erweiterungen:

Enigmail zum Signieren, zur Schlüsselsuche, zum Ver- und Entschlüsseln, das dann durch den GNU Privacy Guard (GnuPG) ausgeführt wird, dieser erzeugt auch die benötigten Schlüsselpaare.

HowTo:

http://wiki.piratenpartei.de/PGP/HowTo_PGP_mit_Thunderbird_unter_Windows

# Tools für Speicher



**TrueCrypt**

ist eine Software zur Datenverschlüsselung, insbesondere zur vollständigen oder partiellen Verschlüsselung von Festplatten und Wechseldatenträgern.

Das Programm läuft unter Windows ab der Version 2000, unter Mac OS X ab Version 10.4 und unter Linux mittels FUSE.

**UnterAndroid**

Androids in Java realisierte Verschlüsselung (Java Cryptography Architecture, kurz: JCA) verwendet schwache Zufallszahlen. Das betrifft potentiell alle Apps, die auf Android-Smartphones Verschlüsselung einsetzen.

Das Problem lässt sich auf eine schlechte Intialisierung des eingesetzten Pseudozufallszahlen-Generators zurückführen (Pseudo Random Number Generator, PRNG)s.

Ein solcher PRNG liefert zwar Zahlenfolgen die nicht erkennbar korreliert sind; aber mit dem gleichen Startwert liefert er jedes Mal die gleiche Folge. Kommen nur wenige Startwerte zum Einsatz, gibt es nur wenig "Zufallszahlen" und Angreifer können ihre Brute-Force-Attacken auf bestimmte Wertebereiche einschränken.

# Linksammlung

BSI Grundschutzkatalog

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Verschlüsselung von eMails

http://wiki.piratenpartei.de/PGP/HowTo_PGP_mit_Thunderbird_unter_Windows

BSI-Standard 100-2 Vorgehensweisen zum IT-Grundschutz

https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30758/standard_1002.pdf

BSI-Standard 100-3 Risikoanlaysen zum IT-Schutz („Vorabkontrolle“)

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard_1003_se_pdf.pdf?__blob=publicationFile

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_ergaenzung_pdf.pdf?__blob=publicationFile

# Danke für die Aufmerksamkeit!

Noch Fragen?