Update IT-Recht 2018

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
c/o Rechenzentrum Universität Würzburg

Über mich

Stabsstelle IT-Recht für die bayerischen staatlichen Universitäten und Hochschulen

c/o Rechenzentrum Universität Würzburg
Rechenzentrum Julius-Maximilians-Universität Würzburg

Zuvor u.a. wissenschaftlicher Mitarbeiter in der Rechnerbetriebsgruppe der Juristischen Fakultät
IT-Support, IT-(Rechts)-Kurse

Rechtsassessor - Volljurist

Wahlstation in Manchester UK
Eversheds LLP

Rechtsinformatikzertifikat
Ludwig-Maximilians-Universität München

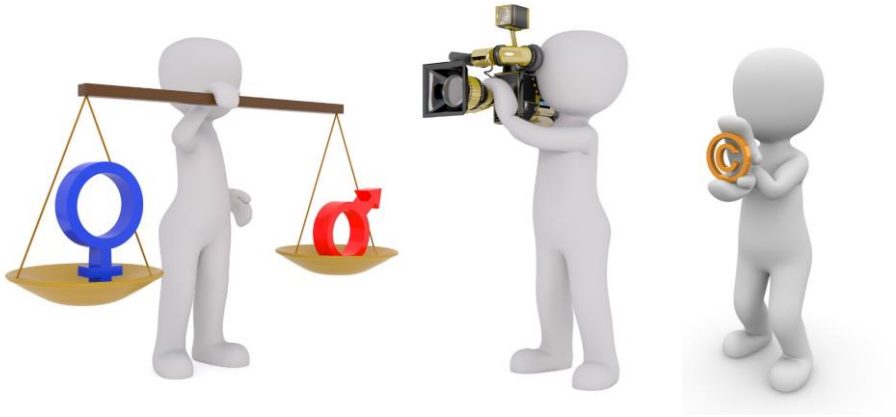
Zertifizierter Informationssicherheitsbeauftragter
Ostbayerische Technische Hochschule Regensburg

Microsoft Licensing Professional

Agenda

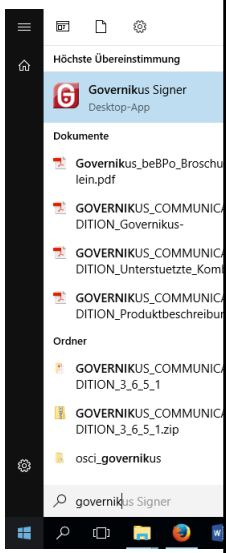
- News
- Verträge
- Reform des § 203 StGB
- Fernmeldegeheimnis
- Haftung für Rechtsverstöße
- Informationssicherheit
- Informationssicherheitskonzepte

IT-Recht News



Governikus Signer - Auflagen für den Betrieb

- Auflagen zur Anbindung an ein Netzwerk:
  - geeignet konfigurierte Firewall
  - Verwendung geeigneter Anti-Viren-Programme
- Auflagen zur Sicherheit der IT-Plattform und Programme
  - Gewährleistung der Integrität der Programme
  - manipulationssichere Hardware
- Auflagen zum Schutz vor manuellem Zugriff Unbefugter und beim Datenaustausch per Datenträger
- Anforderungen an den sicheren Betrieb
  - Es sind hinreichend komplexe Passwörter zu verwenden
  - Passwörter sind geheim zu halten



IT-Sicherheit beim IT-Einkauf

IT-Sicherheit in EVB-IT

- Gewährleistungsrecht
- No-Spy-Klausel
  - Schadsoftwarefreiheit
  - Funktionsoffenlegung

Aber: Gab es in der Ausschreibung einen Fragenkatalog dazu?

Ferner im Vergaberecht

- Der öffentliche Auftraggeber akzeptiert [als Konformität] … insbesondere ein technisches Dossier des Herstellers

Zudem

- No-Spy-Klausel nicht in allen EVT-IT Verträgen

Gesetzliche Schweigepflicht für Admins

Hintergrund: Geheimnisschutz für Dienstgeheimisse sehr weit reichend

Nunmehr in dieser Hinsicht Outsourcing möglich

➔wenn Offenbarung für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist

- ➔Zero Admin Knowledge vorzuziehen
- ➔besser nur verschlüsselt schutzwürdige Daten aus der Hand geben

Zusätzlicher Schutz

- Vertraulichkeitsvereinbarung (in EVB-IT AGBs integriert)

Internetzugang und VoIP aber auch E-Mail

Was darf ich grundsätzlich nicht?

- Kenntnis nehmen von Inhalt und Umständen der Kommunikation
  Art. 13 GG, § 88 Abs. 1-3 TKG, Art. 112 Abs. 1 BayVerf

Was darf ich?

- Das für die Diensterbringung Erforderliche kennen
- Meine Systeme schützen § 88 Abs. 3 S. 1 TKG

Internetzugang und VoIP aber auch E-Mail

- Störungen oder Fehler an Telekommunikationsanlagen erkennen, eingrenzen oder beseitigen § 100 Abs. 1 S. 1 und 2 TKG
  - ➔Störung auch bei Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten
  - ➔Störung ist auch die Möglichkeit eines unerlaubten Zugriffs auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer
- Eingeschränkt auch die Bekämpfung von Leistungserschleichung und Betrug

Spaßbremse: Ersetzt die DSGVO diese detaillierte Regelung?

Einschätzung: Nein, da TKG die E-Privacy-Richtlinie umsetzt.

Grenzen für Schutzmaßnahmen

Schutzmaßnahmen, Störungs- oder Fehlererkennung, -eingrenzung oder -beseitigung müssen erforderlich sein.

In der Umsetzung geht es darum, dass alle Maßnahmen, die in das Fernmeldegeheimnis eingreifen, verhältnismäßig sind.

- Einer der im Gesetz vorgesehenen (Schutz-)Zwecke wird verfolgt
- Es gibt keine mildere, ebenso wirksame Maßnahme
- Der Nutzen der Maßnahme überwiegt die Beeinträchtigung der Rechte der Nutzenden

Haftung (vereinfacht)

DFN-Kommunikationsdienste:
Jeden Missbrauch unverzüglich abstellen und informieren

§ 99 UrhG Unternehmenshaftung	Plattformen mit eigenen & zueignen gemachten Inhalten	§ 10 TMG Hosting und Plattformen	§ 8 und 9 TMG Accessprovider
Schadensersatz bei (Hochschul-) Forschung Lehre Verwaltung	Keine Haftungs-Privilegien, d.h. Schadensersatz	Unterlassen Beseitigung der Störung Anwaltskosten der Gegenseite	Nunmehr auch keine Störerhaftung
Anregung: Dienstliche Tätigkeiten über separates WLAN (nicht eduroam) Alt. Nutzerkreise		Server anderer Hochschulen Beiträge und Dateien von Lernenden Private Dateien	Bayern-WLAN eduroam Internet für Pool-Rechner Privates Surfen

Der Datenschutzverweis des Bay-EGovG

Datenschutzverweis des Bay-EGovG

BayDSG
- Angemessenen Verhältnis zu dem angestrebten Schutzzweck
- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

DSGVO
- Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos
- Pseudonymisierung
- Verschlüsselung
- Gewährleistung der Vertraulichkeit
- Gewährleistung der Integrität
- Gewährleistung der Verfügbarkeit
- (Gewährleistung der Belastbarkeit der Systeme)
- Verfahren zur Wiederherstellung der Verfügbarkeit
- Regelmäßiger Überprüfung
- Bewertung und Evaluierung

Informationssicherheitskonzepte

Pflicht zur Informationssicherheit bereits seit **30. Dezember 2015** im Gesetz verankert!

Rechtssicherste Lösung für Konzepte bis spätestens **1. Januar 2019**
- Grundschutz des BSI
- ISO 270xx
- ISIS12

Bei besonders kleinen Einheiten kann auch reichen:
- VdS3473
- ISA+

Eine Zertifizierung ist möglich.

Die Standards sind die „fachliche Grundlage“ für die Konzepte.

Was umfasst ein Konzept nach BayEGovG?

1. Informationssicherheitsleitlinie

Weitere Punkte
- Zuweisung von Verantwortlichkeiten
- Sicherstellung der Fortbildung der ISB
- Festlegung und Dokumentation der Abläufe bei IT-Sicherheitsvorfällen

2. Information, Weiterbildung, Sensibilisierung
- Vergleichbar mit Schritt 2 in ISIS12
- Schulungsangebote etablieren

3. Sicherheitskonzepte leben – ganzheitlicher Ansatz vorzugswürdig
- Regelungen der Themen wie BYOD, Telearbeit, Entsorgung
- Vergleichbarer Prozess wie bei Datenschutzfreigabe
- „Risikobeurteilung“ für den jeweiligen Prozess
- Risikobehandlung orientiert an Art. 7 BayDSG / Art. 32 DSGVO
- Kontrolle der Umsetzung
- Fortschreibung der Prozesse

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Johannes Nehlsen
Tel.: 0931/31-84217
rz-stabsstelle-it-recht@uni-wuerzburg.de

https://www.rz.uni-wuerzburg.de/dienste/it-recht/anwendertag2017