Netzwerksicherheit und Recht

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

Über mich

- Volljurist
  - Referendariat OLG München
  - Wahlstation bei Eversheds UK
- Rechtsinformatikzertifikat an der Ludwig-Maximilians-Universität
- Informationssicherheits-beauftragter, OTH Regensburg
- Microsoft Licensing Professional
- Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
  - Datenschutz
  - E-Government
  - E-Procurement
  - IT-(Sicherheits-)recht
  - Urheberrecht
- Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

Themen

- Informationssicherheitsrecht
- Verkehrssicherheitspflichten
- Telemediendienste
- Wann bin ich Telekommunikationsdienstenanbieter?
- Aufbewahrung von Log-Daten
- Juristisches Abwägen
- Datenschutz mal ganz kurz

Ein Hinweis

Anhang Anforderungen und Maßnahmen für Arbeitsstätten nach § 3 Absatz 1

6.5 Anforderungen an die Benutzerfreundlichkeit von Bildschirmarbeitsplätzen

(5) Eine Kontrolle der Arbeit hinsichtlich der qualitativen oder quantitativen Ergebnisse darf ohne Wissen der Beschäftigten nicht durchgeführt werden.

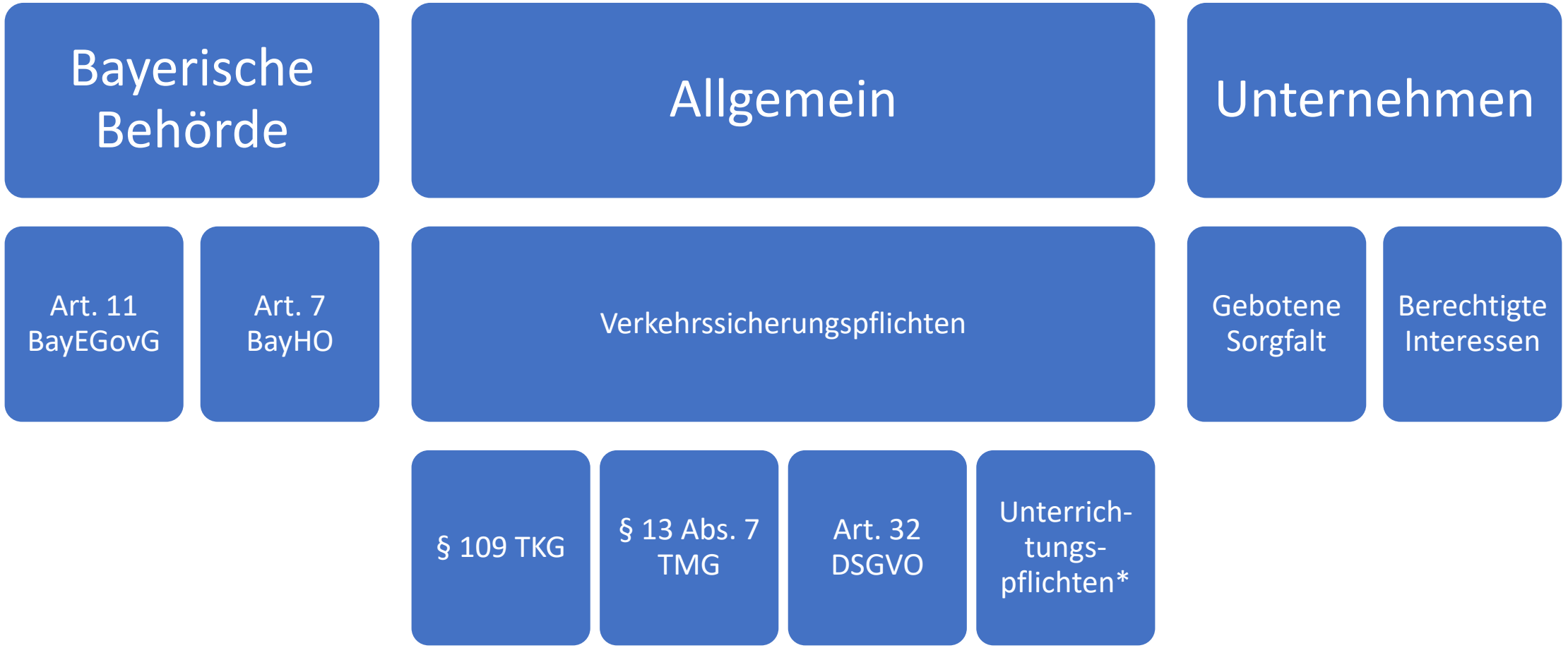
Vielleicht in einer Ausschreibung

Der Auftraggeber schätzt insbesondere folgende Informationen als personenbezogene Daten ein:

- Eindeutige Webseitenadressen
  z.B. www.meinecloud.de/rechteusernamedateiname
- IP-Adressen (v4 und v6)
- Hardwareadressen
- Samples
- Metadaten, Events und Logs mit zugeordnetem Endgerät

Ausschnitt aus der Landkarte „Informationssicherheitsrecht“

Pflichten (vereinfacht)



Verkehrssicherungspflichten (vereinfacht)

Grundsätzliches

- Berechtigte Sicherheitserwartungen des Verkehrs im jeweils betroffenen Lebensbereich
- Nicht jedes Risiko gegenüber jedermann

- Erforderlichkeit von Sicherungsmaßnahmen
  - Verkehrserwartungen
  - Bestimmungsgemäße Benutzung
  - Naheliegendes Fehlverhalten
  - Konkretisierung durch öffentlich-rechtliche und private Standards
- Zumutbarkeit konkreter Sicherungsmaßnahmen
  - Wirtschaftliche Zumutbarkeit
  - Eintrittswahrscheinlichkeit und das zu erwartende Ausmaß des drohenden Schadens

Aus der Praxis im WLAN

1. Bestehen von Prüfpflichten

➔Bekannte und beherrschbare Risiken

Beispiel WLAN

- Weitergabe Zugangsdaten
- Schwache Verschlüsselung
- Fehlerhafte Konfiguration

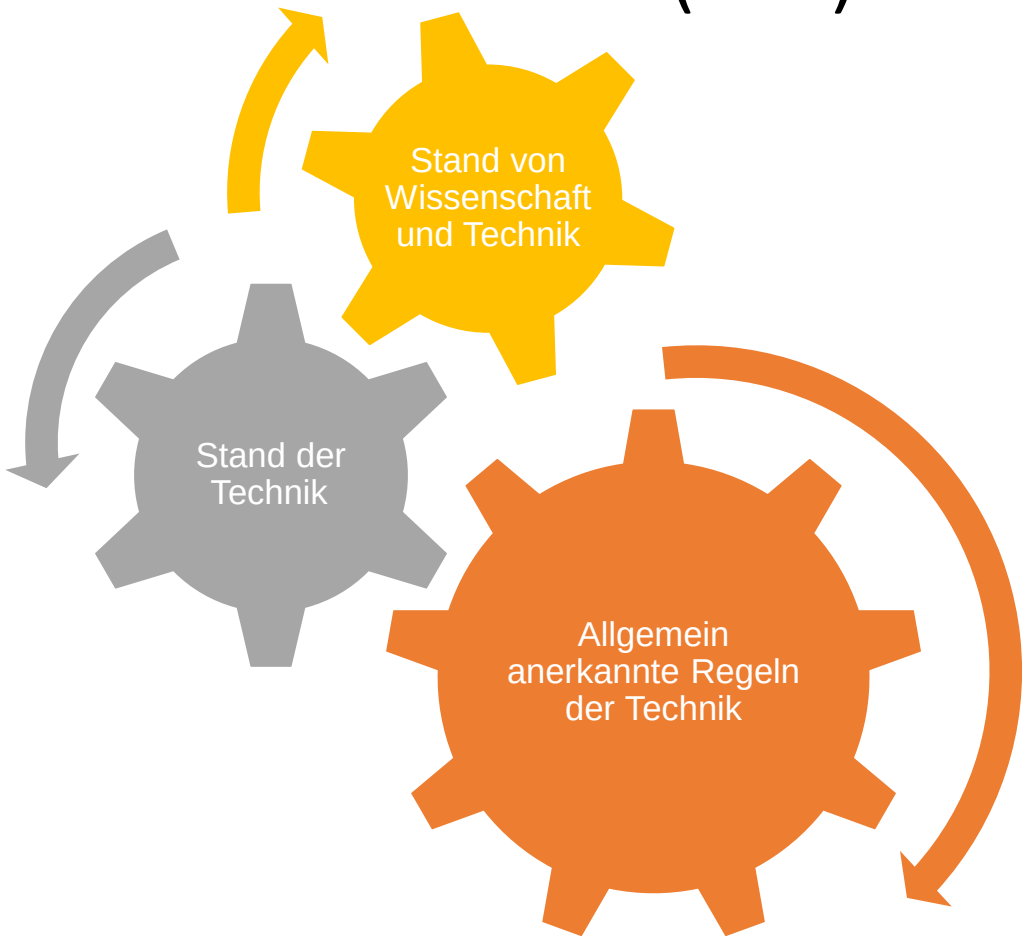
2. Weitergehen mit der Technik?
   - Derzeit für Privatanwender nicht
   - Aber bei Neukauf

Insbesondere daheim

- WPA2 (noch)
- (Gutes) Individuelles Passwort für WLAN und Router
- Automatische Sicherheitsupdates
- u.U. gemietete WLAN-Router
- Kommerzielle Gäste-Hotspots

Technikstand für Juristen (DE)

- Schritt halten mit wissenschaftlicher und technischer Entwicklung
- Front der technischen Entwicklung
- Mögliche Abweichung
- Herrschende Auffassung unter den technischen Praktikern



IT-Sicherheit für „Apps und Web“

Ziele

- Schadsoftware eindämmen
- „Patch“-Pflicht
- Verantwortung zuweisen

§ 13 Abs. 7 TMG

- Kein unerlaubter Zugriff
- Datenschutz
- Störungsschutz

Umsetzung

- BSI? OWASP?
- Artt. 24, 25, 32, 35 DSGVO
- Vertrags-pflichten

IT-Sicherheits-Gesetz 2.0 *

- Möglichkeit Systeme abzuschalten
- Unterrichtungspflicht bei Vorfällen an BKA

Wo bin ich denn?

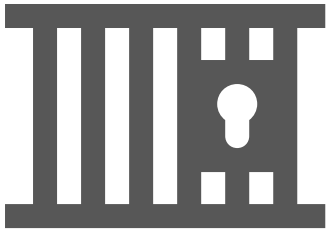
- Internes Kommunikationsangebot
  - Einfacher Datenschutz
    - Prinzipien
    - Erlaubnisnormen
    - Sicherheitspflichten
- Wenn nachhaltiges Dienstangebot für Dritte
  - Spezialschutz - Telekommunikation
    - Fernmeldegeheimnis (D)
    - Erlaubnisnormen
    - Sicherheitspflichten

Was darf ich nicht?

Was darf ich grundsätzlich nicht?

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

Sonst …



Kleine gesetzliche Ergänzungen in § 100 Abs. 1 TKG

(1) 1 Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. 2 Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.	(1) 1 Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. 2 Die Kommunikationsinhalte sind nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung. 3 Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. 4 Die Daten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind. 5 Eine Nutzung der Daten zu anderen Zwecken ist unzulässig. 6 Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. 7 Der Diensteanbieter muss dem betrieblichen Datenschutzbeauftragten, der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 6 in diesem Zeitraum schriftlich berichten. 8 Die Bundesnetzagentur leitet diese Informationen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. 9 Der Betroffene ist von dem Diensteanbieter zu benachrichtigen, sofern dieser ermittelt werden kann. 10 Wurden im Rahmen einer Maßnahme nach Satz 1 auch Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung erhoben und verwendet, müssen die Berichte mindestens auch Angaben zum Umfang und zur Erforderlichkeit der Erhebung und Verwendung der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung enthalten.

- Aus 2 Sätzen und 472 Zeichen werden
- 10 Sätze und 1265 Zeichen
- Interne Meldepflichten
- Berichtspflichten
- Externe Meldepflichten an Datenschutzaufsicht und Bundesnetzagentur mit Weiterleitung an Bundesamt für Sicherheit in der Informationstechnik

Datenarten

- Bestandsdaten
  - Beispiel: „Account“
- Nutzungsdaten
  - Nur eingeschränkt weiter verarbeitbar
  - Beispiel: „Logfiles“

TKG mit gesonderten Regeln zu

- Standortdaten
- Teilnehmerverzeichnisse
- Verkehrsdaten
  - Beispiel: Vergabe dynamischer IP-Adressen durch den Provider
- Steuerdaten
  - Beispiel: Headerdaten in von Protokollen, Informationen aus den jeweiligen Layern

Steuerdaten

BT-Drs 18/11808 S. 9

„Es handelt sich um Informationen, die sich aus den verschiedenen Layern des sogenannten OSI-Schichtenmodels der ITU ergeben, also um Informationen zu technischen Übertragungsprotokollen, nicht jedoch um Inhalte eines Kommunikationsvorganges, die damit übertragen werden.“

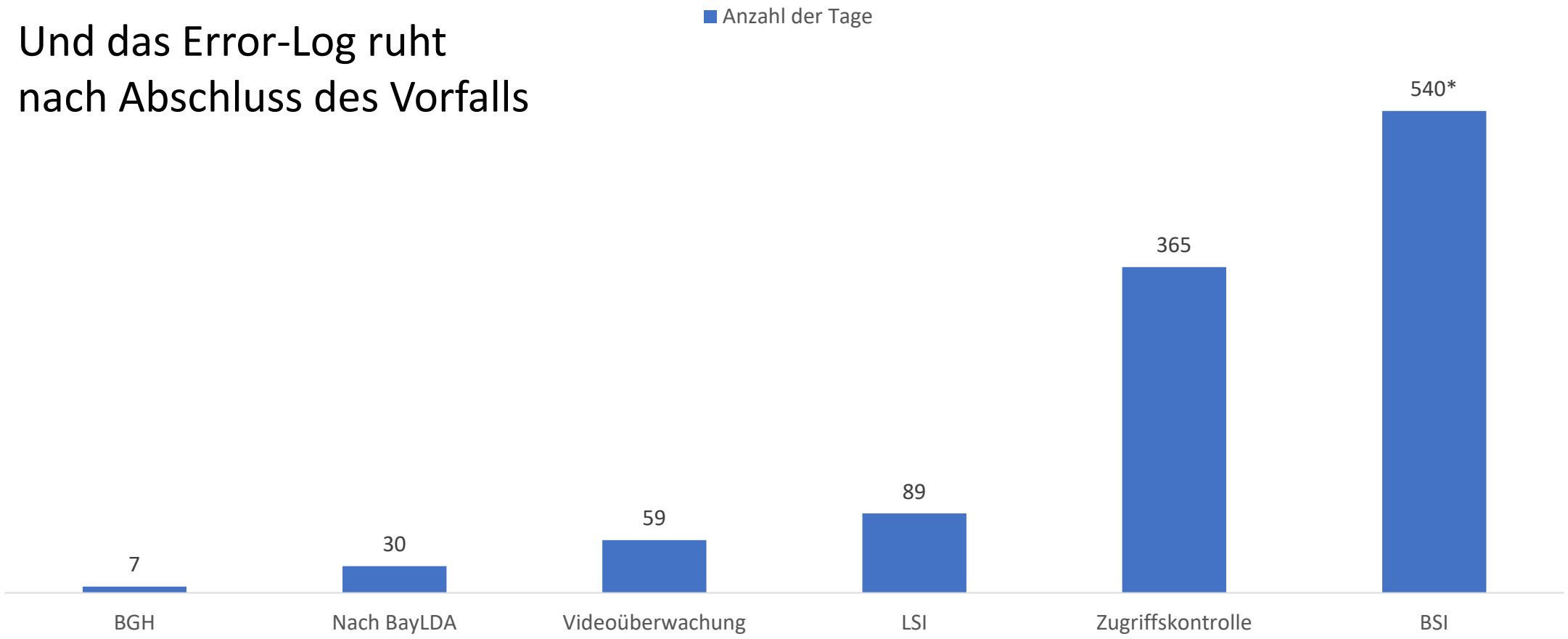
http://dipbt.bundestag.de/dip21/btd/18/118/1811808.pdf

Was darf ich (§ 100 TKG)?

- Das für die Diensterbringung ‚erforderliche' kennen
- Meine Systeme schützen
- Störungen oder Fehler an Telekommunikationsanlagen erkennen, einzugrenzen oder beseitigen
  - "Telekommunikationsanlagen" sind technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können
  - Störung auch bei Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten
  - Störung ist auch bei der Möglichkeit eines unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer
- Maßnahmen zur Bekämpfung von Leistungserschleichung und Betrug

Am … Tage ruhte das Access-Log

Und das Error-Log ruht
nach Abschluss des Vorfalls



Um was geht es also wirklich?

Abwägung		**„Gefährdung“**		
		gering	mittel	schwer
„Interessen“	klein	offen	eher nein	nein
	mittel	eher ja	offen	eher nein
	hoch	ja	eher ja	offen

Wie kann ich in der Abwägung gestalten?

- Was ist mein Angebot?
  - E-Mail
  - E-Mail mit Werbung
  - E-Mail mit starker Sicherheit
- Die Gewichtung der Interessen und der Eingriffsintensität beinhaltet einen eigenen Gestaltungsspielraum, der auch nicht vollumfänglich gerichtlicher Prüfung unterliegt.
- Wie gut können die Interessen wirklich erreicht werden?
- Kann der Eingriff durch Ausnahmen, Ausweichmöglichkeiten oder Kontrollen abgeschwächt werden?

Und der Aufwand für den Rest aus der DSGVO?

- Informationen an Betroffene
- Umsetzung von Betroffenenrechten
- Dokumentation
- Datenschutzfreundliches Design
- Datenschutzfreundliche Voreinstellungen
- Datensicherheit
- Bewältigung von Datenschutzverletzungen
- Datenschutzfolgeabschätzung … „Bayerische Blacklist (Behörden)“

Fazit

- Verdichtung von rechtlichen Informationssicherheitsvorgaben
- Datenschutz verhindert keine erforderliche Sicherheitsmaßnahmen, auch nicht
- Das Recht ist hier Technologie neutral
- Ihr Einsatz beginnt aber eine umfassende Konzeption und Prüfung
- Der Bedarf kann am Ende anderes als erwartet aussehen

Praxistipp

- Der Mitbestimmung obliegt nur das „Wie“ nicht das „Ob“
- Systeme von Datensicherheit bzw. –kontrolle von den übrigen trennen

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

Johannes Nehlsen

Tel.: 0931/31-84217

Johannes.nehlsen@uni-wuerzburg.de

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

Twitter privat: @JoNehlsen

Nehlsen - Netzwerksicherheit und Recht