

# Dezemberupdate 2019

# Informationssicherheitsrecht

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

# Updates zu Art. 11 Abs. 1 BayEGovG?

- [Stand der Technik](#)
- Siegel Kommunale IT-Sicherheit
- Ergänzender Praxistipp: [SiKoSH](#)
- Suchen Sie Ihre alten Regelungen!
  - Benutzerordnungen
  - Hausordnungen
  - Allgemeine Geschäftsordnung
  - Vorgaben aus Kooperationen
- Nutzen Sie auch das, was Sie haben!

# Was kommt aus dem E-Government

Schon immer oder schon länger

- Informationssicherheit
- Digitale Verwaltungsleistungen
- Onlinestellen von Formularen
- Barrierefreiheit

1. Januar 2020

- Informationssicherheitskonzepte
- Verschlüsselte Kommunikation
  - DFN-PKI
  - BayernPortal
  - Aber auch Chatlösungen denkbar (Delta Chat, Threema, Line, ...)
- E-Payment
- Akzeptanz der europäischen eID
- E-Rechnungs-Empfang (April 2020)

# Erinnerung OTT-Dienst ohne Fernmeldegeheimnis

EuGH C-193/18 und C 142/18

- Internes Kommunikationsangebot / „Over-the-Top“-Dienste
  - Einfacher Datenschutz
    - Prinzipien
    - Erlaubnisnormen
    - Sicherheitspflichten
- Wenn nachhaltiges Dienstangebot für Dritte (mit Signalübertragung)
  - Spezialschutz - Telekommunikation
    - Fernmeldegeheimnis (D)
    - Erlaubnisnormen
    - Sicherheitspflichten

# Und was heißt das nun?

- Für E-Mail gilt das Fernmeldegeheimnis nicht
- Nur Computerfax bleibt aber im Fernmeldegeheimnis
- Art. 32 DSGVO und Art. 11 Abs. 1 BayEGovG statt §§ 100, 109 TKG
- Keine Strafbarkeit mehr nach § 206 StGB
- Es können daher die der tatsächlichen Bedrohungslage angemessenen Sicherheitsmaßnahmen getroffen werden. Auch ein Verzögern der Zustellung oder Löschen von E-Mails kann zulässig sein.

# Meldepflichten zur Erinnerung

## Meldung an Verfassungsschutz (Art. 24 BayVSG)

- Bei Verdachtsmomenten für den Ursprung des Angriffs bei einer fremden Macht
- Bei Verdachtsmomenten für organisierten Kriminalität

## Meldung an andere Einrichtungen („Cyberabwehr“)

- Wenn aus der Organtreu geboten (etwa bei Vorfall über Mail-Konto einer anderen öffentlichen Stelle)

## Meldung an Bay LfD (Art. 33 DSGVO)

- Bei Risiken Vorlage bei der Hochschulleitung, ob Vorfall dem Landesbeauftragten für Datenschutz zu melden ist

## Benachrichtigung der Betroffenen (Art. 34 DSGVO)

- Bei hohen Risiken in Folge der Datenschutzverletzung
- User, die Daten eingegeben haben
- Kommunikationspartner, wenn Zugriff für die Postfächer der User erfolgte

# Kommt die Updatepflicht für Anwender und Hersteller?

## Art. 6 Richtlinie EU 2019/770

- Vertragsgemäßheit  
U.a. auch die Leistungsmerkmale wie Funktionalität, Kompatibilität, Zugänglichkeit, Kontinuität und Sicherheit
- Pflicht zur Bereitstellungen von Updates, wenn keine Vertragsmäßigkeit
  - Bei Leistung über einen Zeitraum
  - Vom Verbraucher erwartbar
- Informationspflicht über Updates
- Obliegenheit des Verbrauchers nach Bereitstellung die Updates zu installieren
- Haftung für ein oder zwei Jahre ab Bereitstellung

# Updatepflicht aus Hochschulsicht

- Bereich DFN
  - Es ist grundsätzlich jeder Missbrauch gemäß der Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste zu verhindern.
- Benutzerrichtlinien
- Maßnahmen zur Sicherheit der Datenverarbeitung (Art. 32 DSGVO)
- Dienste
  - Für diese sind ggf. noch weitere Pflichten zur Sicherheit zu erfüllen.
  - Für Anlagen, die Telekommunikation dienen, die aus § 109 Abs. 1 TKG, für Anlagen die Telemediendienste "ausliefern" § 13 Abs. 7 TMG.
  - Zum Stand der Technik dürfte u.a. auch ein Schwachstellen und Patchmanagement gehören (vgl. [Handreichung](#) S. 78 ff)



# Datenerhebung und Zweckänderung für Sicherheit

Art. 4 Abs. 5 Richtlinie EU 2019/770

Diese Richtlinie gilt nicht für Verträge, die Folgendes zum Gegenstand haben: ...

f) Software, die der Unternehmer im Rahmen einer freien und quelloffenen Lizenz anbietet, sofern der Verbraucher keinen Preis zahlt und die vom Verbraucher bereitgestellten personenbezogenen Daten durch den Unternehmer ausschließlich zur Verbesserung der Sicherheit, der Kompatibilität oder der Interoperabilität dieser speziellen Software verarbeitet; ...

# Art. 6 Abs. 1 BayDSG

Öffentliche Stellen, die personenbezogene Daten verarbeiten dürfen, dürfen diese auch [...] zur Gewährleistung der Netz- und Informationssicherheit ...

Jedoch zu beachten:

Informationspflichten gegenüber den Betroffenen (Art. 13 Abs. 4 DSGVO)

Wir verarbeiten Bestandsdaten, Verkehrsdaten und Steuerdaten auch zur Gewährleistung der Netz- und Informationssicherheit. Allgemein erläutern wir unsere Maßnahmen auf unserer Informationsseite zur Informationssicherheit.

Hinweise Widerspruchsrecht und weiteren Betroffenenrechten finden Sie auf unserem Internetauftritt unter [Datenschutz](#).

# Whistleblowing

- Nach Impressum, Datenschutzinformationen, Cookie-Informationen und Erklärung zur Barrierefreiheit kommt nun noch ...
- ... das Whistleblower-Portal
- Umsetzung der Richtlinie EU 2019/1937 in nationales Gesetz steht noch aus

## Vorschläge

- Kontaktpunkte DSB, Personalrat, Schwerbehindertenvertreter, Interne Revision, Arbeitsschutz und Sicherheitsbeauftragter, ...
- OpenSource-Lösungen verfügbar (z.B. [GolbaLeaks](#))
- Erreichbarkeit über TOR?

# Vielen Dank für Ihre Aufmerksamkeit!



Kontakt:

Johannes Nehlsen

Tel.: 0931/31-84217

[Johannes.nehlsen@uni-wuerzburg.de](mailto:Johannes.nehlsen@uni-wuerzburg.de)

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

Twitter privat: @JoNehlsen

Nehlsen – Dezemberupdate 2019 Informationssicherheitsrecht

Dieses Werk ohne Zitate, geschützte Marken, Icons und unwesentlichem Beiwerk ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).