Update IT-Recht 2018 Nachmittag

Johannes Nehlsen

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

Agenda

- Organisatorische Aspekte

- Überblick Recht
- Asset-Verwaltung
- Beschaffung
- Lieferantenbeziehungen

- Sicherheitsvorfälle und Detektion
- Notfallmanagement
- Compliance

Digitalisierungsrecht - Update Zeitplan

Geltung ab	Inhalt	Gesetz
bestehend	Datenschutz	BayDSG, TMG, TKG, u.a.
bestehend	Netzanschluss, Internet, E-Mail, VoIP	§ 109 Abs. 1 TKG
bestehend	Dienst- und Amtsgeheimnis	diverse
25. Juli 2015	Sicherheit Onlinedienste	§ 13 Abs. 7 TMG
30. Dezember 2015	Informationssicherheit	Art. 8 Abs. 1 S. 1 BayEGovG
30. Juni 2016	Schutz für Telekommunikationsanlagen	§ 100 TKG
09.November 2017	Neuerung bei Dienstgeheimnissen	§ 203 StGB
1. Januar 2018	Regeln zu Einkäufen bis 50.000 €	UVgO
25. Mai 2018	Datenschutz allgemein	Datenschutz-Grundverordnung
unbekannt	Datenschutz für Onlinedienste	E-Privacy-Verordnung
1. Januar 2019	Informationssicherheitskonzepte	Art. 8 Abs. 1 S. 2 BayEGovG

Gesetz	Beispiele für (Pflicht-)IT-Dienstleistungen
eIDAS-Verordnung	• Akzeptanz digitaler Nachweise (Signaturen, Siegel, Fernsignatur, etc.)
E-Government-Gesetz	• Digitale „Erreichbarkeit“ • eID bei Identifikationsprüfung • Bereitstellung für Verschlüsselungsverfahren (Kommunikation) • Dienste digitalisieren • Verfahren digitalisieren • eAkte
Gerichtsverfahrensordnungen	• Digitale Kommunikation mit den Gerichten
Verwaltungsverfahrensgesetz	• Digitale Beglaubigungen von Urkunden • Digitale Kopien von Urkunden
E-Government-Gesetz II	• ePayment • eRechnung
DFG	• Sicherung und Aufbewahrung von Primärdaten für 10 Jahre • Sabotageschutz für Forschungsvorhaben
DFN	• Abstellen von Rechtsverletzungen im Forschungsnetz • Einhalten der Regelungen zur PKI • Einhalten der Regelungen der DFN-AAI

Schnittmenge von IT- und Datensicherheit 2018

1. Leitlinien mit Bekenntnis zur Verantwortung der Leitung
2. Dokumentationspflicht
3. Schulung und Sensibilisierung
4. Asset-Kenntnis
5. Kontrolle von Design und Konfiguration
6. Rollen und Rechtemanagement
7. Einsatz von Verschlüsselung
8. Gewährleistung der Ziele Vertraulichkeit, Integrität und Verfügbarkeit
9. Ausfallsicherheit und Wiederherstellbarkeit
10. Kontrolle und Überwachung
11. Kontrolle bei Einschaltung Dritter
12. Regelmäßige Überprüfung
13. Bewertung und Evaluierung

Wirtschaftlichkeit und Sparsamkeit

Wirtschaftlichkeit

- Günstigste Relation zwischen dem verfolgten Zweck und den einzusetzenden Ressourcen
- Ausrichtung auf möglichst geringem Mitteleinsatz
- Mitteleinsatz mit Bestreben des bestmöglichen Ergebnisses

Sparsamkeit

- Nur Appellcharakter ohne rechtlich inhaltliche Bedeutung

Die Wirtschaftlichkeit bezieht sich nicht nur auf die haushaltrechtlich bereitgestellten Mittel, sondern auf jedwede Kosten, also auch diejenigen, die im kameralistischen Haushaltswesen keine Abbildung finden (Wiesner/Westermeier, S. 51).

Quelle: Nomos-BR/von Lewinski/Burbat BHO/Kai von Lewinski/Daniela Burbat BHO § 7 Rn. 1-36, beck-online

Assets

Art. 73 BayHO und VV zu Art. 73 BayHO insbesondere Nr. 3

Leitungsaufgabe:

Bestandsverzeichnisse sind mindestens alle zwei Jahre vom Leiter der Dienststelle oder einem Beauftragten unvermutet zu prüfen

Nicht: Verbrauchsmittel, geringwertigen oder kurzlebigen Gebrauchsgegenstände

Rückausnahme Sachgesamtheiten

➔ Erfassen (Monitor, Dockinglösung, Adapter?)

Mindestanforderungen

- Ort
  - Dienststellenbezeichnung mit Dienststellennummer
  - Gebäudenummer
  - Raumnummer
  - Materiallagernummer oder Materiallagerbezeichnung (optional)
  - Organisationseinheit-Nummer (optional)

Assets

- Gegenstand
  - Inventarnummer bzw. Inventarkennzeichen
  - Geräteart/Warenart/Bezeichnung
  - Typ/Fabrikat/Seriennummer/Buchkennzeichen (bei Bibliotheken mit Büchern)
  - Tag des Zugangs/Abgangs/Liefertag
  - Anzahl Zugang/Abgang
  - Bestand
  - Anschaffungskosten/Herstellungskosten
  - Lieferant/Hersteller/Name der Firma/Firmennummer
  - Vermerke/Sonstiges

  Optional
  - Klassifikationsbezeichnung und ggf. Klassifikationsnummer
  - Zugangsart (mit ggf. Zugangsartschlüssel)
  - Verwendung

Immaterielle Werte

Pflicht zum Vermögensverzeichnis

➔Art. 73 BayHO und VV zu Art. 73 BayHO Nr. 1. S. 3

Dokumentation muss aus den Lizenzverträgen erforderlichen Zuweisungsumfang enthalten

Prüfung ähnlich wie für Sachen durch die Leitung der jeweiligen Dienststelle

Erfassung des Updatestand nur teilweise mit Haushaltsrecht begründbar, im Übrigen als Maßnahme Datenschutzverletzungen zu dedektiveren.

Webshop

- Zertifikate
- Neuer Loadbalancer
- Erarbeitung Prüfkonzept

- Wegfall zentraler Freigaben
- Neue ADV nach DSGVO Dezember 2017
- Neuer DSGVO Code of Conduct
- Interne Vorprüfung Bilderlizenzen erfolgt

Was steht an?

- Schritt für Schritt zu noch mehr Sicherheit
- Selbstverpflichtung zum GÉANT Data Prote Code of Conduct
- Anpassungen an Datenschutzgrundverordr
- Bayernweite Datenschutzfreigabe
- Barrierefreiheit
- Verbesserung der Lizenztexte
- Bilderlizenzierung

22.02.2017 Nehlsen - Das Recht rund um die Portale

Lieferanten

Auftrags(daten)vereinbarung

- Adobe
- Bechtle (SCCM, Imageaufspielen)
- Citavi (demnächst)
- Dropbox
- Microsoft
- Google
- HPE
- Spider
- Teamviewer
- Turnitin

Fehlend

- Bechtle
- Cisco
- MicroFocus
- VmWare (jedoch [nicht gelebte] Pseudonymisierung möglich)

….

Verbesserungspotential

- Apple
- T-Systems (Treuhand)

DSGVO Erwägungsgrund 49

Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams — CERT, beziehungsweise Computer Security Incident Response Teams — CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. **Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.**

Etwas verständlicher

Prüffragen
- Was ist mein SLA
- Was schütze ich? Kassen mit Steuergeldern, Forschungsdaten, Poolrechner?

Gewährleistung der Netz- und Informationssicherheit
- Vertraulichkeit, Verfügbarkeit, Integrität, …

Unbedingt notwendig und verhältnismäßig
- Es gibt nichts, das weniger in „Rechte“ eingreifen, aber gleich effektiv ist
- Verfolgte Ziele, Ausweichmöglichkeiten, Möglichkeit von Ausnahmen

Entscheidungssicherheit (gäbe es z.B. im Telekommunikationsrecht)
- Gesetzliche Vorentscheidung
- Richtung vorgegeben
- Rechtsprechung
- Umsetzung akzeptierter (rechtlicher) Standards (z.B. ISO …)

Verhältnismäßigkeitsmatrix

Bei Patt: Wie gut wird der Zweck wirklich erreicht? Schwere des Eingriffs gelindert durch Ausnahmen / Ausweichen / Kontrolle? Wertung der Verwaltung ebenfalls von Gewicht (Gestaltungsspielraum).		**Intensität des Eingriffs**		
		gering	mittel	schwer
Wertigkeit des verfolgten Ziels	klein	offen	eher nein	nein
	mittel	eher ja	offen	eher nein
	hoch	ja	eher ja	offen

Sicherheitsvorfälle

IT-Sicherheits-Vorfälle

- DFN Informationspflicht (aber meist CERT – Mitglieder)
- Keine geschriebene gesetzliche Meldepflicht
- Ausnahme in § 100 TKG? ➔ Rosinen picken bei der Anwendbarkeit
- Sonderfall Organtreue

Meldepflicht auf alle (bayerischen) Behörden begründet aus dem ungeschriebenen Verfassungs- und Verwaltungsrechtsgrundsatz der Organtreue. Beschränkt mit Blick auf Art. 77 Abs. 2 Verfassung des Freistaates Bayern, soweit eine (erhebliche) Gefährdung anderer Behörden durch den Sicherheitsvorfall besteht.

Sicherheitsvorfälle

Art.

„Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Meldepflicht bei Datenschutzvorfällen! (Art. 33 DSGVO)

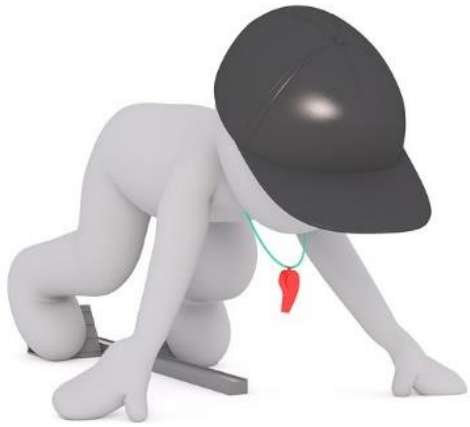
Ausnahme:

… es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

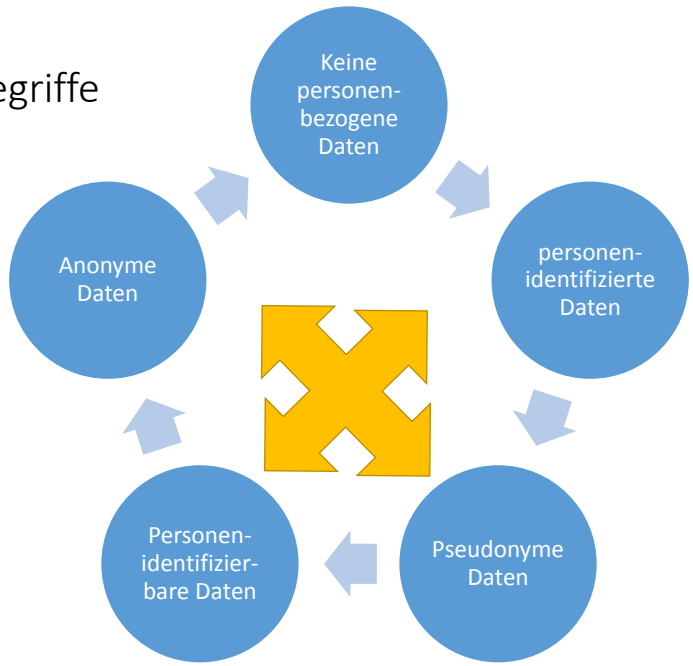
Benachrichtigung der Betroffenen (Art. 34 DSGVO),

wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen durch den Datenschutzvorfall besteht.

Notfallmanagement



Begriffe



Pseudonyme Daten

Gegenüber dem Original verkleinert
Napoleon Vier aus nl Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 nicht portiert“ lizenziert.

Pseudonym = mit Zusatzwissen identifizierbar

Beispiel: Max Müller wird zu ID123
Odysseus zu Οὖτις

Treuhänderische Pseudonymisierung: Ein Dritter entfernt die identifizierbaren Merkmale, in der eigenen Datenbank selbst kein Personenbezug

Eigene Pseudonymisierung: Verwaltungsoberfläche zeigt Daten ohne identifizierbare Merkmale, in einer separaten Datenbank besteht noch mit Personenbezug

Echte anonyme Daten

EuGH Urteil vom 19.10.2016 C-582/14
Wann endet der Personenbezug von Daten?
- sehr hoher personeller Aufwand …
- sehr hoher wirtschaftlicher Aufwand …
- praktisch nicht durchführbar …
- gesetzliche Verbote …

… einen Personenbezug herzustellen

Widerspruch von bestimmt – bestimmbar bzw. identifiziert – identifizierbar?

Maßgeblicher Zeitpunkt
- Erhebung
- Verarbeitungsvorgang

Folge: Regelmäßig prüfen, ob inzwischen Personenbezug besteht

Unterschiedliche Begriffsdefinitionen

Aufsatz Rechtsfragen zu Cloud-Angeboten für Hochschulen

Verarbeiten

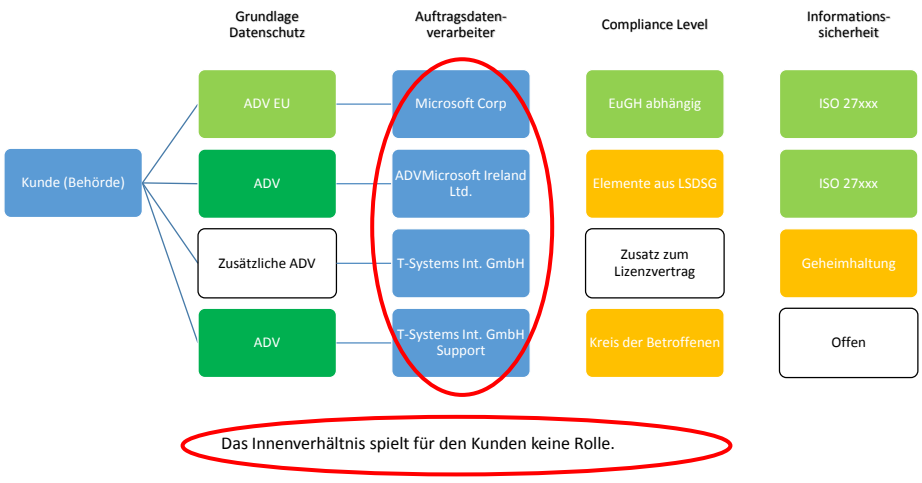
Übermitteln

Dritte

Folgen der unterschiedlichen Begriffsdefinitionen

Einordnung	DS RL	BDSG	DSGVO
Eigene Server EWR	Ja	Ja	Ja
Eigene Server Weltweit	Ja, aber	Ja, aber	Ja, aber
ADV im EWR	Ja	Ja	Ja
ADV weltweit für Unternehmen	Ja, aber	Ja, aber	Ja, aber
ADV weltweit für Behörden	Ja, aber	Ja, aber	Ja, aber

Microsoft Treuhandlösung



Privacy by default und by design

Privacy by Design
➔ Einsatz von Pseudonymen auf Nutzeroberfläche
➔ Richtiger Einsatz von Verschlüsselung
➔ Rollen und Rechtemanagement

Privacy by Default oder Facebook-Klausel
➔ Sichtbarkeit in Portalen erst nach Nutzerinteraktion
➔ Datensparsame Einstellungen bei Telemetrie

Verschlüsselung und Stand der Technik

Stand der Technik immer im Bezug zur jeweiligen Tätigkeit

BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Verschlüsselungscheck für Unternehmen in Bayern

➔Kein RC4, sowenig SHA1 wie möglich und wenn möglich PFS & HSTS

➔DNSSEC und DANE

- Hilfe über https://bettercrypto.org/
- Test über https://www.ssllabs.com/ssltest/
- Linux und Apache Konfiguration prüfen
  - Teiltest über https://observatory.mozilla.org/

8. Risiken

- ☐ Diskriminierung
- ☐ Identitätsdiebstahl
- ☐ Finanziellen Verlust
- ☐ Rufschädigung
- ☐ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
- ☐ Unbefugte Aufhebung der Pseudonymisierung
- ☐ Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

9. Risikoanalyse

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

Ihre Antwort eingeben

Entwurf ADV Check Risikoassessment

Formular und Prüffragen zur Dienst-Beantragung

13. Pflichten gemäß § 7 Benutzungsordnung für Informationsverarbeitungssysteme der Universität Würzburg

- ☐ Nutzerdatenbank
- ☐ Ansprechpartner für die Betreuung
- ☐ NetzVA

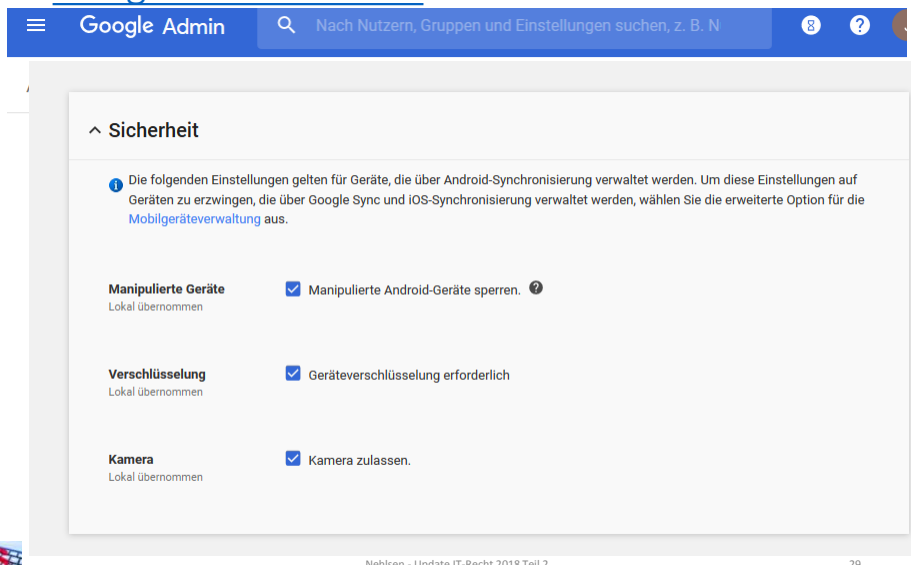
14. Ist der Dienst eine kritische Infrastruktur gemäß § 2 Abs. 10 BSIG i.V.m. mit den sprechenden Verordnungen?

- ○ Ja
- ○ Nein
- ○ Unsicher

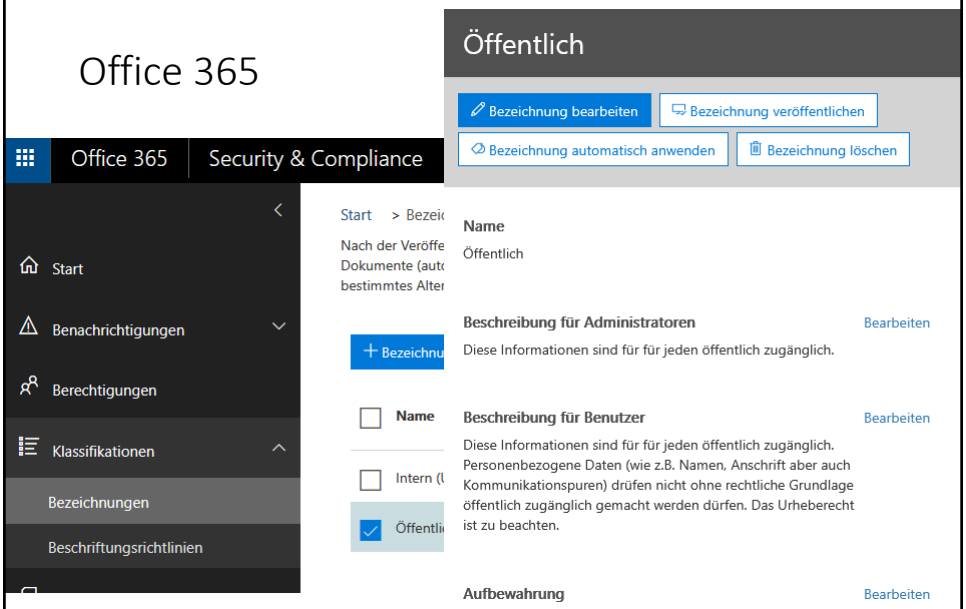
Hilfsmittel zur Umsetzung

- ✓Verzeichnis für Verarbeitungstätigkeiten
- ✓Transparenzpflichten
  https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf
  Bald auch StudiSoft und WebShop
- ✓Fragenkatalog für Softwarebeschaffung
- ✓Handreichung der Teletrust zum Stand der Technik
- ✓Empfehlung des BSI
- ✓ IT-Strategie
  - DFG
  - Gemeinsame Orientierungshilfe der Rechnungshöfe

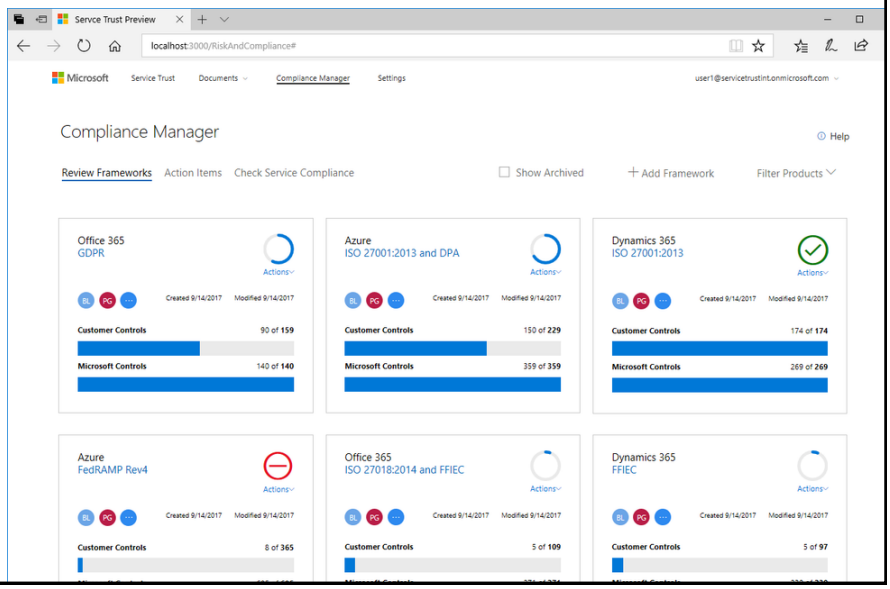
Google for Education



Office 365



Microsofts (Office 365) Compliance Manager



Beispiel für Lücke durch neue Rechtsprechung

Bisher:

- Starke Einschränkungen beim Umgang mit Nutzungsdaten für Anbieter von Webseiten und Apps
- Abgebildet in zahlreichen IT-Benutzungsordnungen

Änderungen:

- BGH Urteil Az. VI ZR 135/13 - 16. Mai 2017
- EuGH C-582/14 - 19.10.2016 (Fall Breyer)
- § 13 Abs. 7 TMG mit Vorgaben zur Dienstgestaltung 25. Juli 2015

Folge: IT-Benutzungsordnungen können zu eng sein!

Empfehlung: Ob § 11 – 15 TMG ab Mai 2018 unter der DSGVO weiter Gültigkeit entfallen ist stark umstritten. Daher ist eine Anpassung der IT-Benutzungsordnungen nach DSGVO vorzugswürdig.

(Neben-)Compliance

- Vergaberecht
  - ➔ Prozesssicherung bei Unterschwellenvergaben
- Urheberrechte
  - ➔Lizenzmanagement
  - ➔ Clearing von Hosting und Vermietungen
  - ➔ Sicherer Bilderpool für den Webauftritt
  - ➔ Gute Anleitung für die Lehre
  - ➔ Trennung von Lehre und kommerzieller Weiterbildung
- Rundfunk
  - ➔ Prüfung der Häufigkeit von Livestreams
  - ➔ Beobachtung der Rechtsentwicklung
- Jugendschutz
  - ➔ Ernsthaft Prüfung der Notwendigkeit
- Arbeitsschutz
  - ➔ Prüfung der Dokumentation und Ergänzung der Gefährdungsanalysen

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