



Teams in deutschen Amtsstuben?

Johannes Nehlsen



Über mich

- Volljurist
 - Studium LMU München
 - Referendariat OLG München
 - Wahlstation bei Eversheds UK
- Rechtsinformatikzertifikat an der Ludwig-Maximilians-Universität
- Zertifikat (OTH Regensburg) Informationssicherheitsbeauftragter
- Microsoft Licensing Professional (von vor einigen Jahren)
- Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
 - Datenschutz
 - E-Government
 - E-Procurement
 - IT-(Sicherheits-)recht
 - Urheberrecht
 - ➔ Beantwortung der IT-Rechtsfragen von strategischer hochschulübergreifender Bedeutung

Keine Themen für heute

- Eine Erklärung, was Teams ist.
- Eine Prüfung, ob die Auftragsverarbeitung von Microsoft den gesetzlichen Anforderungen genügt.
- Eine rechtliche Lösung für echte Clouddienste mit Bezug zu den Vereinigten Staaten von Amerika.
- Feinheiten aus öffentlich-rechtlichen und gesetzlichen Geheimhaltungs- und Vertraulichkeitsverpflichtungen.
- Grenzen aus Melderecht oder den Landeskrankenhausgesetzen.

Wie geht's?



https://commons.wikimedia.org/wiki/Category:Freilichtmuseum_Beuren#/media/File:Beuren-freilichtmuseum-14-rathausH2a.jpg

Einfach machen!

Microsoft Teams for Education

Zum 13. Mai 2020 wurde den weiterführenden Schulen in Bayern Microsoft Teams ergänzend zu den Angeboten von mebis zur Verfügung gestellt.

Nähere Informationen zu diesem Angebot finden Sie auf der Homepage des Staatsministeriums für Unterricht und Kultus (StMUK).

Die **Akademie für Lehrerfortbildung und Personalführung (ALP)** bietet sowohl **E-Sessions** als auch **Selbstlernkurse** zu Microsoft Teams an.



[Informationen des StMUK](#)

[E-Sessions der ALP](#)

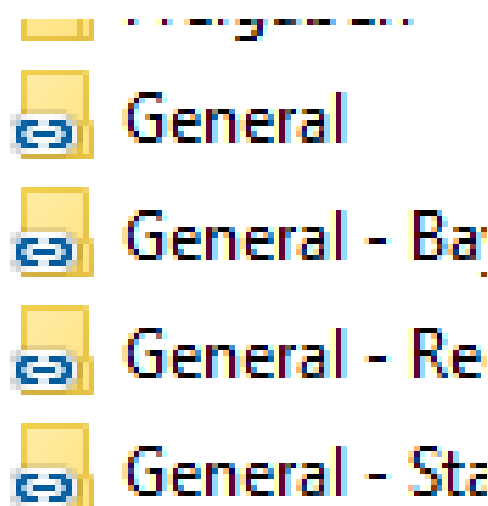
[Selbstlernkurse der ALP](#)

<https://www.mebis.bayern.de/infoportal/empfehlung/microsoft-teams/>

Was fehlt (möglicherweise)?

- Grünes Licht für risikoscheue Entscheider
- Überzeugen bei ethischen oder moralischen Ansichten
- Schnittstellen in Dienste für das Online-Zugangsgesetz
- Schnittstelle zu Identitäten
 - eduGAIN / DFN AAI
 - eID
- Schnittstellen zu digitalen Postfächern
 - DE-Mail
 - beA
 - beN
 - beBPo

Ordnungsgemäße Aktenführung (ähnlich GoBD)

- [Positionspapier zum Thema Aktenführung](#) (Rechnungshöfe Bund und Länder)
 - Die öffentliche Verwaltung ist verpflichtet,
 - Akten zu führen (Gebot der Aktenmäßigkeit),
 - alle wesentlichen Verfahrenshandlungen vollständig und nachvollziehbar abzubilden (Gebot der Vollständigkeit und Nachvollziehbarkeit) und
 - diese wahrheitsgemäß aktenkundig zu machen (Gebot der wahrheitsgetreuen Aktenführung).
 - Sicherheit von Authentizität und Integrität
 - Aufbewahrungsgebot (Langfristige Sicherung)
 - Anbieten an das Archiv
nach 10 bzw. 30 Jahren vor dem Löschen
- 
- General
 - General - Ba
 - General - Re
 - General - Sta

Anforderungen an die E-Akte

- Schnelle Auffindbarkeit
- Mobil
- Medienbruchfrei
- Standardisierung
- Automatisierung von Geschäftsprozessen
- Revisionssicherheit
- Vereinfachter Austausch
- Verringerung der Sachausgaben
- Verringerung der Personalausgaben
- Transparenz des Verwaltungshandelns
- Barrierefreiheit
- Bürgerfreundlichkeit

Einige der zu betrachtenden Risiken ...

- Wirtschaftlichkeit
- Digitale Souveränität
- Barrierefreiheit
- Umweltschutz
- Nachhaltigkeit
- Agile Entwicklung
- Fehlerfreiheit Anwendungen
- Vertraulichkeit nach § 203 StGB
- Vertraulichkeit nach § 353b StGB
- Vertraulichkeit
- Internationale Verfügbarkeit
- US-Export-Recht
- Verfügbarkeit der Konfiguration
- Verfügbarkeit der abgelegten Daten
- Integrität
- Diskriminierung
- Identitätsdiebstahl oder –betrug
- Finanzielle Verluste
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten
- unbefugte Aufhebung der Pseudonymisierung
- Andere erhebliche wirtschaftliche Nachteile
- Andere gesellschaftliche Nachteile
- Hinderung oder Verlust bei der Ausübung von Rechten und Freiheiten
- Kontrollverlust über die eigenen personenbezogenen Daten
- Ausfall oder Störung von Kommunikationsnetzen
- Ausfall oder Störung von Dienstleistern (WAN)
- Ausspähen von Informationen (Spionage)
- Abhören
- Verlust von Geräten, Datenträgern oder Dokumenten
- Fehlplanung oder fehlende Anpassung
- Offenlegung schützenswerter Informationen
- Manipulation von Informationen
- Ausfall von Geräten oder Systemen
- Verstoß gegen Gesetze oder Regelungen
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- Missbrauch von Berechtigungen
- Nötigung, Erpressung oder Korruption
- Social Engineering
- Identitätsdiebstahl
- Sabotage
- Datenverlust
- ...

Digitale Souveränität = Art. 33 Abs. 4 GG

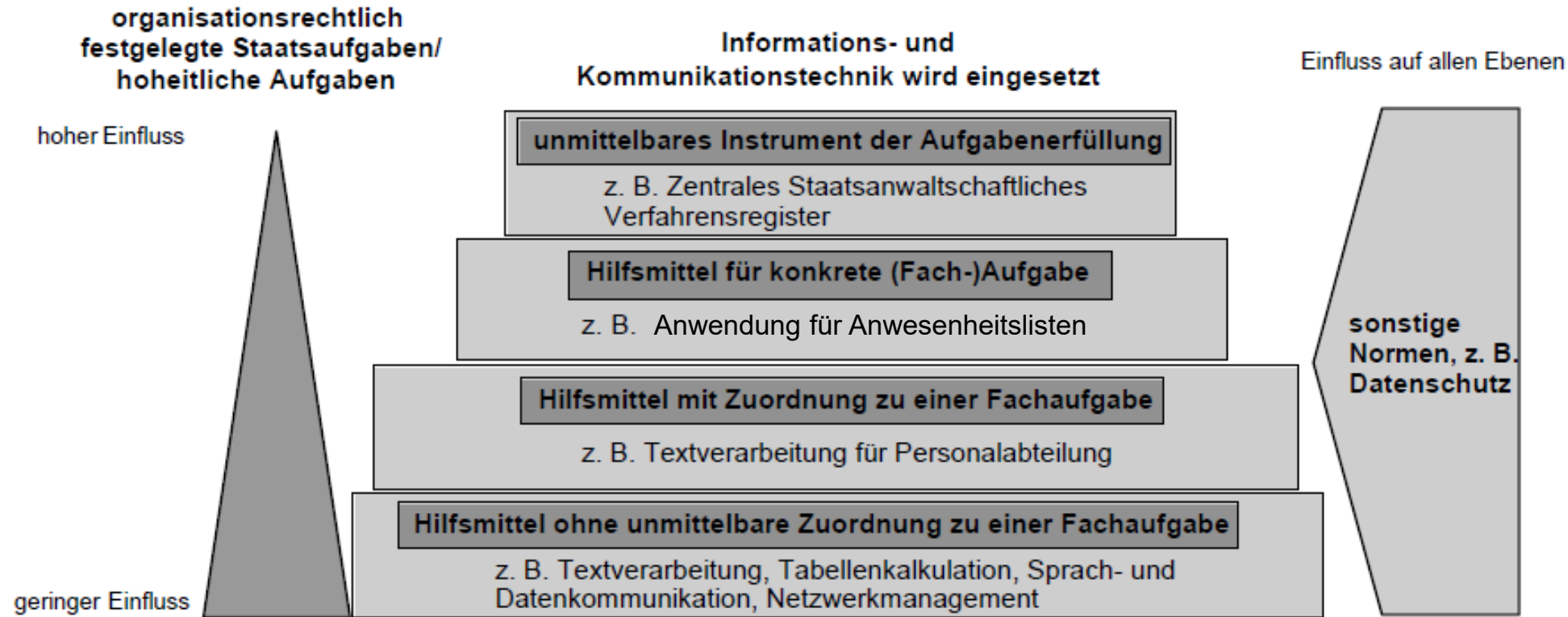


Abbildung 1: Einfluss hoheitlicher Aufgaben und sonstiger Normen auf das luK-Outsourcing

Umsetzung: [Leitsätze der Rechnungshöfe für die Prüfung von luK-Outsourcing](#) S. 6

Herausforderungen – Informationssicherheit

Fefes Blog

Wer schöne Verschwörungslinks für mich hat: ab an felix-bloginput (at) fefe.de!

Fragen? [Antworten!](#) Siehe auch: [Alternativlos](#)

Mon Dec 7 2020

- [\[1\]](#) Leserbrief zu Teams:

zu Teams habe ich noch ein Ärgernis aus dem Feldeinsatz, das banal klingt, aber durchaus sicherheitsrelevant sein kann: die Anwendung klagt beim Öffnen den Eingabefokus. Und das ist nicht neu, siehe diesen Post von 2017:

[Forumsposting bei Microsoft](#)

Szenario: direkt nach dem Windows-Login einen Browser starten, um sich an einer Cloud-Anwendung anzumelden. Während der Passwort-Eingabe öffnet sich Teams etwas verzögert auf einem anderen Monitor mit dem Chat vom Vortag, zieht den Textcursor aus dem Browser-Passwortfeld ab und setzt ihn in seinem Chat ein. Sobald die Return-Taste gedrückt wird, ist die Unterhaltung um ein Geheimnis reicher.

Dieses Szenario ist so unrealistisch, dass es mir schon zweimal passiert ist (ja ja, fool me twice). Ich bin nur froh, dass meine Passwörter aktuell keine Schimpfwörter beinhalten. Man kann den Post zwar nachträglich löschen, aber er verschwindet nicht völlig aus dem Chat, sondern wird eine Weile als gelöscht markiert dargestellt. Alles sehr vertrauenswürdig.

Ich hab ja auch schon ein-zwei Mal bei Kunden Slack oder Teams einsetzen sollen und war jedesmal erschüttert, was für ein offensichtlicher Ranzkack das ist. Träge wie Treibsand, produktivitätsvernichtend wie Treibsand, ... wenn es dabei den Blutdruck nicht so hochtreiben würde, könnte man fast von einer Entschleunigung reden und es als Wellness-Maßnahme verkaufen.

Mir ist ja die ganze Zeit schon nicht klar, wieso irgendjemand seine eigenen Mitarbeiter mit sowas torpedieren würde.

Aber dann hab ich mir gedacht: Vielleicht ist das wie bei Behörden. Da bemisst sich die Wichtigkeit eines Abteilungsleiters ja auch daran, wie viele Leute der unter sich hat. Je mehr desto wichtiger. Das schafft Anreize, mehr Personal zu brauchen. Welche Maßnahme eignet sich besser als das gezielte Ausbremsen der Mitarbeiter durch Sabotagesoftware wie Slack oder Teams? Früher hat man dafür Großraumbüros und tägliche Statusmeetings gemacht, aber das ist ja mit Covid nicht mehr so möglich. Also muss man irgendwie anders verhindern, dass die Mitarbeiter keine komplexeren Gedanken fassen können.

In diesem Sinne: Teams ist das neue Großraumbüro.

[ganzer Monat](#)

Proudly made without PHP, Java, Perl, MySQL and Postgres
[Impressum](#) [Datenschutz](#)

<https://blog.fefe.de/?q=teams+fokus>



Best Practices

Trust and Safety

▲ Includes front-end JavaScript libraries with known security vulnerabilities — 24 vulnerabilities detected

Some third-party scripts may contain known security vulnerabilities that are easily identified and exploited by attackers.

[Learn more.](#)

Library Version	Vulnerability Count	Highest Severity
Bootstrap@3.3.7	5	Medium
jQuery@3.3.1	3	Medium
Lo-Dash@4.17.4	7	High
AngularJS@1.5.14	9	High

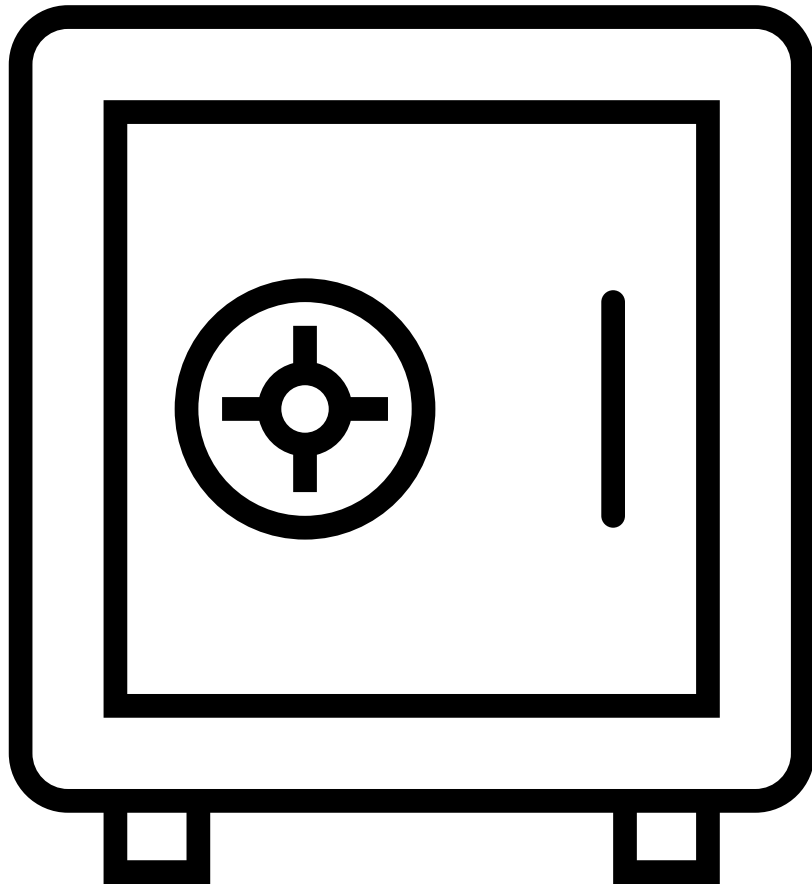
General

▲ Registers an `unload` listener

▲ Browser errors were logged to the console

▲ Missing source maps for large first-party JavaScript

Herausforderungen – § 203 StGB



- Geschützt sind alle fremden Geheimnisse (auch Verstorbener)!
- Wer muss u.a. darauf achten:
 - Betriebsarzt
 - Datenschutzbeauftragte
 - Personalrat
- Jeder Amtsträger, dem etwas offenbart worden ist
- Mitwirkung (fremder) IT-Dienstleister nur sofern und soweit „erforderlich“
→ (P) Nutzung von Kundendaten auch für eigene Zwecke durch Microsoft
- Unbegrenzte Geheimhaltungsverpflichtung bezogen auf „fremde Geheimnisse“ (nicht nur Kundendaten)

Herausforderungen – Personaldatenschutz



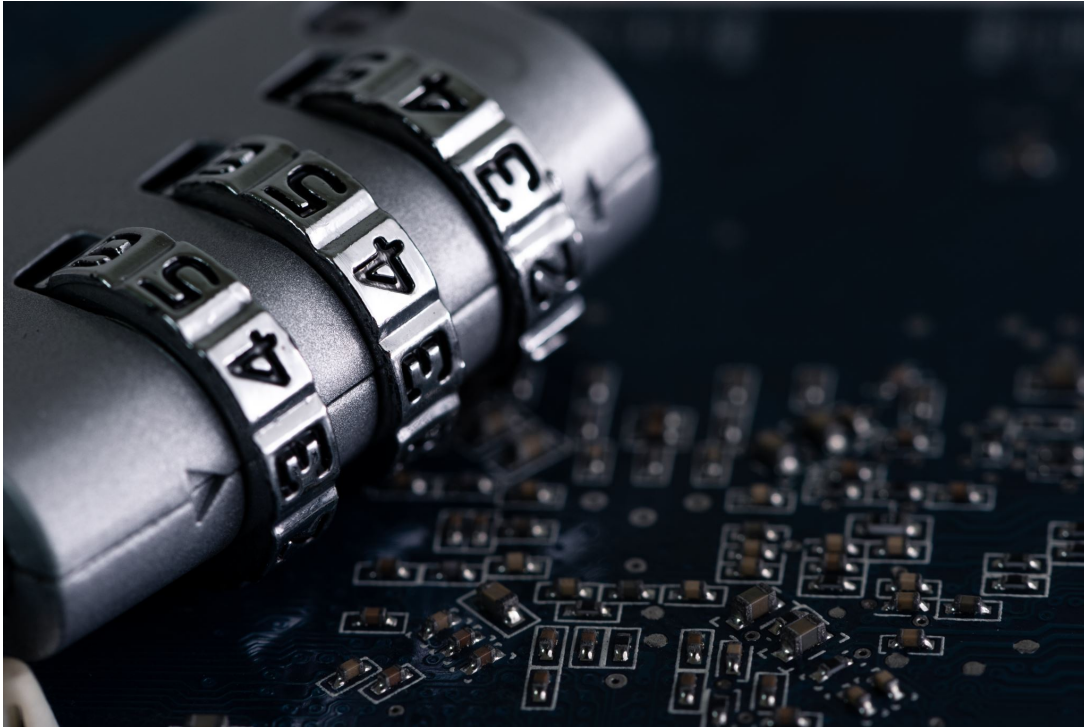
- Mitbestimmung (allgemein)
- Umfasst alle Personalaktendaten (etwa Art. 104 BayBG, § 85 LBG NRW)
 - ➔ Grenzbereich insbesondere Empfang von Bewerbungen, Krankmeldungen, Zeugnisentwürfe, Schichtplanungen, ...
- Auftragsverarbeitung in Bayern, Art. 108 Abs. 3 BayBG
 - Lösung des Auftragsverarbeiters muss essentiell für den Betriebsablauf sein oder Lösung des Auftragsverarbeiters muss erheblich kostengünstiger sein
 - Verpflichtung nach Verpflichtungsgesetz für nicht öffentliche Auftragsverarbeiter erforderlich

Herausforderungen – Sozialdatenschutz



- Umfasst alle Sozialdaten (§ 67 Abs. 1 SGB X)
- Auftragsverarbeitung geregelt in § 80 SGB X
 - Anzeigepflicht bei der eigenen Rechts- oder Fachaufsicht
 - Außerhalb des EWR nur zulässig bei Angemessenheitsbeschluss
 - ➔ Aktuell daher wenn Übermittlungen in die USA erfolgen nicht möglich
 - Lösung des Auftragsverarbeiters muss essentiell für den Betriebsablauf sein und Lösung des Auftragsverarbeiters muss erheblich kostengünstiger sein
 - ➔ Rückausnahme nur mehrheitlicher Kontrolle durch Bund und Länder
- Wertung für Daten mit Bezug zum Sozialrecht übertragbar?

Herausforderungen – Datenschutz



- Bewertung der Auftragsverarbeitung (u.a. Core-Services)
- Bewertung von Diensten ohne Auftragsverarbeitung
- Dienste von Dritten (Arbeitsbeschaffungsmaßnahme für Jurist:innen)
- Teile in Verantwortung von Microsoft soweit E-Privacy-RL wegen EECC?

Herausforderungen – Urheberrecht



- Gifs oft nur unter „Fair use“ in den Vereinigten Staaten nutzbar
- Habe ich überhaupt Rechte die Dateien mehrfach oder in der Cloud (ggf. in mehreren Ländern) zu speichern?
- Tipp für DE: Jedenfalls Gifs in Teams deaktivieren ... ;-(
- Wo kein Kläger, da kein ...

(Teil-)Checkliste

- Entscheidung der Leitung mit Restrisikenübernahme
- Ordnungsgemäße Aktenführung
- Barrierefreiheitserklärung
- Ggf. Antrag bei der zuständigen Finanzbehörde
- Mitbestimmung
- Datenschutzdokumentation und –information
- Keine Gifs, keine Memes, ...
- White-Listing für Apps, Bots, ...
- Grenze der zulässigen Teams-Integration (u.a. Art. 33 Abs. 4 GG)

Hochschulthemenseite unter <https://go.uniwue.de/ms-gdpr>

Vielen Dank für Ihre Aufmerksamkeit!



Kontakt:

Johannes Nehlsen

Johannes.nehlsen@uni-wuerzburg.de

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

Twitter privat: @JoNehlsen

Nehlsen – Teams in deutschen Amtsstuben?

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