Datenklassifizierung als Schlüssel für Cloudnutzung

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

Ihr Referent

Haupttätigkeit:

Stabsstelle IT-Recht
der bayerischen staatlichen Universitäten und Hochschulen

Hintergrund:

- Volljurist
  Studium Ludwig-Maximilians-Universität
  Referendariat OLG München, Wahlstation bei Eversheds UK
- Rechtsinformatikzertifikat an der Ludwig-Maximilians-Universität
- Zertifikat Informationssicherheitsbeauftragter (OTH Regensburg)
- Microsoft Licensing Professional
- Twitter privat: @JoNehlsen

Digitale Souveränität = Art. 33 Abs. 4 GG

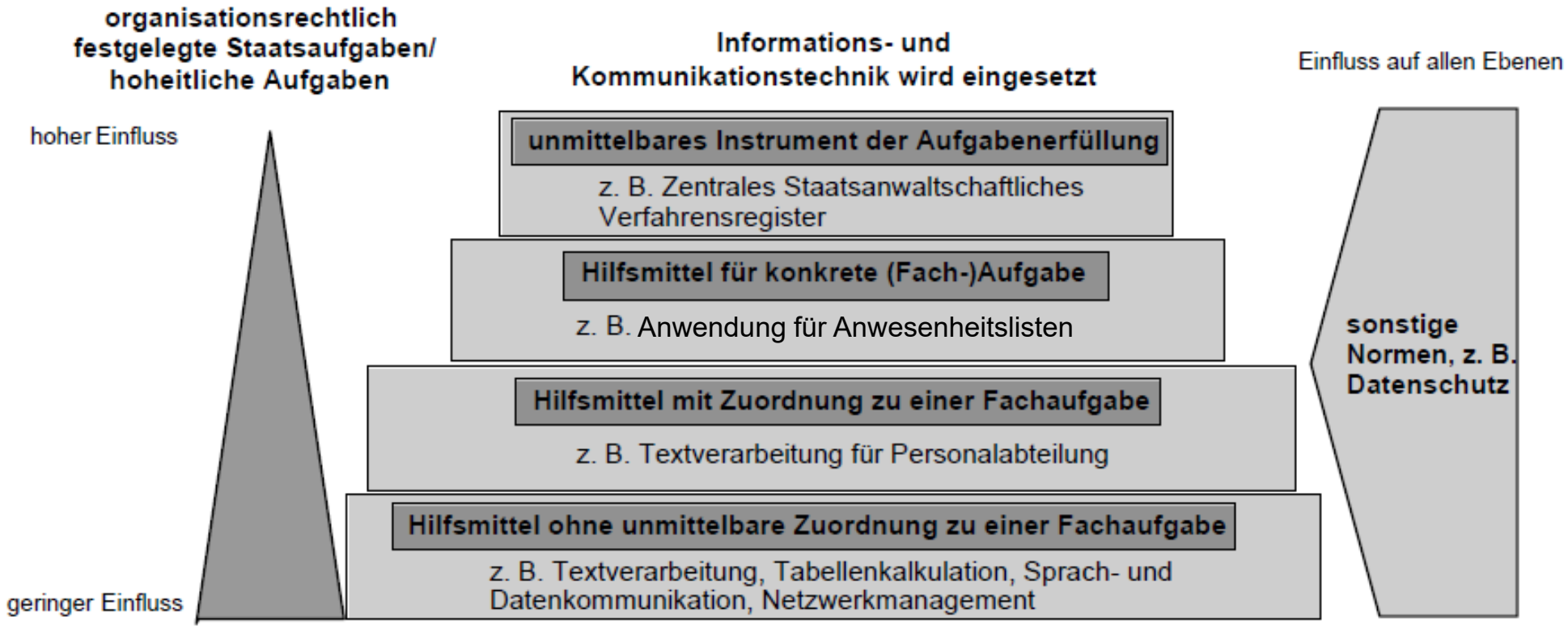

Abbildung 1: Einfluss hoheitlicher Aufgaben und sonstiger Normen auf das IuK-Outsourcing

Umsetzung: Leitsätze der Rechnungshöfe für die Prüfung von IuK-Outsourcing S. 6

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)

Kennen Sie Ihren Aktenplan?

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

Personalaktenrecht

- Umfasst alle Personalaktendaten (etwa Art. 104 BayBG, § 85 LBG NRW)
  ➔ Grenzbereich insbesondere Empfang von Bewerbungen, Krankmeldungen, Zeugnisentwürfe, Schichtplanungen, …
- Auftragsverarbeitung in Bayern, Art. 104 Abs. 3 BayBG
  - Lösung des Auftragsverarbeiters muss essentiell für den Betriebsablauf sein und Lösung des Auftragsverarbeiters muss erheblich kostengünstiger sein
  - Verpflichtung nach Verpflichtungsgesetz für nicht öffentliche Auftragsverarbeiter erforderlich
- Auftragsverarbeitung in NRW, § 91a LBG NRW
  - Besondere Vertragsvorgaben
  - Lösung des Auftragsverarbeiters muss essentiell für den Betriebsablauf sein und Lösung des Auftragsverarbeiters muss erheblich kostengünstiger sein
  - Gesonderte Geheimhaltung auf den Schutz der Personalaktendaten
  - Unteraufträge sind individuell zustimmungspflichtig

Aus sonstigen Rechtsgebieten

Steuerrechtlich relevante Unterlagen, § 146 AO

➔ Speicherung in Deutschland oder Ausnahme bei der zuständigen Finanzbehörde beantragen

Urheberrecht

➔ Begrenzung bei Materialien aus § 60a UrhG auf den Teilnehmerkreis

Gesetz zum Schutz von Geschäftsgeheimnissen

➔ Erforderlichkeit von angemessen Geheimhaltungsmaßnahmen

Datenschutz

➔ Risikoangemessene Maßnahmen

Telemedienrecht

➔ Neben Datenschutz auch Zugriffsschutz und Gewährleistung der Verfügbarkeit

Archivrecht

➔ Vor dem Löschen müssen Daten auf ihre Archivwürdigkeit geprüft werden

Vorklassifizierung aus dem Datenschutz

Datenkategorie	Norm	Standardschutzbedarf
Nicht personenbezogene Daten	Art. 2 Abs. 1 DSGVO	Nicht nach Datenschutz
Identifizierbare personenbezogene Daten	Art. 1 Abs. 1 Alt. 2 DSGVO	Ja
Pseudonyme personenbezogene Daten	Erwägungsgrund 26 DSGVO	Ja
Identifizierte personenbezogene Daten	Art. 1 Abs. 1 Alt. 1 DSGVO	Ja
Personenbezogene Daten unter Berufsgeheimnis	Erwägungsgrund 85 DSGVO	Gesteigert
Personenbezogene Daten aus der Personalakte bzw. unter Sozialgeheimnis, Steuergeheimnis oder besonderen Amtsgeheimnis		Gesteigert
Personenbezogene Daten Minderjähriger	Erwägungsgrund 75 DSGVO	Gesteigert bis erheblich gesteigert
Besondere Verarbeitungsformen, insbesondere große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen	Erwägungsgrund 75 DSGVO	Gesteigert bis erheblich gesteigert
Besondere Kategorien personenbezogener Daten: • rassische und ethnische Herkunft • politische Meinungen, • religiöse oder weltanschauliche Überzeugungen • Gewerkschaftszugehörigkeit • genetischen Daten, • biometrischen Daten • Gesundheitsdaten oder • Daten zum Sexualleben • Daten der sexuellen Orientierung	Art. 9 DSGVO	Erheblich gesteigert
Personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten	Art. 10 DSGVO	Erheblich gesteigert

Beispiel einer Klassifizierungsrichtlinie

- Vorschlag der Stabsstelle Informationssicherheit der bayerischen staatlichen Universitäten und Hochschulen

Vertraulichkeitsstufe ->	öffentlich (V1)	intern (V2)	<Kürzel> vertraulich (V3)	Streng vertraulich (V4)
Informationsgruppe ->	Beispiele: Vorlesungsverzeichnis, Pressemitteilungen Flyer, öffentliche Teile der Webseite, öffentliche Veranstaltungsprogramme	Beispiele: Intranet, Regelwerke, Arbeitsanweisungen, Schriftverkehr, E-Mails der Abt. Kommunikation, interne Telefonverzeichnisse, interne Veranstaltungen	Beispiele: personenbezogene Daten, Reise-, Lohnabrechnung, Forschungsdaten, techn. Daten (Baupläne sensibler Räume, Netzwerkpläne), geschützte Studienarbeiten, Prüfungswesen	Beispiele: in Zusammenarbeit mit Dritten (Militär, Forschung, Wirtschaft) aus einer dienstlichen oder vertraglichen Verpflichtung
Maßnahmen für Dokumente				
Zugriffsschutz/Zugang zu Informationen	keine Einschränkung	Der Zugriff ist auf Hochschul-/Universitätsangehörige im notwendigen Umfang beschränkt.	Der Zugriff ist gemäß dem Grundsatz "Kenntnis nur, wenn erforderlich"	Genehmigung durch Informationseigentümer/-in starke Authentisierung
Speichern auf Netzlaufwerken mit Zugriffsschutz oder internen Cloudsystemen	unverschlüsselt	unverschlüsselt	unverschlüsselt	verschlüsselt
Speichern auf externen Cloudsystemen	unverschlüsselt	unverschlüsselt (ADV)	verschlüsselt (ADV)	verschlüsselt (ADV)

Beispielhafte Regelung für persönliche Dienste ohne Auftragsverarbeitung (etwa Grammarly)

Erlaubt

- Urheberrecht
  Verarbeitung von (beabsichtigten) Zitaten und eigene Texten
- Datenschutz
  Eigene und veröffentlichte Personenbezogen Daten (z.B. Namen von Autorinnen und Autoren)

Verboten

- Daten mit Bezug zur Personalakte
- Gutachten und Korrekturen
- Finanzdaten
- Sozialdaten
- Unveröffentlichte Daten
- Verträge und „Veraktetes“

Beispielhafte Festlegung für Microsoft 365

- Zu jedem Dienst von Microsoft 365 gibt es auch ein Alternativangebot
- Komplette Synchronisation von pseudonymen Accounts ohne Benutzerprofil und Geräten zur Lizenzaktivierung und Gerätemanagement
- Opt-In und zusätzlicher Benutzerordnung für die Clouddienste, insbesondere Teams und OneDrive for Business (einschließlich Klarnamen
- Übliche Aktenführung und Ablage von Finanzdaten möglich, wenn lokal ein Backup der Daten vorgehalten wird
- Umfassende Konfiguration der Sicherheitseinstellungen in Microsoft 365
- Klassifizierung z.B. mit Öffentlich, Lehrmaterial, Intern (Default), Vertraulich
- Aufbewahrungsrichtlinie auch zur Beurteilung der Archivwürdigkeit von Daten
- Nutzung für anvertraute Geheimnisse (z.B. Prüfungen) und Daten aus der Tätigkeit von Berufsgeheimnisträgern (z.B. Personalrat) nur mit zusätzlicher Geheimhaltungsvereinbarung
- Sozialdaten (z.B. Kommunikation mit Schwerbehindertenvertretung) und Personalaktendaten (z.B. die Nebenakten und in diese Aufzunehmende Kommunikation, z.B. erhaltene Krankmeldung)
  ➔ Exchange verbleibt lokal zusätzlich wird Verschlüsselung mit DFN-PKI angeboten
  Alternative bei Wirtschaftlichkeit: Proxydienste oder eigenes Key-Management + A5
- Alle Zusatzdienste (z.B. Übersetzung, Untertitel, besondere Funktionen für die Barrierefreiheit)
  ➔ Nutzung wird nur nach Belehrung, Vorgaben und mit Opt-In freigeschaltet

Checkliste zu Cloudprojekten

- Auftragsverarbeitung tragbar, aber Fragen zum internationalen Datentransfer leider offen.
- Tauglich bei Risikoübernahme i.d.R. ohne ergänzende Maßnahmen bis für Klassifikation „Intern“
- Nur kontrolliertes Outsourcing zulässig, da Hilfsmittel auch für konkrete Fachaufgaben ➔ Gleichzeitiger Aufbau von Alternativen
- Gutes Informationssicherheitskonzept und Funktionalitäten, jedoch einiges jeweils bei der Hochschule umzusetzen (etwa Multi-Faktor-Login, Labels für Klassifizierung), daher geeignet für Telemediendienste und für zu schützende Geheimnisse
- Schutz für anvertraute Geheimnisse und Berufsgeheimnisträger darf zusätzlicher Geheimhaltungsvereinbarung
- Anbieter gewährleistet Verfügbarkeit ➔ Backup bleibt Aufgabe der Hochschule
- Zusätzlicher Schutz (eigene Verschlüsselung und eigenes Key-Management) für „Kronjuwelen“
- Ggf. lokale Lösung für Sozialdaten und Personalakten wirtschaftlicher ➔ Cloud-Kommunikation nur für Studierende ohne Funktionen, Ämter oder Hilfskrafttätigkeit

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 – Datenklassifizierung als Schlüssel für Cloudnutzung