The law and the Public Cloud for the Public Sector

Johannes Nehlsen

GLOBAL SECURITY AND COMPLIANCE COMMUNITY CONFERENCE

08 FEBRUARY 2021

Sponsor

Gesellschaft für Digitalisierung und digitalen Fortschritt e.V.

http://gdf-digital.org/

Johannes Nehlsen

- Volljurist, Regierungsrat, DSB, ISB, …
- 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 in Bayern

Agenda

- Ordnungsgemäße Aktenführung
- Nachhaltigkeit (u.a. Barrierefreiheit und Klimaziele)
- Auftragsverarbeitung und Kommunikationsdienstleistungen
- Vertraulichkeit – § 203 StGB
- Sozialdatenschutz
- Personaldatenschutz
- Patientendatenschutz
- Digitale Souveränität

Public Cloud als Partner für die Verwaltung

Was verlangen die Anbieter?

Beispiel: Microsoft Online Services Data Protection Addendum, Last updated December 9, 2020

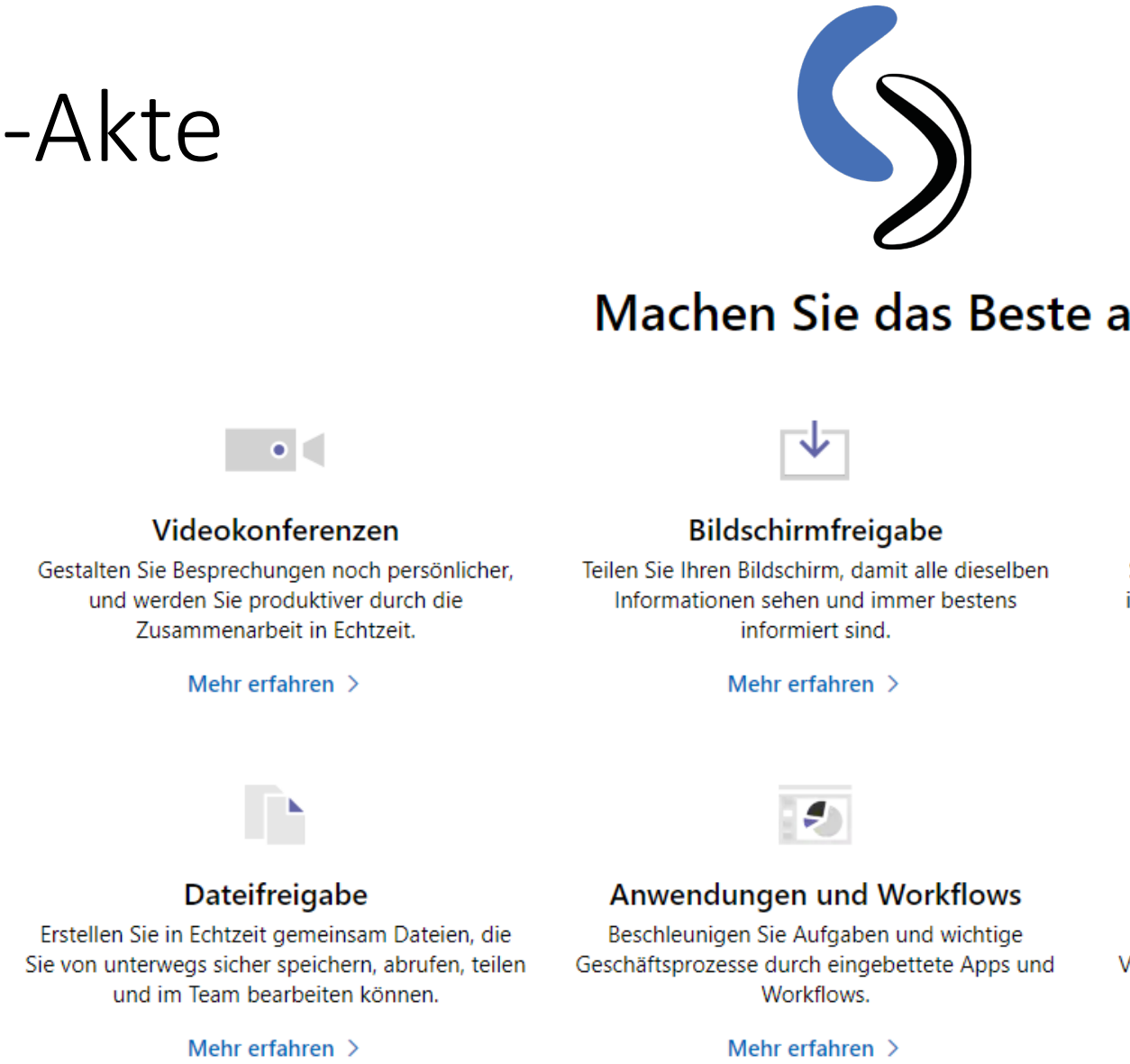
„Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Online Services in a manner consistent with Customer's legal and regulatory obligations."

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 zu gewährleisten,
  - Aufbewahrungsgebot (Langfristige Sicherung) zu erfüllen.
- Anbieten an das Archiv nach 10 bzw. 30 Jahren vor dem „Löschen“.

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

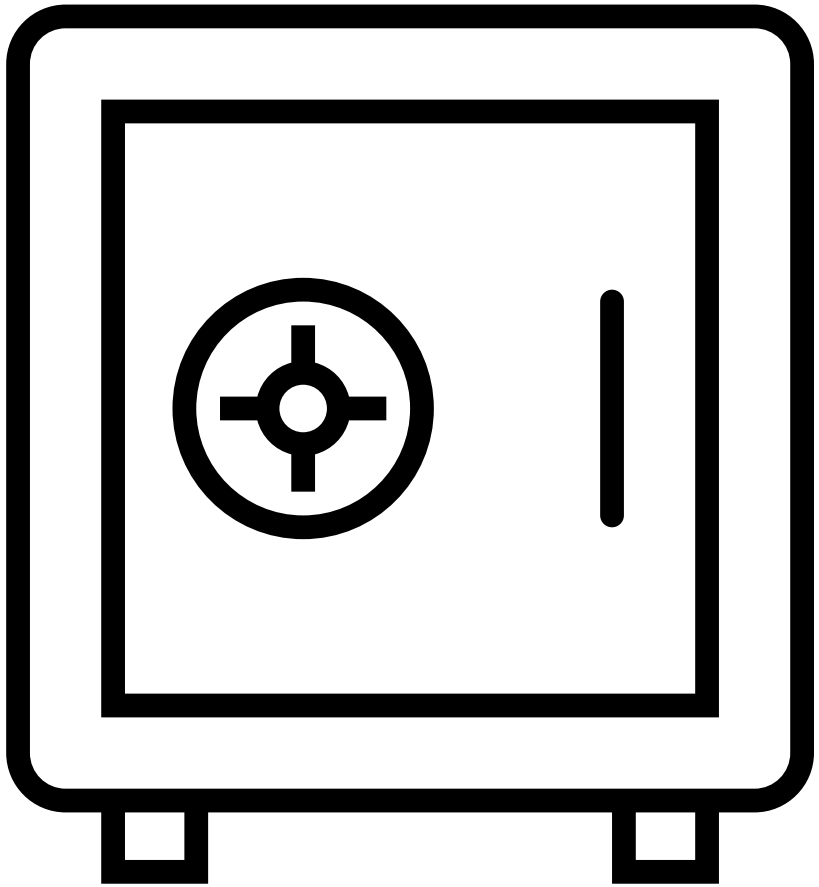


Nachhaltigkeit

Art. 3 GG

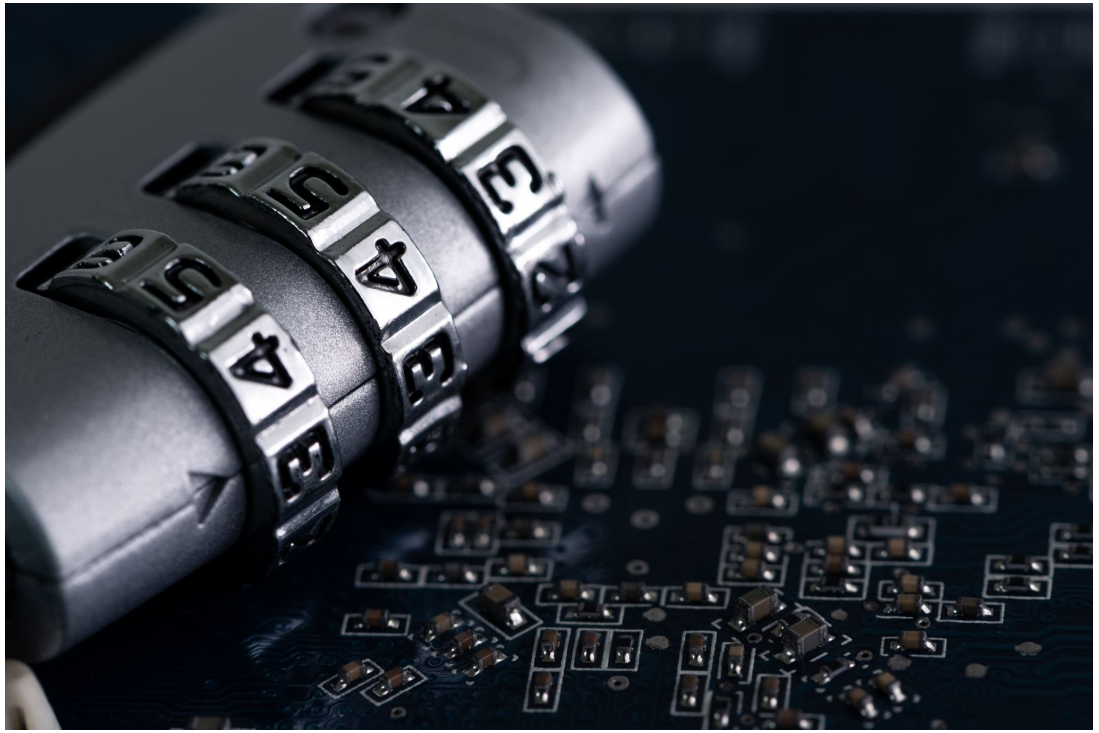
Art. 20a GG

Herausforderungen – § 203 StGB



- Geschützt sind alle fremden Geheimnisse (auch Verstorbener)!
- (P) Lernergebnisse von KI mit vom Schutz umfasst?
- Wer muss u.a. darauf achten:
  - Betriebsarzt, Datenschutzbeauftragte, Personalrat
  - Jeder Amtsträger, dem etwas offenbart wird
- Mitwirkung (fremder) IT-Dienstleister nur sofern und soweit „erforderlich“
  ➔ Externe IT, ja, aber (P) Nutzung von Kundendaten auch für eigene Zwecke
- Zeitlich unbegrenzte Geheimhaltungsverpflichtung bezogen auf „fremde Geheimnisse“ (nicht nur Kundendaten)
- Verpflichtung der Dienstleister zu dieser Geheimhaltung erforderlich

Herausforderungen – Datenschutz



- Bewertung der Auftragsverarbeitung
- Für welche Dienste findet die Auftragsverarbeitung Anwendung?
- Marktplätze für Apps von Drittanbietern
- Teile in Verantwortung vom Anbieter soweit E-Privacy-RL wegen des europäischen Code für elektronische Kommunikation?

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
    oder Lösung des Auftragsverarbeiters muss erheblich kostengünstiger sein
    ➔ Rückausnahme nur mehrheitlicher Kontrolle durch Bund und Länder
- Wertung für Daten mit Bezug zum Sozialrecht übertragbar?

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

Patientendatenschutz

Beispiel: Art. 27 BayKrG

- Abs. 4 S. 5 ➔ Auftragsverarbeitung nur soweit keine schutzwürdigen Belange der Patienten beeinträchtigt
- Abs. 6 ➔ besondere Schutzmaßnahmen technischer und organisatorischer Art, insbesondere gegen nicht unberechtigte Verwendung oder Übermittlung
- (P) Nutzung der Daten durch den Dienstleister für eigene Zwecke

(P) Diensteanbieter nutzt Kundendaten für eigene Zwecke

1. **Denkbare Zweckänderungen aus der Auftragsverarbeitung**
   - Verbesserung der Barrierefreiheit ➔ (P) Datenintensiv
   - Verbesserung der Energieeffizienz ➔ (P) Indirekte Leistungsdaten
   - Verbesserung der Sicherheit ➔ (P) Sprechende URLs, Dateinamen und Betreffzeilen
   - Produktverbesserungen aus eingegangen Fehlermeldungen
2. **Außerhalb der Auftragsverarbeitung**
   - Kompatibilitäts- und Sicherheitsupdates (Wertung aus RL 2019/770/EU)
   - Zwingend zur Abrechnung und Berichterstattung erforderliche Nutzungs- und Kontaktdaten
   - Erlaubte Datenverarbeitungen sofern regulierter Kommunikationsdiensteanbieter mit gesetzlichen durch das Strafrecht geschützten Vertraulichkeitspflichten

Daten aus 1 und 2 dürften inkompatibel zu weiteren Zweckänderung sein und Anonymisierung ist als Verarbeitungsschritt ebenfalls zu rechtfertigen!

Besondere Herausforderungen abseits von 1 und 2

- Forschung und Produktweiterentwicklung
- Offenlegungen entgegen Art. 48 DSGVO

Herausforderung US-Export-Kontrollrecht

- Können durch Cloudanbieter nun tatsächlich durchgesetzt werden.
- Sind nicht immer deckungsgleich mit den europäischen Außenwirtschaftsrecht.
- Eine Abhängigkeit könnte in Extremfällen die gesetzliche Aufgabenerfüllung verhindern.
- Einbeziehen in AGB ggf. unwirksam.

Digitale Souveränität = Art. 33 Abs. 4 GG

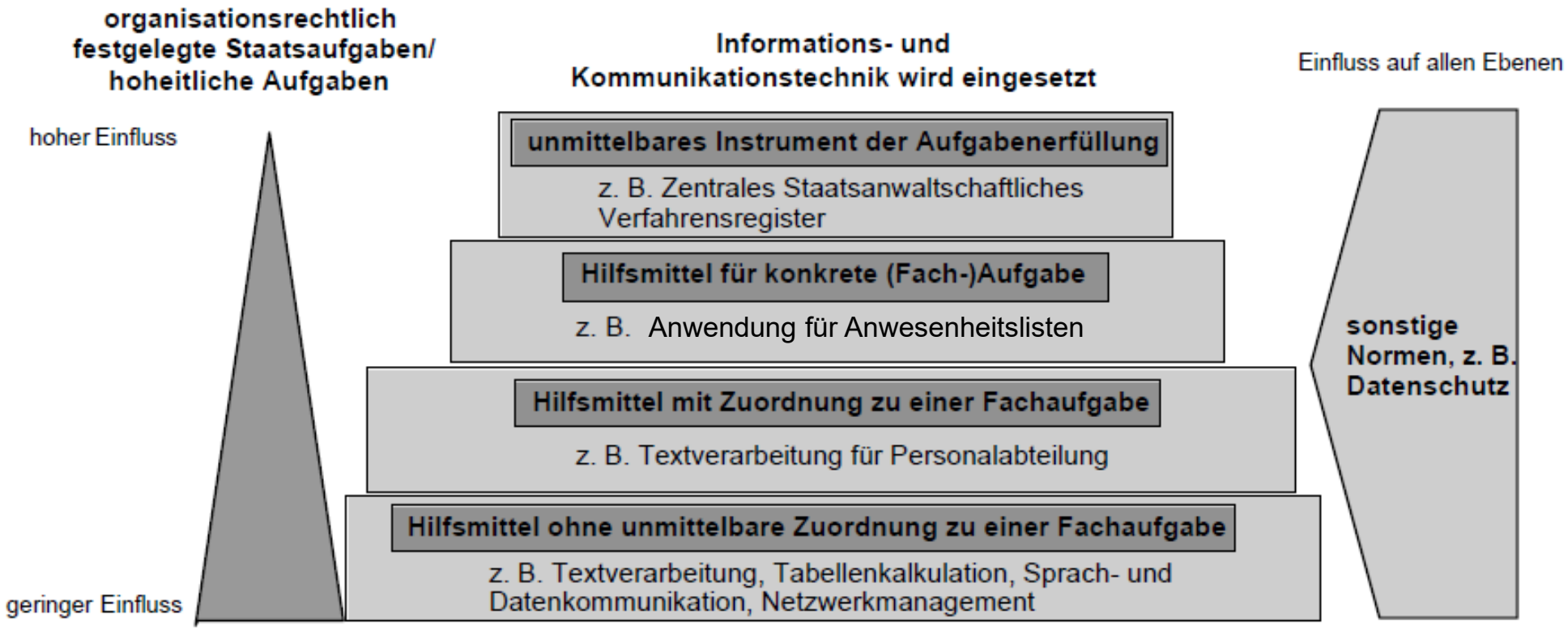


Abbildung 1: Einfluss hoheitlicher Aufgaben und sonstiger Normen auf das IuK-Outsourcing

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

Checkliste

- Gewährleistung der ordnungsgemäßen Aktenführung
- Barrierefreiheit
- Gute Nachhaltigkeitsansätze
- Keine Lücken in der Auftragsverarbeitung
- Vertraulichkeit der Kommunikation
- Verpflichtung auf Vertraulichkeit nach Bitkom-Muster + Auslandsklausel
- Ggf. Verpflichtung nach Verpflichtungsgesetz bei Zugriff auf Personaldaten
- Zusätzliche Maßnahmen bei besonders geschützten Gütern (z.B. Verschlüsselung außerhalb der Kontrolle des Anbieters)
- Export von Sozialdaten nur in den EWR bzw. soweit Angemessenheitsbeschlüsse vorliegen
- Nicht ohne Plan, Kontrolle und umsetzbares Exit-Szenario in die Public Cloud
- Keine Abhängigkeit durch vom Anbieter durchsetzbaren US-Export-Kontrollen

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 – The law and the Public Cloud for the Public Sector