Clouddienste rechtssicher beschaffen

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Ihr Referent

Haupttätigkeit:

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Sitz am Rechenzentrum der Universität Würzburg

Datenschutzbeauftragter für die virtuelle Hochschule Bayern

Datenschutzbeauftragter der Technischen Universität Nürnberg

Hintergrund:

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

Themen

- Für was und was sind Preis und Gegenleistung?
- Was sollte die Vertragsgrundlage sein?
- Datenschutz, aber was denn?
- Digitale Souveränität, muss das sein?
- Welche Pflichten sollte ich meinen Nutzern geben?
- Kann ich bei der Risikoklassifikation mir das Leben etwas vereinfachen?

Wann gilt der rechtliche Rahmen?

- Jeder Dienst
- Jedes Addin
- Jede Erweiterung
- Jede (optional) verbundene Erfahrung
- Für jede Einstellung …

Leider auch für mich …

Rechtsrahmen

- Behindertengleichstellungsgesetze
- Datenschutzrecht
- Digitalgesetze
- Haushaltsrecht
- Informationssicherheitsrecht
- Patentrecht?
- Personalrecht und Mitbestimmung
- Sicherheitsforschung?
- Steuerrecht?
- Telemedien- und Telekommunikationsrecht
- Urheberrecht
- Vergaberecht

…

Wie bezahle ich die Dienste?

Wir verwenden Ihre Daten nicht für Werbezwecke …

“When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section.“

Beispiel aus den Microsoftverträgen

Customer authorizes Microsoft:

(i) to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and

(ii) to calculate statistics related to Customer Data or Professional Services Data

in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer.

Those purposes are:

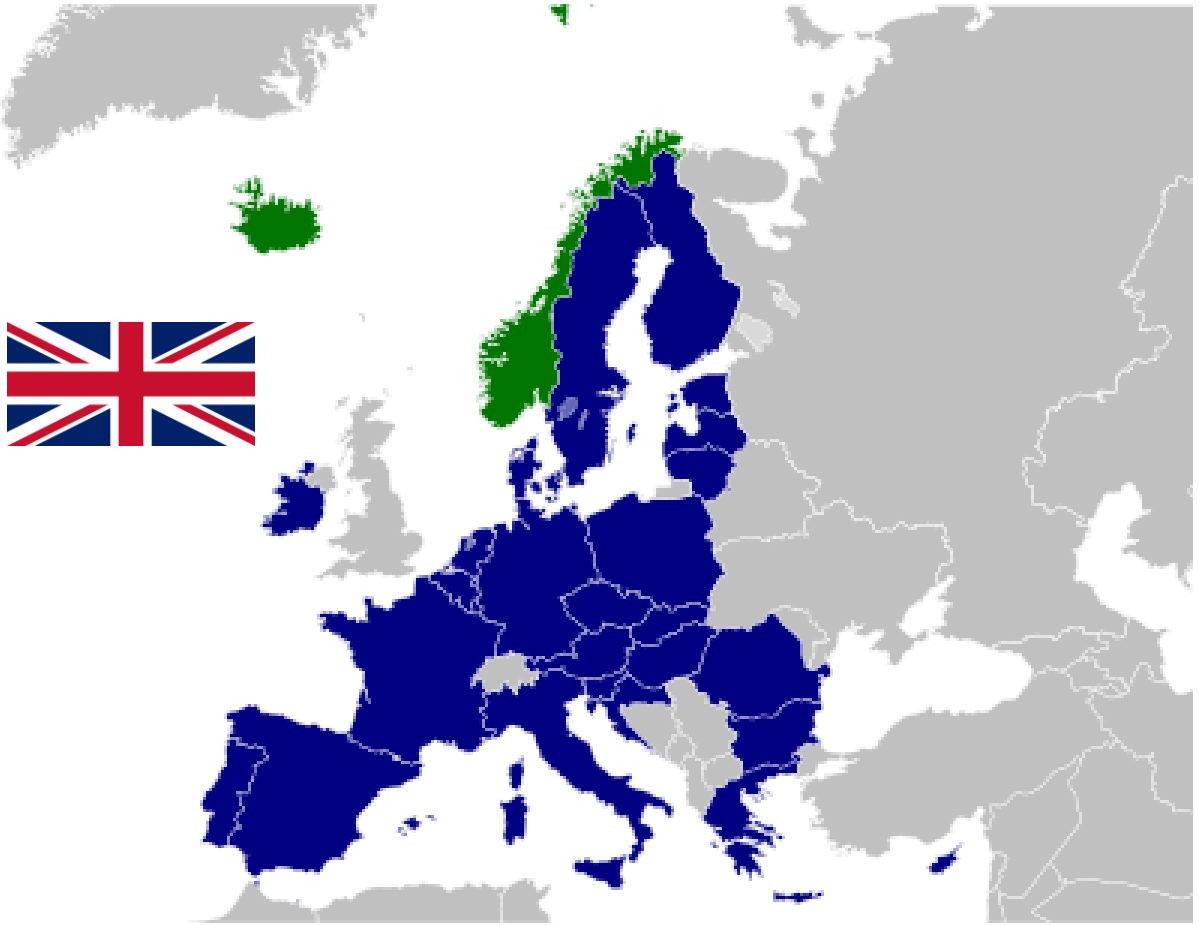
- billing and account management;
- compensation such as calculating employee commissions and partner incentives;
- internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
- financial reporting.

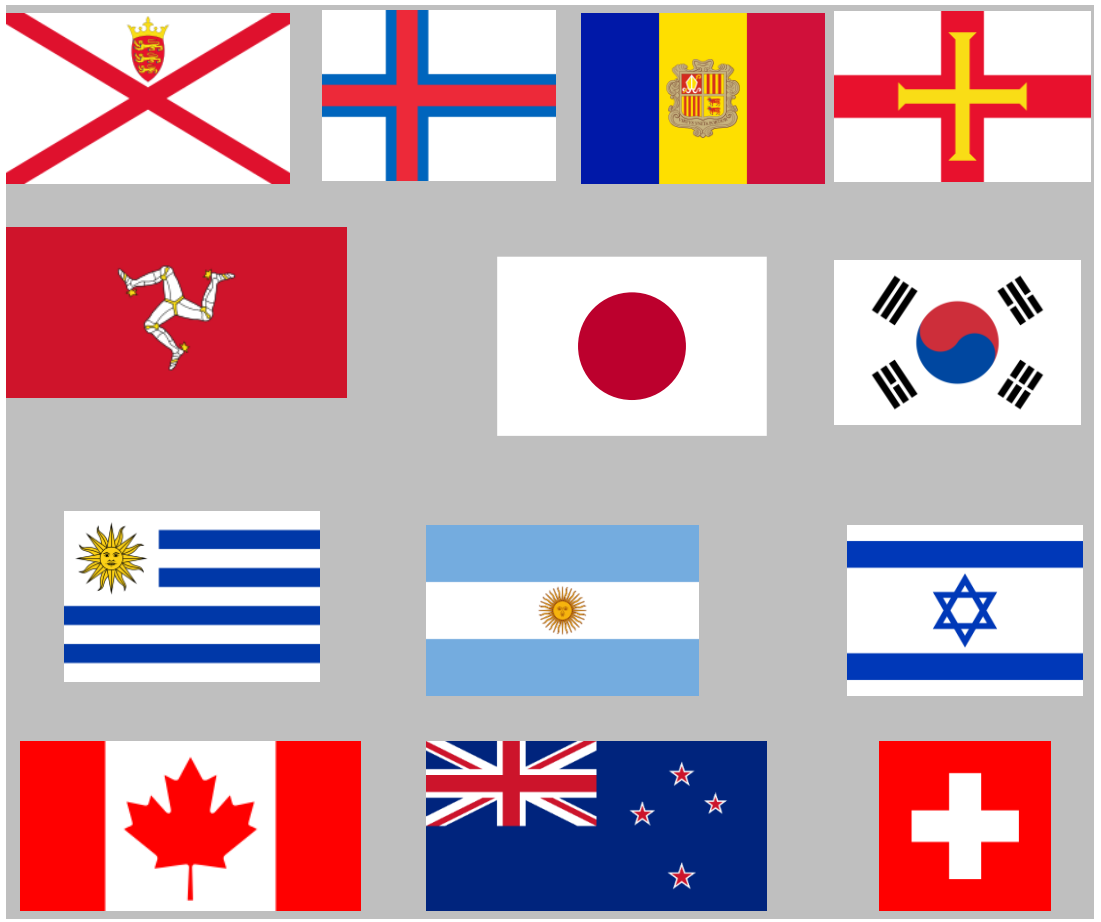
Beschaffungsrahmen

- EVB-IT Cloudvertrag
  - Einarbeitung wegen Komplexität erforderlich
  - Schnelle Nutzung über die Anlagen
    - EVB-IT Cloud Anlage auftragnehmerseitige AGB
    - EVB-IT Cloud Kriterienkatalog für Cloudleistungen
- Integration und Umgang mit Updates sowie Produktänderungen
  - Empfehlung analog zu Verbraucherverträgen ausgestalten
- Greift jedoch nicht bei Beschaffungen auf Grundlage von Konditionenverträgen, etwa bei Adobe oder Microsoft …

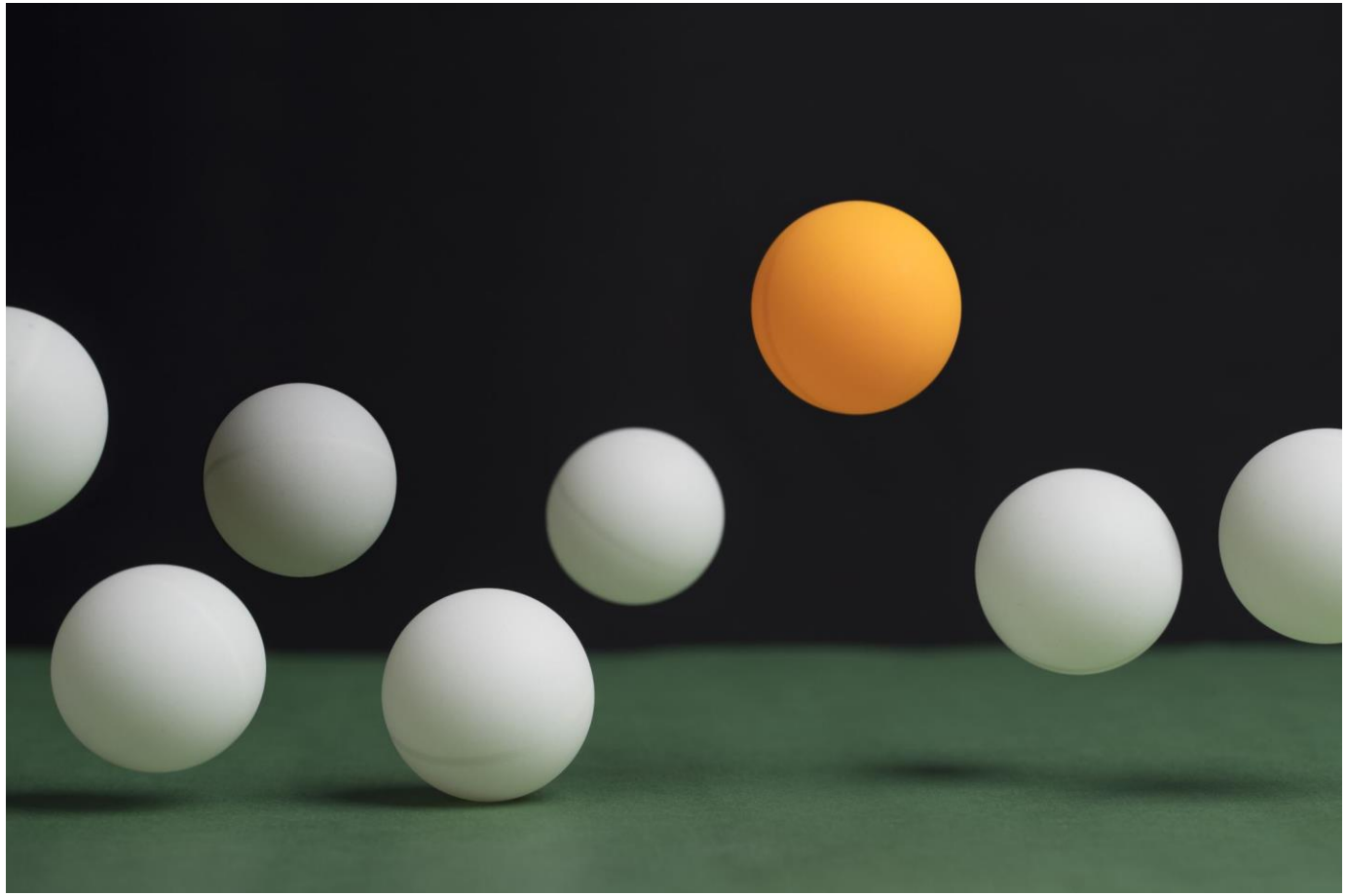
Europäischer Datenschutz

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en





Internationaler Datentransfer



Internationaler Datentransfer - II

- In Länder ohne angemessenes Datenschutzniveau nur noch möglich, wenn
  - Seltene Ausnahmen greifen
  - Standardvertragsklauseln genutzt werden
  - Aufwendige zusätzliche Maßnahmen getroffenen werden
    - Technischer Natur (Verschlüsselung, ggf. Pseudonymisierung)
    - Teilweise auch vertragliche (z.B. Transparenzpflichten, Rechtswegpflicht, Vertragsstrafen) oder organisatorische Fragen
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

  Use Case 6: mit unverschlüsselten Daten und ohne Rechtsschutz gegen Behörden im Drittstatt für Betroffene nicht möglich

  ➔“then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights”
- Oft Entscheidung der Leitung für Dienste mit internationalem Datentransfer mit Risikoübernahme gegen Rat des Datenschutzteams ohne ausreichende Garantien

Checkliste Dokumente für den Datenschutz

- Wo stehen die Server (mehr eine politische Frage)?
- Von wo wird welches Supportlevel erbracht?
- Gibt es eine Verarbeitung von aggregierten Daten? Wer darf diese Daten sehen?
- Gibt es Drittbetroffene bei der Datenverarbeitung?
  - Dann Auftragsverarbeitung (übliche Abkürzungen AVV, DPA, veraltet ADV)
  - Optimal-Fall: Muster der eigenen Hochschule durchsetzen; sonst Prüfung der angebotenen Auftragsverarbeitung des Anbieters
  - Bei Forschungsvorhaben mit einer geringen Anzahl an betroffenen kann die Auftragsverarbeitung auch durch erweiterte Einwilligungen ersetzt werden
- Weitere Dokumente neben der Auftragsverarbeitung
  - Liste der Unterauftragsverarbeiter
  - Analyse der Datenschutzschutzsituation in den Empfängerländern ((D) TIA = (Data)Transfer Impact Assessment)
  - Auditberichte und Zertifikate (z.B. SOC II)
  - Unterstützungsdokumente zur Datenschutzfolgenabschätzung

Checkliste als Erweiterung für die Vertraulichkeit

- Fallen die zu verarbeitenden Informationen unter den Schutz von § 203 StGB?
  - Wichtig der Schutz ist weiter als der für personenbezogene Daten!
  - Schutz gilt auch wenn Betroffene versterben!
  - Optimal Nutzer der Bitkom einsetzen.
  - Wegen der potentiellen Strafbarkeit unbedingt mit Rechtsamt abstimmen.
- Werden Personalakten abgelegt?
  - Regelmäßig besondere Vertraulichkeitsregeln erforderlich, teilweise bis zu einer Verpflichtung nach dem Verpflichtungsgesetz!
- Werden steuerrechtlich relevante Unterlagen abgelegt?
  - Speicherung dann grundsätzlich nur im Europäischen Wirtschaftsraum

Digitale Souveränität = Art. 33 Abs. 4 GG

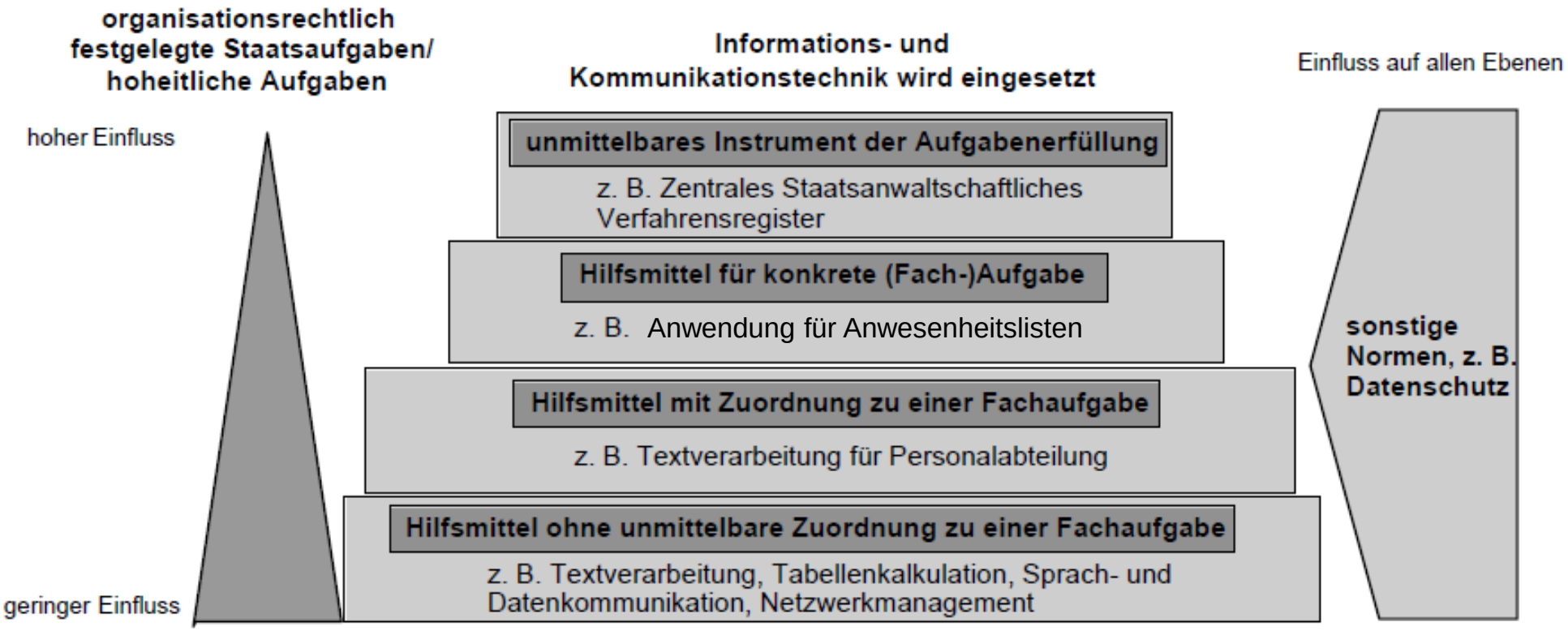


Abbildung 1: Einfluss hoheitlicher Aufgaben und sonstiger Normen auf das IuK-Outsourcing

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

Digitalgesetze Bayern I

Art. 3 Digitale Entscheidungsfähigkeit des Freistaates Bayern

(1) Die eigenständige digitale Entscheidungs- und Handlungsfähigkeit des Freistaates Bayern ist durch geeignete Maßnahmen zu sichern. Der Freistaat Bayern unterhält hierfür staatliche Rechenzentren und staatlich verfügbare Netze, geeignete Cloud-Dienste und weitere geeignete Technologien und Anwendungen. Der Freistaat Bayern wirkt mit dem Bund und anderen Ländern im Bereich der Digitalisierung in geeigneter Weise zusammen.

(2) Der Freistaat Bayern schützt die Funktionsfähigkeit und den Zugang zu kritischen staatlichen Infrastrukturen und Netzen.

(3) Der Freistaat Bayern, die Gemeindeverbände und Gemeinden treffen nach Maßgabe dieses Gesetzes angemessene Maßnahmen zur Abwehr von Gefahren für die Sicherheit ihrer informationstechnischen Systeme.

Digitalgesetze Bayern II

(4) Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen offene Software verwenden und offene Austauschstandards nutzen, soweit dies wirtschaftlich und zweckmäßig ist. **Den Gemeindeverbänden und Gemeinden sowie den sonstigen Körperschaften des öffentlichen Rechts wird die Verwendung offener Software im Sinne des Satzes 1 empfohlen.**

(5) Die Behörden des Freistaates Bayern sollen bei Neuanschaffungen von Software die Gebrauchstauglichkeit, das Benutzererlebnis und die Benutzerfreundlichkeit berücksichtigen sowie Nutzersicht und Wirtschaftlichkeit gleichrangig behandeln.

Bremen

Gesetz zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen

§ 1 Sicherheit und digitale Souveränität, Verlässlichkeit der Versorgung

…

Die Einbeziehung von Unternehmen, welche den Voraussetzungen des Absatzes 1 nicht genügen (sonstige Unternehmen), zur Erfüllung eines Vertrages durch die juristische Person des öffentlichen Rechts als Auftragnehmerin soll nur erfolgen, wenn andernfalls unverhältnismäßige Nachteile zu befürchten sind. Unverhältnismäßige Nachteile liegen insbesondere vor, wenn Leistungen für die Deckung des IT Bedarfs notwendig sind, die nur von sonstigen Unternehmen hergestellt oder angeboten werden oder wenn der Einsatz von Lösungen der öffentlichen Rechts juristischen Person des qualitativ oder quantitativ deutlich schlechtere Ergebnisse als eine Lösung eines privaten Anbieters begründet erwarten lässt.

Vorschlag für Nutzungsregeln

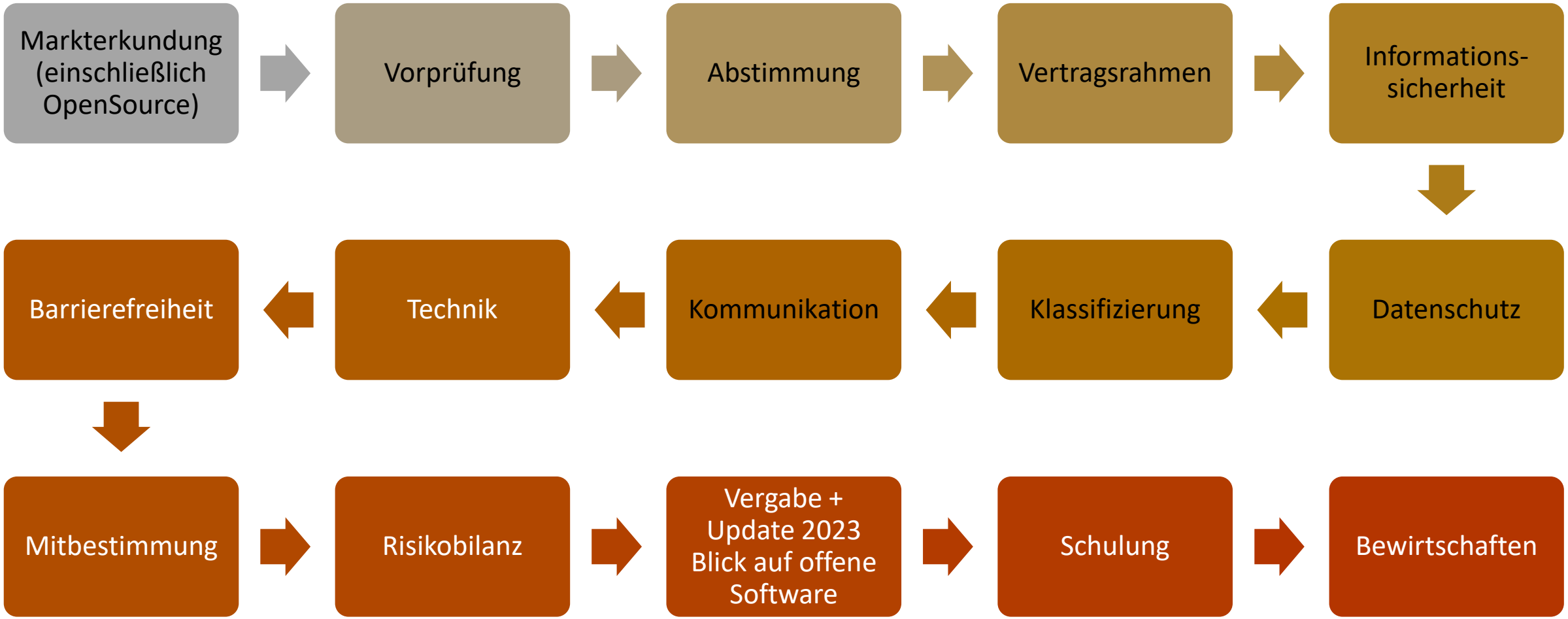
Allgemein gilt: Unveröffentlichte personenbezogene Daten von Personen, die diesen Dienst nicht nutzen (Fall 1), dürften ebenso wenig wie Daten, die besonderer Geheimhaltung oder besonderem Schutz (Fall 2) unterliegen, unverschlüsselt in das Speicherangebot des Dienstes übergeben werden.

- Beispiele für Fall 1 sind etwa Anwesenheitslisten oder Listen von Teilnehmenden einer Veranstaltung aber auch transkribierte Interviews; Beispiele für Fall 2 sind etwa Krankmeldungen und Forschungsverträge mit Geheimhaltung.
- Soweit eine Zulässige Verarbeitung personenbezogener Daten Dritter erfolgt, müssen Sie die Vorschriften des Datenschutzes einhalten und die Erfüllung der Informationspflichten sicherstellen.

Vorschlag für eine Basisrisikoklassifikation

Risikowert	Besonders geringes Risiko	Geringes Risiko	Normales Risiko	Substanzielles Risiko	Hohes Risiko
Diensteart	Dienste die Inhalte über eine Netzwerkverbindung nur nach Interaktion der Nutzerinnen und Nutzer zum Download bereitstellen	Dienste, die über eine Netzwerkverbindung Inhalte auch ohne Interaktion der Nutzerinnen und Nutzer bereitstellen	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer nur temporär verarbeiten	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer abspeichern aber nicht in sonstiger Form verarbeiten	Dienste, die über eine Netzwerkverbindung die hochgeladenen Inhalte der Nutzerinnen und Nutzer verarbeiten und nicht nur abspeichern
Daten-schutz	Nur einzelne Betroffene	Nur einzelne Betroffene jedoch weniger Kontrolle	Drittbetroffene denkbar, jedoch Verarbeitung nicht intensiv	Drittbetroffene denkbar, gewöhnlicher Grad an Verarbeitungsintensität	Regelmäßig Drittbetroffene und Intensive Datenverarbeitung
Infor-mations-sicherheit	Kein Unterschied zum bedachten Surfen im Internet	Gefahrdung der Integrität denkbar	Wohl kein dauerhafter Abfluss von Informationen	Abfluss von Informationen nicht ausschließbar, aber einfache Schutzmöglichkeiten vorhanden	Abfluss von Informationen nicht ausschließbar, jedoch teilweise bessere Verfügbarkeit als intern möglich.
Beispiel	Microsoft eigene Onlinebilder in Office einfügen	Updates für Microsoft Office	Übersetzer in Microsoft Office	Microsoft OneDrive	Automatisierung von Workflows mit PowerAutomate

Ein Weg zur Lösungsimplementierung



Vorbereitung

- Markterkundung und Vorprüfung
  - ✓Austausch in der Hochschulgemeinschaft
  - ✓Input aus den Arbeitskreisen (z.B.: Datenschutz, Informationssicherheit, …)
- Abstimmung
  - ✓Gemeinsam statt einsam
- Vertragsrahmen
  - ✓Gleiche Konditionen für alle
  - ✓Unterschriftsarme Verträge
  - ✓Berücksichtigen der Hochschulbesonderheiten
- Kommunikation

Prüfen und Einstellen

- Kommunikation
- Informationssicherheit
  - Prüfung der Informationssichersicherheitszertifizierungen
  - Austausch von „Best Practices“
- Datenschutz
  - Auftragsverarbeitung, Musterdokumentation, Musterinformation, Mustertexte für Einwilligungen
- Klassifizierung
  - Welcher Dienst für was?
  - Nutzungsbedingungen
  - Geheimhaltungsvereinbarung erforderlich?
- Technik
  - Provisionierung, Branding, …
- Barrierefreiheit
  - WCAG 2.1 Level AA und mehr …

Interne Prozesse und Vergabe

- Einbindung
  - Datenschutzbeauftragte
  - Informationssicherheitsbeauftragte
  - Personalrat
  - Sonstige Interessensvertreter
- Entscheidung
  - Gesetzlicher Rahmen
  - Risikobereitschaft
- Vergabe
  - Gemeinsam beschaffen oder Musterdokumentationen teilen

Vielen Dank für Ihre Aufmerksamkeit!

Johannes Nehlsen

Tel.: 0931/31-84217

johannes.nehlsen@uni-wuerzburg.de

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

Twitter privat: @JoNehlsen

Nehlsen – Cloudlösungen rechtssicher beschaffen