Rechtsvertrauen in die Public Cloud

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Datenschutzbeauftragter für die Virtuelle Hochschule Bayern

Über mich

- Volljurist
  - Referendariat OLG München
  - Wahlstation bei Eversheds UK
- Rechtsinformatikzertifikat an der Ludwig-Maximilians-Universität
- Zertifizierung als Informationssicherheits-beauftragter, OTH Regensburg
- Microsoft Licensing Professional
- Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
  - Datenschutz
  - E-Government
  - E-Procurement
  - IT-(Sicherheits-)recht
  - Urheberrecht
- Datenschutzbeauftragter für die Virtuellen Hochschule Bayern

Agenda

- Rückblick
- Was ist neu?
- Spickzettel Public Cloud
- Umgang mit Risiken
- Datenschutzfolgeabschätzung
- Auftragsverarbeitung
- Informationssicherheit
- Fazit

Aus dem Kontakt zu Anbietern

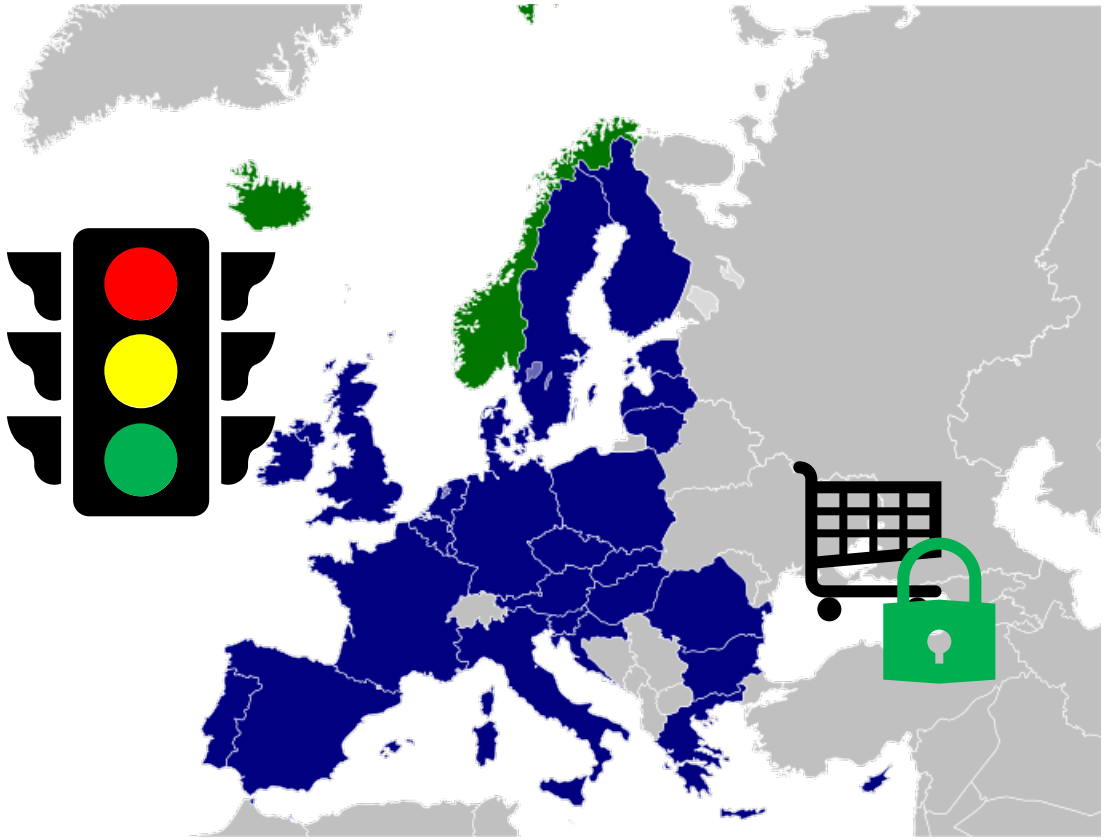
Könnten Sie mir Ihre Auftragsverarbeitung zur Einsicht bereitstellen?

1. Hier finden Sie unsere **Datenschutzerklärung**.
2. Dafür ist der Abschluss einer Vertraulichkeitsvereinbarung erforderlich.
3. Der Abschluss einer individuellen Auftragsverarbeitung ist gegen Aufpreis möglich.

Könnte ich den Auditreport XYZ einsehen?

1. Dazu müssen Sie erst Kunde bei uns sein.
2. Hier können Sie das **Zertifikat** XYZ abrufen.

Datenschutz und Datenfluss



Datenschutz und Datenfluss II

Datenschutz-Grundverordnung

- Regelt für Unternehmen und Behörden (ohne Polizei und Justiz) den Umgang mit Daten
- Fördert den Datenhandel und den Fluss von Daten im Europäischen Wirtschaftsraum
- Setzt als Prinzipen
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - Rechenschaftspflicht

Freier Verkehr nicht-personenbezogener Daten in der Europäischen Union

- Verbot bzw. Einschränkungen von Datenlokalisierungsauflagen
- Welcher Anwendungsbereich bleibt durch den weiten Begriff der personenbezogener Daten?
- Kein Wort in der Verordnung zum Urheberrecht, dass zu einer Datenlokalisierung zwingen kann
- Verordnung könnte zu einem „Joker“ werden, um Freiräume zu schaffen

Zum Einstieg

„Ich wiederhole daher meine schon bislang ausgesprochene Empfehlung an bayerische öffentliche Stellen, auf die Nutzung von Public-Cloud-Diensten mit (auch nur eventuellen) Datenverarbeitungen in den USA zu verzichten und nach anderen, nationalen oder auch europäischen Lösungen zu suchen.“

Quelle: 28. Tätigkeitsbericht der bayerischen Landesdatenschutzbeauftragten

Lokal oder Cloud?

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

„Setzt der Website-Betreiber hierfür ein Analyse-Tool ein, welches Daten über das Nutzungsverhalten betroffener Personen an **Dritte** weitergibt (z.B. soziale Netzwerke oder externe Analysedienste, die Nutzungsdaten über die Grenze der Website hinweg mit Daten von anderen Websites zusammenführen), ist dies nicht mehr erforderlich. Das Ziel – Reichweitenmessung – kann auch mit milderen, gleich geeigneten Mitteln erreicht werden, die deutlich weniger personenbezogene Daten erheben und diese nicht an Dritte übermitteln (z. B. ohne Einbindung Dritter **über eine lokale Implementierung einer Analysesoftware**).“

Orientierungshilfe der Aufsichtsbehörden

für Anbieter von Telemedien

Quelle: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (Hervorhebung durch Johannes Nehlsen)

Neu seit März 2017

Reform des § 203 StGB

- Umfasst insbesondere auch die Geheimhaltungspflicht aus § 203 Abs. 2 StGB
- Nun ist das Admin-Ehrenwort strafrechtlich verbindlich
- Verpflichtung zur Geheimhaltung muss jedoch vorausgehen

Geheimnisschutzgesetz

- Geheimnisse rechtlich nur geschützt, wenn Sicherheitsmaßnahmen zur Geheimhaltung ergriffen worden sind.

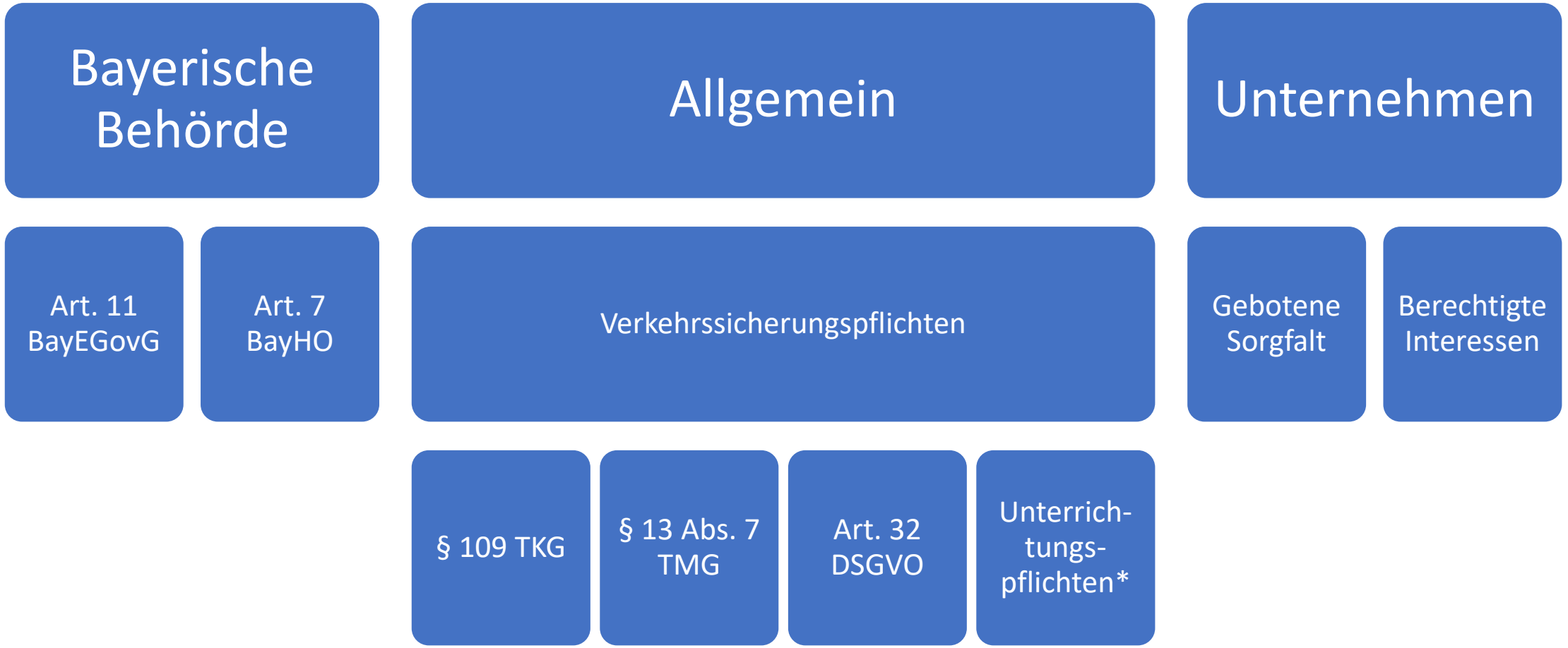
Spickzettel für die Public Cloud

- Bezahlung erfolgt mit Geld und Nutzungsanalyse (Leitungsentscheidung)
- Datenschutzinformation an alle Nutzenden
- Datenschutzfolgeabschätzung
- Beteiligung des Personalrates
- Lokales Backup der Daten (einschließlich Konfiguration)
- Sicherheitskonzept (Intern + Anbieter)
- Anlage 6.5 Arbeitsstättenverordnung

Für „öffentliche Stellen außerdem“

- Beachtung der Leitsätze der Rechnungshöfe zum IuK-Outsourcing
- Wirtschaftlichkeitsuntersuchung

Risikovorsorge im IT-Alltag

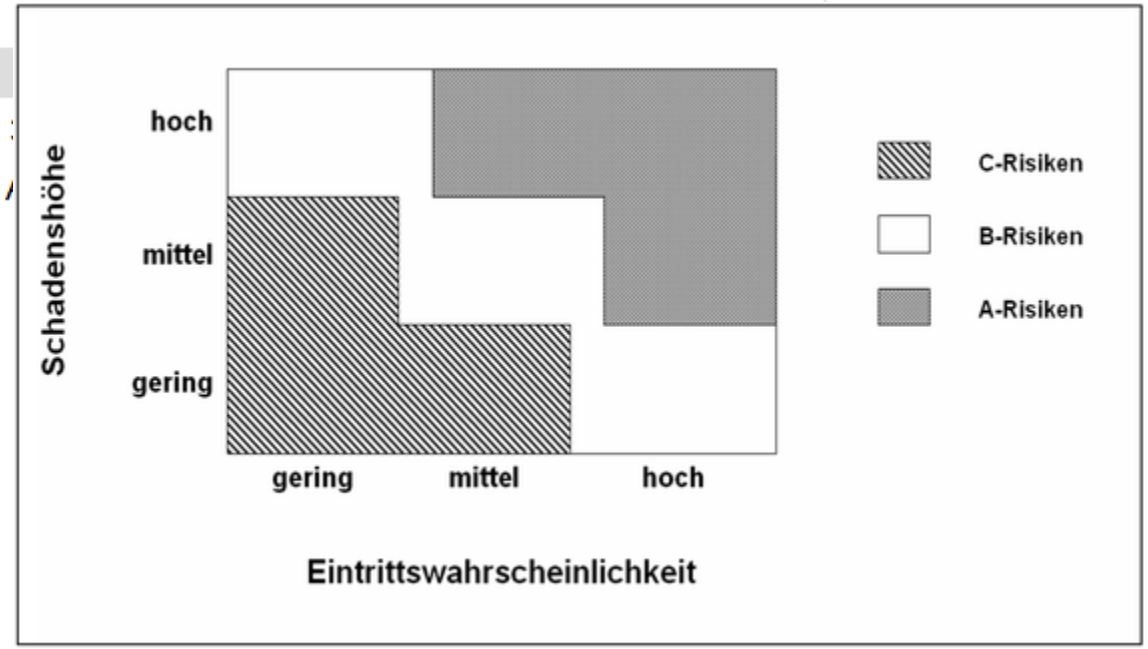


Woher ist das bekannt?

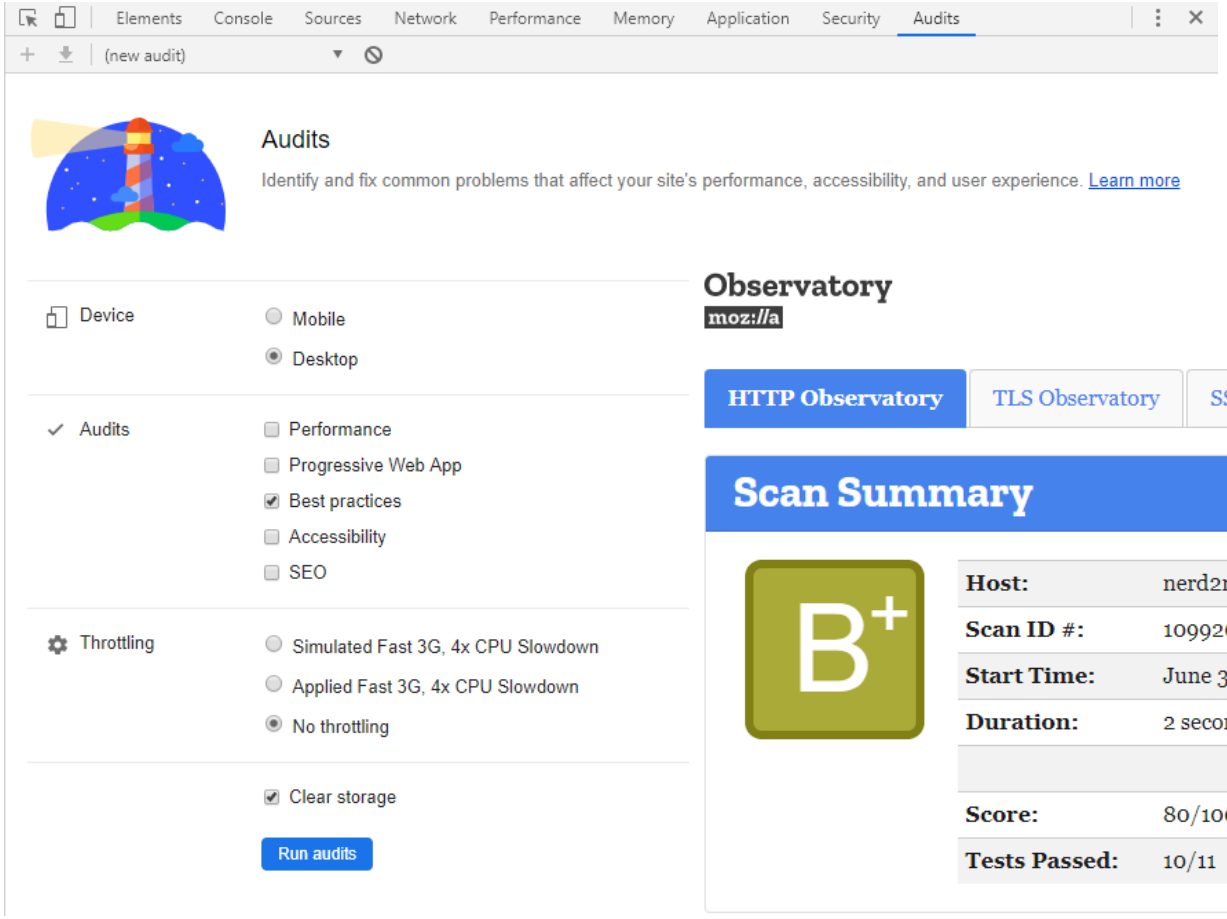
Inhaltsverzeichnis

- **630-F Verwaltungsvorschriften zur Bayerischen Haushaltsordnung (VV-BayHO) Bekanntmachung de…**
  - Inhaltsübersicht (amtlich)
  - + A. Verwaltungsvorschriften zur Bayerischen Haushaltsordnung (VV-BayHO)
  - − B. Anlagen zu den VV-BayHO
    - Anlage zu den VV zu Art. 7 BayHO
    - Anlage zu den VV zu Art. 34 BayHO (VV Nr. 4 zu Art.
    - Anlage 1 zu Art. 44 BayHO (ANBest-I) (VV Nr. 5.1 zu A

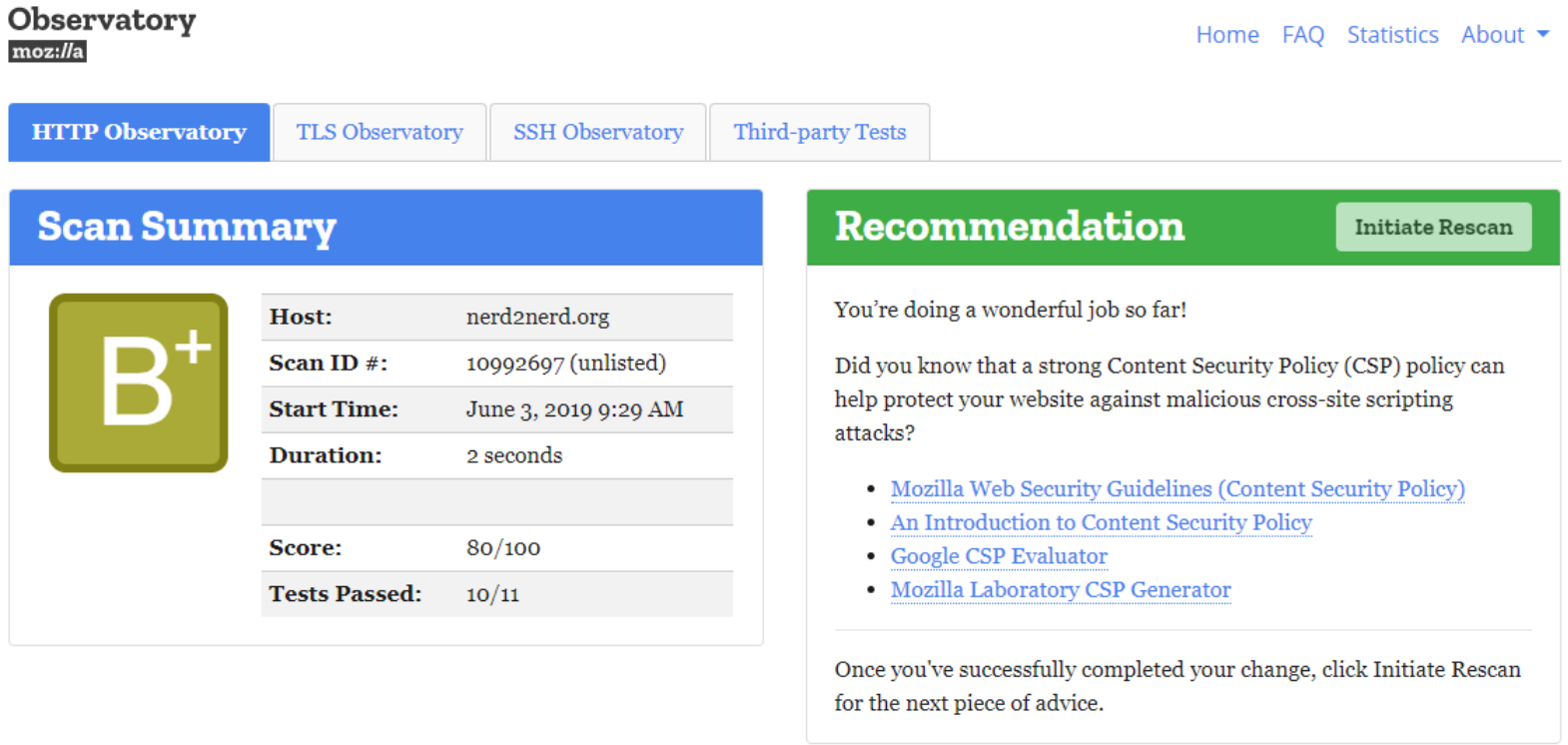
[Wirtschaftlichkeitsuntersuchung]



Live-Demo – Wie stets um die Loginseite



https://web.dev/
https://observatory.mozilla.org/

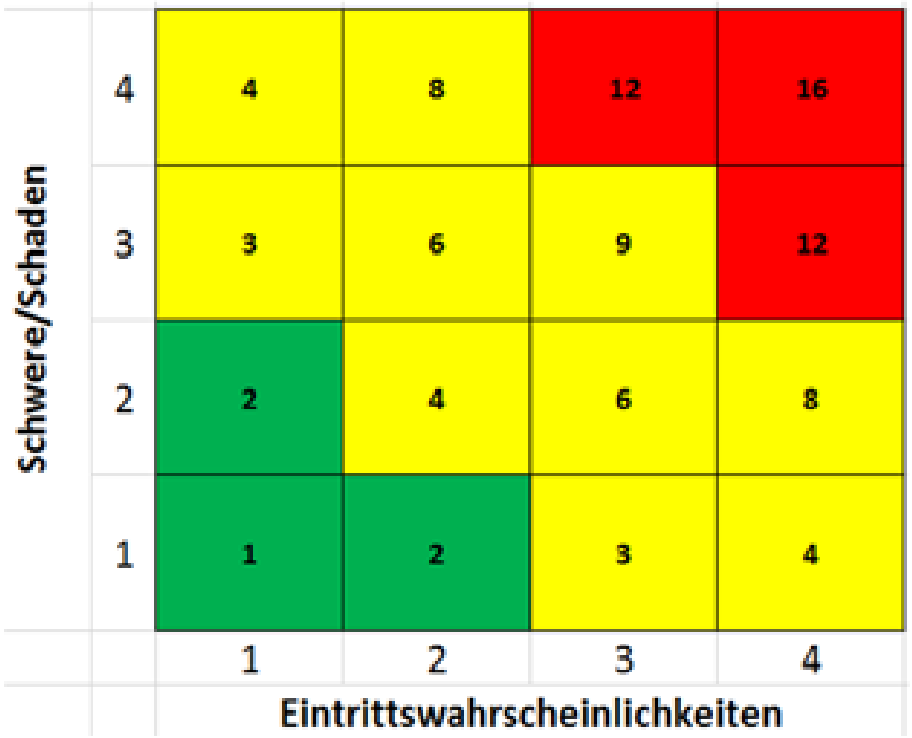


Risikoklassifikation

ICO Template unter Open Government Licence v3.0

Severity of impact				
	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Übliche 4x4 Risikomatrix



Judgments of Likelihood

Alltagssprache	Fachausdruck	Eintrittswahrscheinlichkeit in Prozent
Almost no chance	„remote“ (fern liegend)	0 bis < 20 %
Very unlikely	„Highly improbable“ (höchst unwahrscheinlich)	ab 20 bis < 30 %
Unlikely	„Improbable“ (unwahrscheinlich)	ab 30 bis < 40 %
Roughly even chance	„Roughly even odds“ (um den Mittelwert 50 % herum)	ab 40 bis < 60 %
Likely	„Probable“ (Wahrscheinlich, vermutlich, voraussichtlich)	ab 60 bis < 80 %
Very likely	„Highly probable“ (sehr wahrscheinlich)	ab 80 bis < 90 %
Almost certainly	„Nearly certain“ (fast, beinahe sicher)	ab 90 bis < 100 %

Quelle: Office of The Director of National Intelligence – National Intelligence Council: Background to „Assessing Russian Activities and Intentions in Recent US Elections“: The Analytic Process and Cyber Incident Attribution, 6 January 2017, p. 13. Übertragung ins Deutsche: A. Rösler.

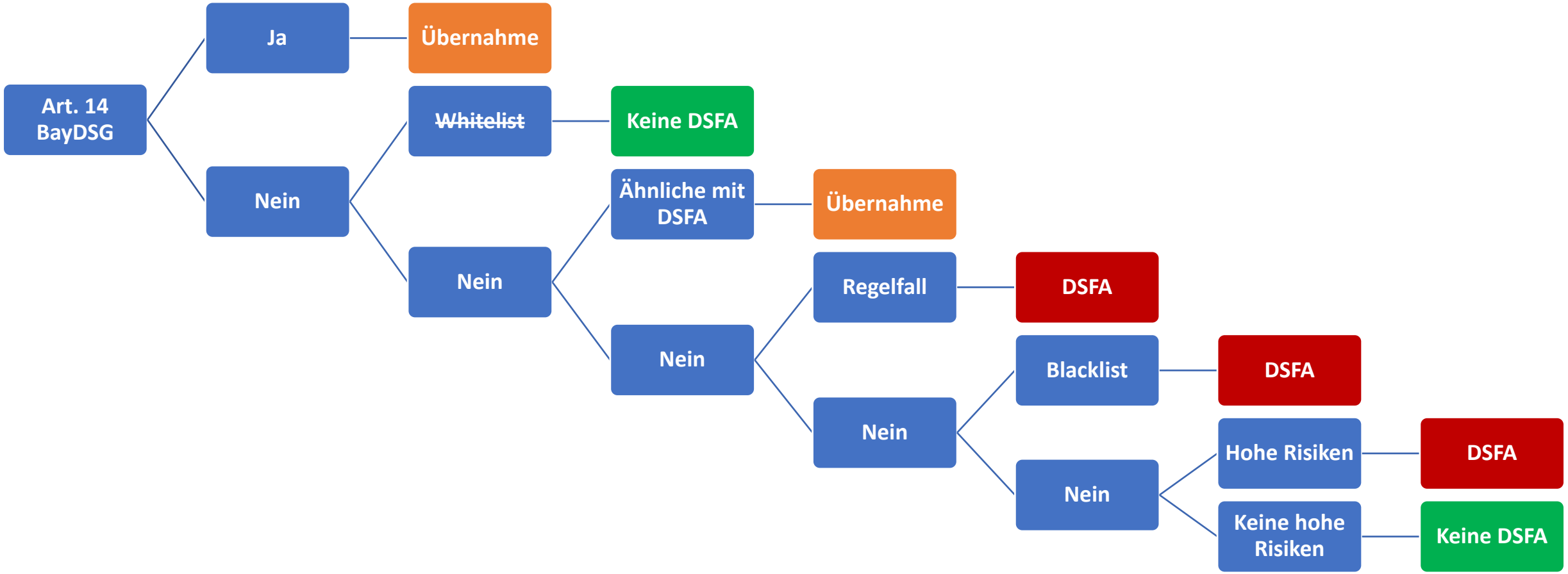
Und der Aufwand für die Umsetzung der DSGVO?

- Informationen an Betroffene
- Umsetzung von Betroffenenrechten
- Dokumentation
- Datenschutzfreundliches Design
- Datenschutzfreundliche Voreinstellungen
- Datensicherheit
- Bewältigung von Datenschutzverletzungen
- Datenschutzfolgeabschätzung … „Bayerische Blacklist (Behörden)“

Klassifizierung von Daten durch die DSGVO

Kategorie	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
Identifizierbare personenbezogene Daten	Art. 1 Abs. 1 Alt. 1 DSGVO	Ja
Personenbezogene Daten unter Berufsgeheimnis	Erwägungsgrund 85 DSGVO	Gesteigert
Personenbezogene Daten 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

Datenschutzfolgenabschätzung – Vorprüfung (BY)



In Worten für die Dokumentation

Es liegt weder eine zu übernehmende Datenschutzfolgeabschätzung vor, noch eine Anwendung einer „White-List“.

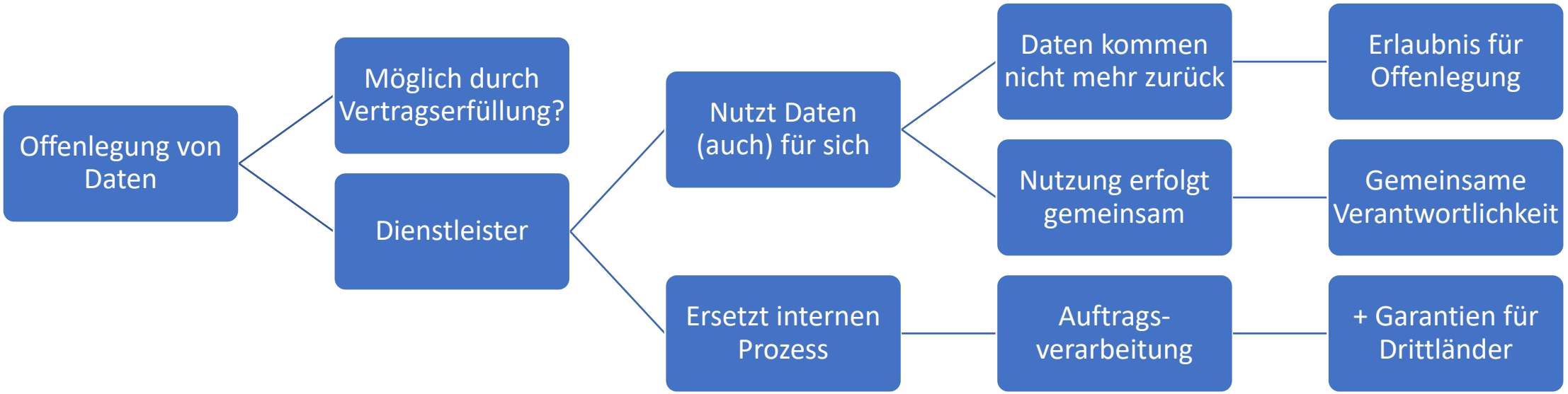
Die konkrete Verarbeitungstätigkeit weist auch keine Ähnlichkeit zur solchen auf, für die bereits eine Datenschutzfolgeabschätzung durchgeführt worden ist.

Ein Regelfall gemäß Art. 35 Abs. 3 DSGVO liegt nicht vor. Die konkrete Verarbeitungstätigkeit ist auch nicht in der „Black-List“ der Aufsicht genannt.

Bei der Verarbeitungstätigkeit kommen weder neue Technologien zum Einsatz, noch bestehen aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung im rechtlichen Sinne voraussichtlich hohe Risiken für Rechte und Freiheiten natürlicher Personen.

Verbliebenen Risiken wird durch technische und organisatorische Maßnahmen angemessen Rechnung getragen.

Nur Auftragsverarbeitung?



Reichweite von Auftragsverarbeitungen

AWS:

“Customer Data” means the “personal data” (as defined in the GDPR) that is uploaded to the Services under Customer’s AWS accounts
https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Microsoft:

“Customer Data” means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Support Data.
http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=English

Google:

“Customer Data” means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.
https://gsuite.google.com/terms/dpa_terms.html

Drittländer mit angemessen „Datenschutz“

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Orientierungshilfe Auftragsverarbeitung (BY)

https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf

Prüffrage	Ergebnis	Hinweis
Hat der Auftragsverarbeiter zugesagt, die Weisungen des Verantwortlichen zu dokumentieren?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2
Dürfen die im Rahmen der Auftragsverarbeitung verarbeiteten Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Leistung verwendet werden (Gebot der Zweckbindung)?	Erfüllt	Klausel 5a
Wurden dem Auftragsverarbeiter Bekanntgabe, Verkauf, Vermietung oder anderweitige Verwendung der Daten durch Dritte bzw. die kommerzielle Verwendung verboten?	Umsetzbar/Teilweise erfüllt	Klausel 5a
Ist gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2
Wurden diese Personen auf das Datengeheimnis verpflichtet bzw. hingewiesen?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2
Hat sich der Verantwortliche davon durch eine Einsicht in die Verpflichtungs-/ Hinweiserklärungen überzeugt?	Prüfaufgabe	
Wurden die Mitarbeiter des Auftragsverarbeiters bezüglich der Einhaltung des Datenschutzes und der Datensicherheit informiert und geschult?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2
Werden im Rahmen der Auftragsverarbeitung ausschließlich fachlich geeignete Mitarbeiter eingesetzt?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2
Wurde beim Auftragsverarbeiter ein betrieblicher/behördlicher Datenschutzbeauftragter bestellt?	Prüfaufgabe	
Sind dessen Kontaktdaten bekannt?	Prüfaufgabe	
Wurden sowohl von Seiten des Verantwortlichen als auch des Auftragsverarbeiters verantwortliche Ansprechpartner zur Klärung eventuell auftretender fachlicher, technischer und organisatorischer Fragen benannt?	Prüfaufgabe	
Ist die Sicherheit der Datenverarbeitung angemessen gewährleistet (vgl. Art. 32 DSGVO), insbesondere mit Blick auf Pseudonymisierung und Verschlüsselung?	Umsetzbar/Teilweise erfüllt	Umsetzbar in Anlage 2

Datenschutz - Lösungsansätze

- Mehr-Augenprinzip beim Prüfen der Auftragsverarbeitung
- Konsistente Dokumentenstruktur (Verzicht auf Linkketten)
- Keine Dauerhafte Lösung zur Löschung: Vernichtung von „Schlüsseln“
- Verhindern von Schlupflöchern etwa bei der Definition von Kundendaten
- Vermeiden von Diensten mit mangelhaften Datenschutzdesign
  - Option Telemetrie / Analytics zu deaktivieren
  - Einstiegsseiten ohne Tracking
  - Freigabeerfordernis bei Supportfällen
- Keine Zusatzkosten bei Inspektionen (BY)

Vertragliche Absicherung der Datenflüsse - Informationssicherheit

Öffentliche Einrichtungen

BSI-Standards – BSI C5 Testat für Public Cloud

E-Government-Gesetze

Interne Vorgaben

Geheimnisse von Vertrauenspersonen

Amts-/Dienstgeheimnisse

Ausstieg?

Nicht öffentliche Einrichtungen

Industriestandards (etwa ISO 270xx)

Risikovorsorgepflichten

Interne Vorgaben

Geheimnisse von Vertrauenspersonen

Geheimnisschutzgesetz

Ausstieg?

Was kommt?

- Mehr Vorgaben zur Barrierefreiheit (für SaaS)
- Over the Top Dienste unter ePrivacy / Fernmeldegeheimnis?
- Brexit?
- Privacy Shield fällt durch
- Standvertragsklauseln werden fallen
- Strengeres Außenwirtschaftsrecht?
- Gesetzliche Vorgaben zu Forschungsinformationssystemen und Forschungsdatenmanagement
- Und der Evergreen: Einhaltung von Lizenzvorgaben
  - Account-Sharing
  - Zugriff durch Dritte

Take away

- Guter Bezugsrahmen durch Ausschreibungen geschaffen
- Viel Umsetzungsarbeit verbleibt jedoch in den Einrichtungen

Um zum Vortrag:

- Viele Anbieter sind im Kleingedrucktem ehrlich
- Viele Daten können anders Bauwerke leicht kopiert werden. Halten Sie Ihre Daten, die in der Public Cloud liegen, nochmals selbst vor.
- Was für Daten gilt, gilt auch für das Wissen (Konfiguration und Administration)
- Nur selten wird „Default“ reichen
- Vollkostenrechnung wird für einige Anwendungen die Wirtschaftlichkeit der Public Cloud ermitteln können

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 - Rechtsvertrauen in die Public Cloud