25. Mai 2018 – da war doch was?

Die EU-Datenschutz-Grundverordnung tritt in Kraft. Was bedeutet das für die Beschaffung und Bereitstellung von Software?

Johannes Nehlsen

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen
c/o Rechenzentrum Universität Würzburg

Zutaten für erfolgreichen Cloudbeschaffung

- Nicht paranoide Informationssicherheitsbeauftragte
- Progressive Datenschutzbeauftragte
- Offenerer Personalrat
- Modern denkende Rechenzentrumsleitung
- Trendsetter im Team und bei den Administratoren (m/w/d)
- Ehrliche User

Jetzt können Sie in die Cloud!
Oder gibt es Produkte mit denen Sie in die Cloud müssen?

Kostenfreier Aufsatz: Rechtsfragen zu Cloud-Angeboten für Hochschulen

Telemetire

Der „Verarbeiter“ trägt die datenschutzrechtliche Verantwortung!

Aber: Tendenzen gehen Richtung Mitverantwortung des Software einsetzenden Verantwortlichen.

- Privacy by Design
  - ✓ Einsatz von Pseudonymen auf Nutzeroberfläche
  - ✓ Richtiger Einsatz von Verschlüsselung
  - ✓ Rollen und Rechtemanagement
- Privacy by Default
  - ✓ Sichtbarkeit in Portalen erst nach Nutzerinteraktion
  - ✓ Abschalten der Telemetire
  - ✓ Wenn unvermeidbar und Anwendung unverzichtbar
    - Datensparsame Einstellungen bei Telemetrie
    - Ausweichmöglichkeiten schaffen soweit möglich

Checkliste

- Personenbezogene Daten zur Einkaufsabwicklung
  - In welchen Land sitzt der Händler?
- Personengebundene Lizenz
  - In welchem Land sitzt der Anbieter
  - Sind die erhobenen Daten auch wirklich erforderlich (z.B. Geschlecht, E-Mail-Adresse, Vorname, Nachname)
- Cloudservices
  - In welchen Land ist der Anbieter
  - In welchem Land wird gespeichert
  - Welche Dienste (Speicherplatz, Teamarbeit, Chat)
  - Wer ist betroffen?
  - Dürfen Daten extern abgespeichert werden
    ➔ Vorsicht bei Geheimhaltung oder abgabenrechtlich relevanten Daten

Wie kann ich mich sortieren?

- Immer Verantwortlichkeitssphären
  ➔ Hochschule / Händler / Anbieter / Subdienstleister
- Information und Dokumentation
- Gewährung der Betroffenenrechte
- Verarbeitung
  - Nutzende und Administratoren
    - Einwilligung
    - oder universitärer Aufgabe, wenn keine freiwillige Nutzung
  - Gäste
    - Einwilligung
  - Drittbetroffene in den gespeicherten Daten
    - Grundsätzlich nur im Rahmen universitäre Aufgabe

Echte anonyme Daten

EuGH Urteil vom 19.10.2016 C-582/14
Wann endet der Personenbezug von Daten?
- sehr hoher personeller Aufwand …
- sehr hoher wirtschaftlicher Aufwand …
- praktisch nicht durchführbar …
- gesetzliche Verbote …

… einen Personenbezug herzustellen

Beispiele für personenbezogene Daten:
IP-Adressen, Hardwareadressen, Computernahmen, Browserläufe

Folgen
- Datenquellen im Zeitpunkt der „Erhebung“ und dann bei jeder Verarbeitung
- Regelmäßig prüfen, ob inzwischen Personenbezug

Pseudonyme Daten

Gegenüber dem Original verkleinert
Napoleon Vier aus nl Creative-Commons-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 nicht portiert“ lizenziert.

Pseudonym = mit Zusatzwissen identifizierbar

Beispiel: Maxi Müller wird zu ID123
Odysseus zu Οὖτις

Treuhänderische Pseudonymisierung: Ein Dritter entfernt die identifizierbaren Merkmale, in der eigenen Datenbank selbst kein Personenbezug

Eigene Pseudonymisierung: Verwaltungsoberfläche zeigt Daten ohne identifizierbare Merkmale, in einer separaten und geschützten Datenbank besteht noch mit Personenbezug

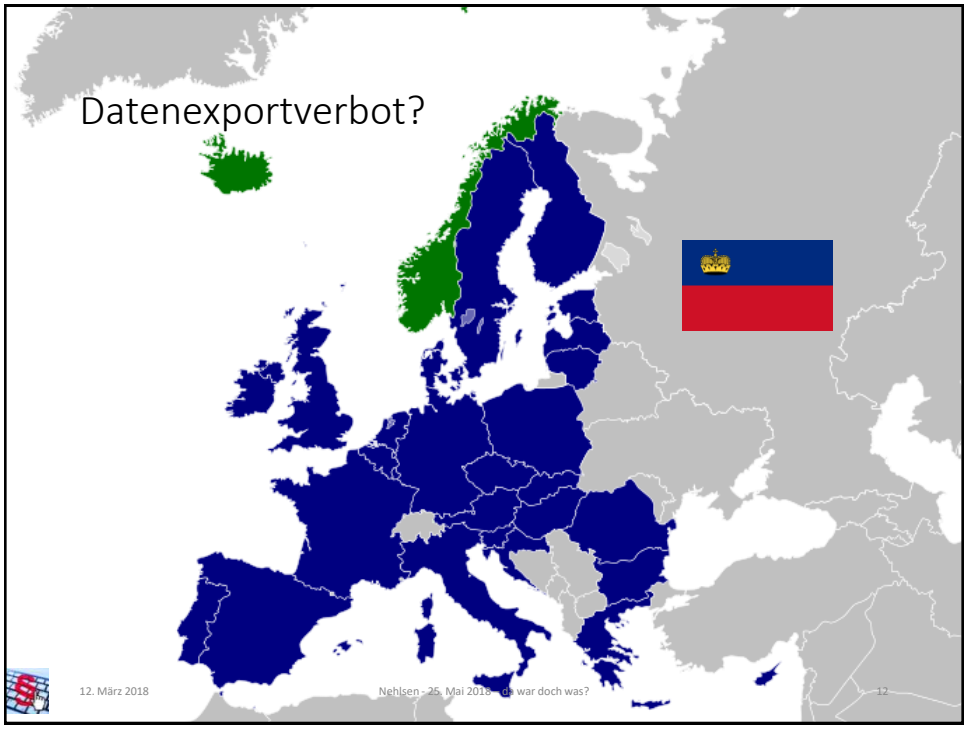
Einwilligung allgemein

- Freiwilligkeit
  Mehr als nur ohne „Zwang“, d.h. nur bei echten Entscheidungsalternativen

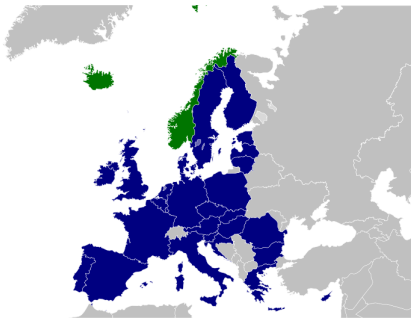
Aufklärung

- über Zweck der Datenverarbeitung
- Folgen einer Verweigerung

- Bei mehreren Erklärungen besondere Hervorhebung



Standort der **eigenen** Server oder der mit der Wartung beauftragten Person



(Auch im EWR)

Erfüllen der Datensicherheit

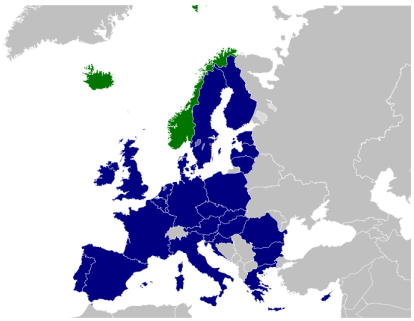
Außerhalb des EWR

- Sicherer Drittstaat
- Einwilligung + Risikoaufklärung
- Genehmigte verbindliche interne Datenschutzvorschriften

Sonderfall USA

- Auch EU-US Privacy Shield möglich (je nach Kategorie)

Auftragsverarbeitung (auch Wartung)



Immer (Auch im EWR)
Erfüllen der Datensicherheit
Vertrag zur Auftragsverarbeitung
Regelung zu Unteraufträgen

Außerhalb des EWR
- Sicherer Drittstaat
- Standarddatenschutzklauseln

Sonderfall USA
- Auch EU-US Privacy Shield möglich (je nach Kategorie)

Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Angemessener Datenschutz
- Sicherer Drittstaat
- Für die USA wenn nach EU-US Privacy Shield (je nach Kategorie) zertifiziert

Geeignete Garantien
- Genehmigte verbindliche interne Datenschutzvorschriften
- Standarddatenschutzklauseln
- Genehmigte EU-Datenschutzzertifizierung (gibt es noch nicht)
- Genehmigung durch die zuständige Aufsichtsbehörde

Alternative
- Einwilligung + Risikoaufklärung
- Für Vertragserfüllung erforderlich
- Im Interesse des Betroffenen zur Vertragserfüllung

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

Vereinfachte Gesamtübersicht zur Offenlegung von Daten

	Hochschule	Anbieter / Lizenzportal	Händler	Subdienstleister
Lizenzdaten mit Einzelabruf	Vertragserfüllung / Haushaltsrecht	Vertragserfüllung	Vertragserfüllung	Auftrags-verarbeitung *
Flatrate	Haushaltsrecht	Berechtigte Interessen?		
Einkauf	Universitäre Aufgabe	Vertragserfüllung	Vertragserfüllung	Auftrags-verarbeitung *
Nutzende und Administration	Einwilligung	Einwilligung / Auftragsverarbeitung		(Unter-)Auftrags-verarbeitung *
	Universitäre Aufgabe	Auftragsverarbeitung		Unterauftrags-verarbeitung *
Gäste	Einwilligung	Vertragserfüllung / Auftragsverarbeitung		(Unter-)Auftrags-verarbeitung *
Drittbetroffene	Universitäre Aufgabe	Auftragsverarbeitung		Unterauftrags-verarbeitung *
Nur Information	Interne Kontrolle + Information	Entscheidung nach Sicherheitsbedürfnis	Gesonderter Vertrag	Kontrollrechte / besondere Vorsicht

Verzeichnis der Verarbeitungstätigkeiten

Zunächst Aufgabe der Leitung, Aufgabe kann aber anderen Stellen zugewiesen werden.

Beispiele unter:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

https://www.rehmnetz.de/__STATIC__/topics/allgemeine-verwaltung/datenschutzverordnung/sonderformate/self/verzeichnis-von-verarbeitungstaetigkeiten-nach-art_1484137548000.docx

Informationspflichten

Situation 1 - direkter Datenerhebung

Unmittelbare Information, ggf. in verkürzter Form und langer Form

Situation 2 – indirekte Erhebung

Information innerhalb eines Monats

Muster unter:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf Seite 8

Sicherheitsmaßnahmen bei Datenverarbeitung

- Pseudonymisierung;
- Verschlüsselung;
- Gewährleistung der Vertraulichkeit;
- Gewährleistung der Integrität;
- Gewährleistung der Verfügbarkeit;
- Gewährleistung der Belastbarkeit der Systeme;
- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall;
- Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Sicherheit der Datenverarbeitung

Ein guter Ansatz ist die Orientierung an ISO 27002 und ihren Kontrollen

Muster

https://www.activemind.de/magazin/technische-organisatorische-massnahmen-dsgvo/

https://www.bvdnet.de/wp-content/uploads/2017/06/Muster_Verz_der_Verarbeitungst%C3%A4tigkeiten_TOMs.pdf

Was ist zu tun?

- Verantwortlichkeitssphären klären
  - Hochschule
  - Händler
  - Anbieter
  - Subdienstleister
- Verantwortlichkeiten und Prozesse intern klären
  - Datenschutzbeauftragte
  - Personalrat
  - Informationssicherheitsbeauftragte
  - Einkauf
- Information und Dokumentation
  - Datenschutzbeipackzettel
  - Tätigkeitsverzeichnisse

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Johannes Nehlsen
Tel.: 0931/31-84217
Johannes.Nehlsen@uni-wuerzburg.de