Datenschutz in Lieferantenbeziehungen

Johannes Nehlsen

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

Über mich

Stabsstelle IT-Recht für die bayerischen staatlichen Universitäten und Hochschulen

c/o Rechenzentrum Universität Würzburg
Rechenzentrum Julius-Maximilians-Universität Würzburg

Zuvor u.a. wissenschaftlicher Mitarbeiter in der Rechnerbetriebsgruppe der Juristischen Fakultät
IT-Support, IT-(Rechts)-Kurse

Rechtsassessor - Volljurist

Wahlstation in Manchester UK
Eversheds LLP

Rechtsinformatikzertifikat
Ludwig-Maximilians-Universität München

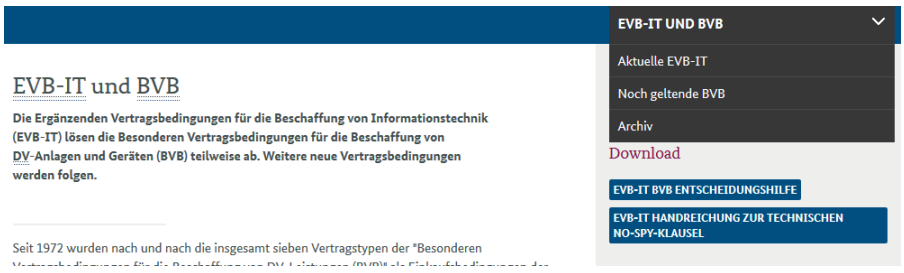
Zertifizierter Informationssicherheitsbeauftragter
Ostbayerische Technische Hochschule Regensburg

Die Hochschule macht doch alles selber!

- Softwareanbieter
- Support und Wartungsleistungen
- Telefonie
- Cloudservices
- Hardwarebeschaffung
- Gewährleistung
- Garantieabwicklung
- Hardwareentsorgung
- Reinigungsleistungen
- Kooperationen

Kein Problem: Wir verwenden doch EVB-IT!

- EVB-IT AGB schaffen nur das gesetzliche Minimum
- Muster der Datenschutzbehörden gehen darüber hinaus
- Haushaltsrecht „missbilligt“ Abweichungen von EVB-IT AGB
- EVB -IT schafft keine Pflichten für Hersteller IT schafft keine Pflichten für T schafft keine Pflichten für Hersteller



Kein Problem wir haben doch IaaS über GÉANT?

23/04/2016 S80 – – Services – Contract notice – Open procedure

I. II. III. IV. VI.

United Kingdom–Cambridge: Software package and information systems

2016/S 080–142458

Contract notice

Services

Directive 2004/18/EC

Section I: Contracting authority

I.1) **Name, addresses and contact point(s)**
GEANT Limited
City House, 126–130 Hills Road

The tender aims to ensure that:
— Suppliers offer a IaaS feature set which matches the Customers' needs;
— Data is handled safely and Suppliers meet European and national regulations;
— The Customers can aggregate demand and costs are affordable and predictable;
— Services can be acquired and used through the Customers' purchasing and management structures;
— Services are connected to and compatible with the Customers network and Identity Management capabilities.

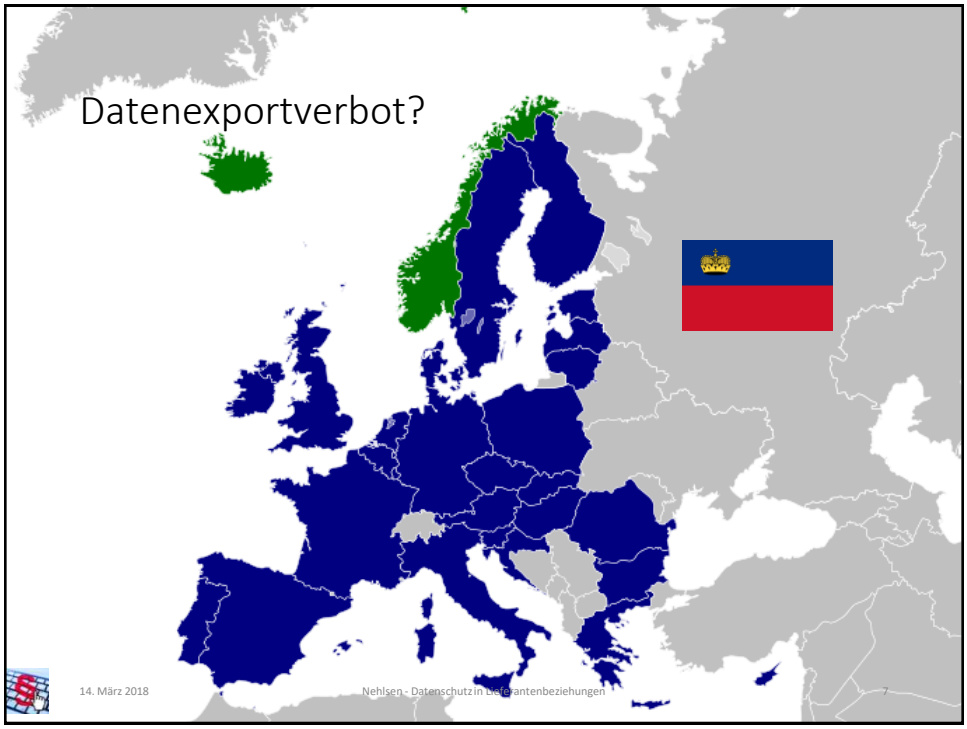
Ich übermittle doch gar keine Daten!

Beispiel:

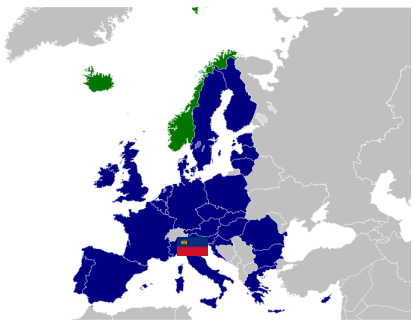
- Der Begriff „übermitteln“

- Keine unterschiedlichen Begriffsdefinitionen zwischen Richtlinie und nationalen Gesetzen
- Einheitliche Begriffe aus der DSGVO
- Vom nationalen Recht unabhängige Auslegung

Kostenfreier Aufsatz: Rechtsfragen zu Cloud-Angeboten für Hochschulen



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



(Auch im EWR)

Erfüllen der Datensicherheit

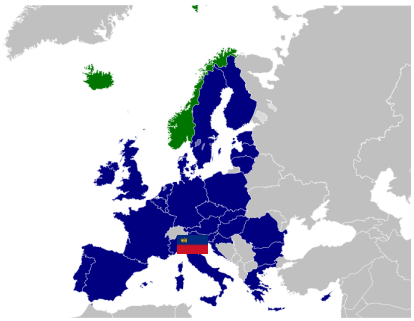
Außerhalb des EWR

- 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

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

Mitverantwortung für Datenverarbeitung der Dienstleiter?

SCHLUSSANTRÄGE DES GENERALANWALTS
YVES BOT
vom 24. Oktober 2017[1]

Rechtssache C-210/16

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
gegen
Wirtschaftsakademie Schleswig-Holstein GmbH,
Beteiligte:
Facebook Ireland Ltd,
Vertreter des Bundesinteresses beim Bundesverwaltungsgericht

(Vorabentscheidungsersuchen des Bundesverwaltungsgerichts [Deutschland])

„Vorlage zur Vorabentscheidung – Richtlinie 95/46/EG – Art. 2, 4 und 28 – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und freier Datenverkehr – Anordnung zur Deaktivierung einer Fanpage im sozialen Netzwerk Facebook – Begriff ‚für die Verarbeitung Verantwortlicher' – Verantwortlichkeit des Betreibers einer Fanpage – Gemeinsame Verantwortlichkeit – Anwendbares nationales Recht – Umfang der Einwirkungsbefugnisse der Kontrollstellen"

Telemetrie

- Privacy by Design
  - ✓ Einsatz von Pseudonymen
  - ✓ Richtiger Einsatz von Verschlüsselung
- Privacy by Default
  - ✓Opt-In für Telemetire
  - ✓ Wenn unvermeidbar und Anwendung unverzichtbar
    - Datensparsame Einstellungen bei Telemetrie
    - Ausweichmöglichkeiten schaffen soweit möglich

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

14. März 2018 Nehlsen - 25. Mai 2018 – da war doch was? 14

Was ist zu tun?

- Verantwortlichkeitssphären klären
  - Hochschule
  - Händler
  - Anbieter
  - Subdienstleister
- Verantwortlichkeiten 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