

Datenschutz in Lieferantenbeziehungen

Johannes Nehlsen

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



Dieses Werk ohne Zitate, geschützte Marken und unwesentlichem Beiwerk ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.

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



14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

3

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

EVB-IT und BVB

Die Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT) lösen die Besonderen Vertragsbedingungen für die Beschaffung von **DV**-Anlagen und Geräten (BVB) teilweise ab. Weitere neue Vertragsbedingungen werden folgen.

Seit 1972 wurden nach und nach die insgesamt sieben Vertragstypen der "Besonderen

EVB-IT UND BVB ▾

Aktuelle EVB-IT

Noch geltende BVB

Archiv

[Download](#)

[EVB-IT BVB ENTSCHEIDUNGSHILFE](#)

[EVB-IT HANDREICHUNG ZUR TECHNISCHEN NO-SPY-KLAUSEL](#)



14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

4

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

1.1) 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.



14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

5

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

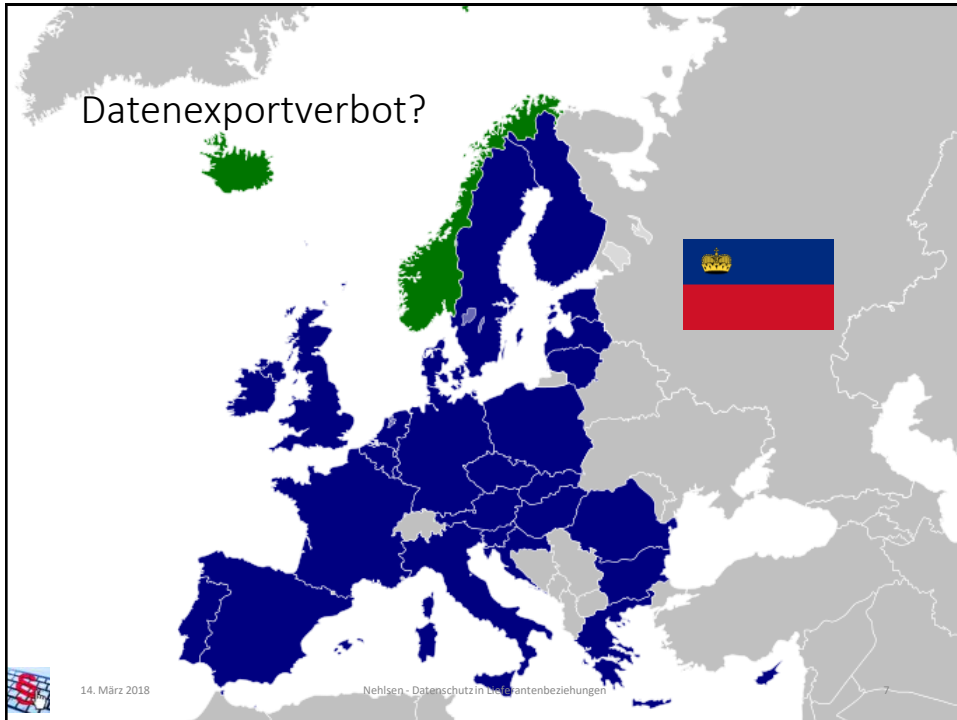
[Kostenfreier Aufsatz](#): Rechtsfragen zu Cloud-Angeboten für Hochschulen



14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

6



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

(Auch im EWR)

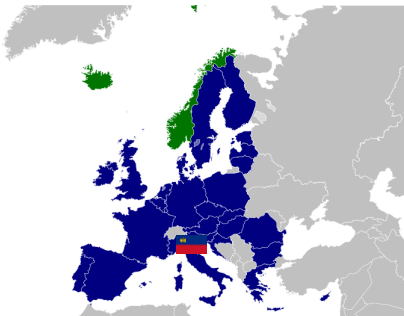
Erfüllen der Datensicherheit

Außerhalb des EWR

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

Sonderfall USA

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

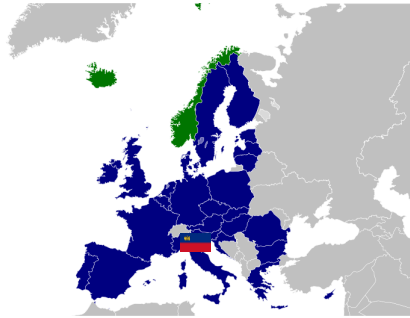


14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

8

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-Datenschutzertifizierung (gibt es noch nicht)
- Genehmigung durch die zuständige Aufsichtsbehörde

Alternativen

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





СЪД НА ЕВРОПЕЙСКИТЕ СЪДИИ
 TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
 SODINI DVŮR EVROPSKÉ UNIE
 DEN EUROPEISKE UNIONS DOMSTOLE
 GERICHTSHOF DER EUROPEISCHEN UNION
 EUROOPA LIIDU KOHUS
 ΑΡΧΑΪΟΤΗΡΕΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
 COURT OF JUSTICE OF THE EUROPEAN UNION
 COUR DE JUSTICE DE L'UNION EUROPÉENNE
 CURTE DE JUSTITIE A UNIUNII EUROPENE
 CURT BIRENTHÉISAS AN AGONTAIS EORFARIGE
 SUD EUROPSKE UNIE
 CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA
 LUXEMBOURG

EUROPOS SAVIENBAS TIESA
 EUROPOS SĄJUNGOS TEISGIMU TEISMAS
 AZ EUROPAI UNIO BÍRSÁGJA
 IL-QORTI TAL-GIUSTIZZJA TAL-UNJONI EWROPEA
 HOF VAN JUSTITIE VAN DE EUROPESE UNIE
 TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
 TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
 CURTEA DE JUSTITIE A UNIUNII EUROPENE
 SUDNY DVŮR EVROPSKÉ UNIE
 SOUDSŤE EVROPSKE UNIE
 EUROOPAN UNIONIN TUOMIOUSTUEN
 EUROPEISKA UNIONENS DOMSTOLE


SCHLUSSANTRÄGE DES GENERALANWALTS
YVES BOT
 vom 24. Oktober 2017¹

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“




14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

11

Telemetrie

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



14. März 2018

Nehlsen - Datenschutz in Lieferantenbeziehungen

12



Vereinfachte Gesamtübersicht zur Offenlegung von Daten

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



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

Johannes Nehlsen – Datenschutz in Lieferantenbeziehungen: Dieses Werk ohne Zitate, Firmenlogos und unwesentlichem Beiwerk ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).

