Big Tech - Vertragswerk zum Datenschutz vs. Realität

Ihr Referent

Haupttätigkeit:

Stabsstelle IT-Recht der bayerischen staatlichen Universitäten und Hochschulen

Nun als HITS IT-Recht des bayerischen Digitalverbund

Sitz am Rechenzentrum der Universität Würzburg

Datenschutzbeauftragter für die virtuelle Hochschule Bayern

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
- X/Bluesky/Mastodon: @JoNehlsen

Agenda

- Bayern
- Auftragsverarbeitungen und Vertragskonstruktionen
- Internationaler Datentransfer
- Kleingedrucktes
- Kopie der Garantien für den internationalen Datentransfer
- Warnung: Wenn Sie lieber gut gläubig bleiben wollen, bitte nicht zu hören.

Bayern ☺

Aktuell über 52 Kurzinformationen und zahlreiche Orientierungshilfen

Internationale Datentransfers Orientierungshilfe Rn 38

Beispiel 1: Ein Landratsamt möchte zur Datenspeicherung die Cloud-Dienste eines Anbieters mit Sitz in Singapur verwenden. Sofern das Landratsamt nicht selbst einen Vertrag mit dem entsprechenden Dienstleister schließt, sondern mit einem in der EU ansässigen Auftragsverarbeiter, der die Daten an den Cloud-Anbieter in Singapur als Unterauftragsverarbeiter übermittelt, ist das Landratsamt nicht als Datenexporteur zu betrachten. Stattdessen muss der Auftragsverarbeiter das Datenschutzniveau prüfen und mit dem Unterauftragsverarbeiter den Abschluss von Standardvertragsklauseln und gegebenenfalls die wirksame Umsetzung zusätzlicher Maßnahmen vereinbaren.

Folgebeispiele dann jedoch mit Pflicht der Nachforschung durch den Verantwortlichen (Rechenschaftspflicht).

Internationale Datentransfers Orientierungshilfe Teil 2 Rn. 95

Praxistipp: Bis auf Weiteres akzeptiert der Bayerische Landesbeauftragte für den Datenschutz unter den oben unter Rn. 94 dargelegten Anforderungen diesen subjektiven, risikobasierten Ansatz, der den SCC zu entnehmen ist und den auch die FAQ der EU-Kommission zu den SCC stützen.

Es ist daher nicht erforderlich, den rein objektiven Ansatz, den die EDSA-Empfehlungen zunächst vermuten ließen und der vor allem eine abstrakte Betrachtung der Gesetze im Drittland zu verlangen scheint, im Rahmen der SCC zu verfolgen.

- ➔ Bisher keine(?) US-Dienste-Anfragen bei großen Clouddiensten bezüglich des Sektors Bildung
- ➔ Daher keine hohen Risiken für Hochschulen, wenn Clouddienste mit Übermittlungen in die Vereinigten Staaten genutzt werden?

AWS

Aus dem DPA

https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf

1.3 Details of Data Processing.

1.3.1 Subject matter. The subject matter of the data processing under this DPA is Customer Data.

“Customer Data” means the Personal Data that is uploaded to the Services under Customer’s AWS accounts.

➔ Verkehrs-, Meta-, und Maschinendaten nicht von der Auftragsverarbeitung umfasst.

Lösung: Soweit es sich bei diesen Daten um personenbezogen Daten handelt, die in Verantwortung des Verantwortlichen verarbeitet werden, sollte „AWS“ Telekommunikationsdiensteanbeiter sein.

Apple School Manager – ohne Worte

WILLKOMMEN BEI APPLE SCHOOL MANAGER*

[Allgemeine Nutzungsbedingungen unter https://school.apple.com/]

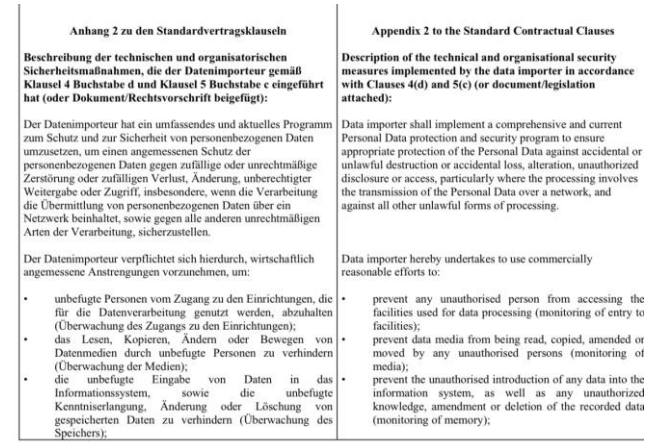
Dieser Apple School Manager-Vertrag („Vertrag“) zwischen Ihrer Einrichtung und Apple regelt die Nutzung der Software, der Services und der Websites, aus denen Apple School Manager besteht (zusammen der „Dienst“), durch Ihre Einrichtung. Sie bestätigen, dass Sie in vollem Umfang gesetzlich befugt sind, Ihre Einrichtung an diese Bedingungen zu binden.

…

D Ihre Überprüfungs-/Inspektionsrechte.

Soweit die DSGVO für die Verarbeitung Ihrer Persönlichen Daten oder jener Ihrer Endnutzer anwendbar ist, liefert Ihnen Apple die Informationen, die notwendig sind, um Artikel 28 der DSGVO zu entsprechen. Falls Sie Überprüfungsrechte gemäß anderen anwendbaren Rechtsbestimmungen haben, liefert Ihnen Apple die Informationen, die notwendig sind, um Ihren Pflichten aus diesen Rechtsbestimmungen nachzukommen. Wenn Sie beschließen, Ihre Überprüfungsrechte aus diesem Abschnitt 3D auszuüben, weist Apple die Einhaltung durch Übergabe einer Kopie der Zertifizierung nach ISO 27001 und der Zertifizierung nach ISO 27018 von Apple nach.

TOM von Apple ????



Anhang 2 zu den Standardvertragsklauseln	Appendix 2 to the Standard Contractual Clauses
Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):	**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**
Der Datenimporteur hat ein umfassendes und aktuelles Programm zum Schutz und zur Sicherheit von personenbezogenen Daten umzusetzen, um einen angemessenen Schutz der personenbezogenen Daten gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust, Änderung, unberechtigter Weitergabe oder Zugriff, insbesondere, wenn die Verarbeitung die Übermittlung von personenbezogenen Daten über ein Netzwerk beinhaltet, sowie gegen alle anderen unrechtmäßigen Arten der Verarbeitung, sicherzustellen.	Data importer shall implement a comprehensive and current Personal Data protection and security program to ensure appropriate protection of the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, particularly where the processing involves the transmission of the Personal Data over a network, and against all other unlawful forms of processing.
Der Datenimporteur verpflichtet sich hierdurch, wirtschaftlich angemessene Anstrengungen vorzunehmen, um:	Data importer hereby undertakes to use commercially reasonable efforts to:
• unbefugte Personen vom Zugang zu den Einrichtungen, die für die Datenverarbeitung genutzt werden, abzuhalten (Überwachung des Zugangs zu den Einrichtungen); • das Lesen, Kopieren, Ändern oder Bewegen von Datenmedien durch unbefugte Personen zu verhindern (Überwachung der Medien); • die unbefugte Eingabe von Daten in das Informationssystem, sowie die unbefugte Kenntniserlangung, Änderung oder Löschung von gespeicherten Daten zu verhindern (Überwachung des Speichers);	• prevent any unauthorised person from accessing the facilities used for data processing (monitoring of entry to facilities); • prevent data media from being read, copied, amended or moved by any unauthorised persons (monitoring of media); • prevent the unauthorised introduction of any data into the information system, as well as any unauthorized knowledge, amendment or deletion of the recorded data (monitoring of memory);
• die Nutzung von Datenverarbeitungssystemen durch unbefugte Personen, die die Übermittlungseinrichtungen nutzen, zu verhindern (Überwachung der Nutzung); • sicherzustellen, dass befugte Personen, wenn sie ein automatisiertes Datenverarbeitungssystem nutzen, nur auf solche Daten zugreifen können, die in ihre Zugriffsberechtigung fallen, (Zugriffskontrolle); • die Überprüfung und Speicherung der Identität von Dritten, an die die Daten durch Übermittlungseinrichtungen übermittelt werden können, sicherzustellen (Überwachung der Übermittlung); • sicherzustellen, dass die Identität aller Personen, die Zugriff auf das Informationssystem haben oder gehabt haben, sowie die Daten, die in das System eingeführt wurden, nachträglich, zu jeder Zeit und von den zuständigen Personen überprüft und aufgezeichnet werden können (Überwachung der Eingabe). • das Lesen, Kopieren, Ändern oder Löschen von Daten in einer unbefugten Art und Weise zu verhindern, wenn die Daten offengelegt und Datenmedien transportiert werden (Überwachung des Transports); und • die Daten durch das Erstellen von Backup-Kopien zu sichern (Überwachung der Verfügbarkeit).	• prevent data processing systems from being used by unauthorised persons using data transmission facilities (monitoring of usage); • ensure that authorised persons, when using an automated data processing system, may access only those data that are within their competence (monitoring of access); • ensure the checking and recording of the identity of third parties to whom the data can be transmitted by transmission facilities (monitoring of transmission); • ensure that the identity of all persons who have or have had access to the information system and the data introduced into the system can be checked and recorded ex post facto, at any time and by relevant persons (monitoring of introduction); • prevent data from being read, copied, amended or deleted in an unauthorised manner when data are disclosed and data media transported (monitoring of transport); and • safeguard data by creating backup copies (monitoring of availability).
Es wird anerkannt, dass die vorstehenden technischen und organisatorischen Maßnahmen dem technischen Fortschritt, organisatorischen Änderungen und anderen Entwicklungen unterliegen und der Datenimporteur gleichwertige alternative Maßnahmen einführen darf, wenn diese Maßnahmen nicht das Datenschutzniveau, das vertraglich vereinbart wurde, vermindern.	It is acknowledged that the foregoing technical and organisational measures are subject to technical progress, organisational changes, and other developments, and the Data Importer may implement adequate alternative measures if these measures do not derogate from the level of protection contractually agreed upon.

https://help.apple.com/pdf/security/de_DE/apple-platform-security-guide-d.pdf

https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-eu-en.pdf

https://support.apple.com/de-de/guide/certifications/apc34d2c0468b/web

Atlassian

2.6. ***Restricted transfers:*** The parties agree that when the transfer of personal data from Customer (as "data exporter") to Atlassian (as "data importer") is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the transfer will be subject to the Standard Contractual Clauses, which are deemed incorporated into and form a part of this DPA, as follows:

(a) In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with Section 2.6(a) of this DPA, the EU SCCs will apply, completed as follows:

i. Module Two or Module Three will apply (as applicable);

ii. in Clause 7, the optional docking clause will not apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes will be as set out in Section 2.10 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in Clause 18(b), disputes will be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A to this DPA, as applicable; and

viii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B to this DPA;

(b) In relation to transfers of personal data protected by the EU GDPR and processed in accordance with Section 2.2(b) of this DPA, the EU SCCs apply, completed as follows:

i. Module One will apply;

https://www.atlassian.com/legal/data-processing-addendum

Part B: Description of processing and transfer (as applicable) for Module 1 of the Standard Contractual Clauses (reference to Sections 2.2(b) as well as 2.6(b) DPA)

All Cloud Products: Atlassian as a controller	
Categories of data subjects	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
Categories of personal data transferred	**Personal data relating to or obtained in connection with the operation, support or use of the Services, e.g.:** *User Account Information,* for example pseudonymous Atlassian IDs, Cloud IDs, Site IDs,Tenant ID, Segment Anonymous IDs *Payment and billing information, to the extent it includes personal data* *Device and connection information, for example:* ● IP address ● Cookie information ● Device information ● Browser information *Information on the use of the Services, for example:* ● Event Name (i.e., what action the user performed) ● Event Timestamp ● Page URL ● Referring URL *Support data** Personal data provided through various Atlassian support channels, including for example Atlassian ID, SEN (Support Entitlement Number), username, contact information and any personal data contained within a summary of the problem experienced or information needed to resolve the support case. * If any user generated content is submitted as attachments via support tickets, Atlassian acts as a processor of such personal data and Sections 2.2(a)as well as 2.6(a) DPA apply accordingly.

ChatGPT
OffTopic: Wer hat ein Text- und Datamining OptOut im Impressum?

Exhibit B

ANNEX II

a. OpenAI will process Customer Data that originates in tl
with the standard contractual clauses adopted by the E
which are deemed entered into (and incorporated into
as follows:
   i. Module Two (Controller to Processor) of the EU
   and OpenAI is processing Customer Data as a p
   ii. Module Three (Processor to Sub-Processor) c
   processor and OpenAI is processing C

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organisational measures as set forth in the OpenAI Information Security Addendum, which will be provided upon request.

b. For each module of the EU SCCs, where applic
   i. The optional docking clause in Clause
   ii. In Clause 9, Option 2 (general writt
   period for prior notice of sub-process
   DPA.
   iii. In Clause 11, the optional language d
   iv. All square brackets in Clause 13 are h
   v. In Clause 17 (Option 1), the EU SCCs v
   data exporter is located;
   vi. In Clause 18(b), disputes will be resolv
   the data exporter is located;
   vii. Exhibit A to this DPA contains the info
   SCCs;
   viii. Exhibit B to this DPA contains the info

[EXT] Fwd: [#7214565] Fwd: [#7214488] Sent by: Johannes Nehlsen, Inquiry for Article 27 Representative Client - OpenAI, L.L.C.

Antworten | Allen antworten

OP OpenAI Privacy <privacy@openai.com>
An RZ-Stabsstelle IT-Recht

Sie haben diese Nachricht am 17.03.2023 17:07 weitergeleitet.
Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

OpenAI Information Security Addendum (Feb 2023).docx 24 KB

Hello,

We received your inquiry. Attached is our Security Addendum. Please reach out to support@openai.com if you have any additional questions.

Thank you,
The OpenAI Team

On Friday, March 17th 2023, 4:46:28 PM rz-stabsstelle-it-recht@uni-wuerzburg.de <rz-stabsstelle-it-recht@uni-wuerzburg.de> wrote:

Name of the Organization Your Inquiry Relates to *: OpenAI, L.L.C.

Vertragskonstruktion des Microsoft-Hochschulvertrages (vereinfacht)

CASA - Rahmen

EES - Beitritt

Zusatzvereinbarung = Besonderheit des Bundesvertrages der Hochschulen

Geheimhaltungsvereinbarung
= zwingend notwendige Ergänzung bei Cloudnutzung

Nutzungsbestimmungen und Datenschutz-/Sicherheitsverpflichtungen für Microsoft Produkte und Dienste
➔ Früher PT und OST

SLA – Verfügbarkeit

Grundlagen für Microsoft 365

Microsoft-Servicevertrag, dient der Regelung für Nebendienste

Microsoft Online-Abonnement-Vertrag (Azure)

SLA - Azure

Grundlagen für Azure ohne Microsoft 365

DPA Terms – Datenschutz / Auftragsverarbeitung
Grundlage für das Outsourcing

Datenschutzerklärung von Microsoft, dient der Regelung, soweit keine Auftragsverarbeitung

Zentrale Verträge Adobe und Microsoft der Hochschulen

Verträge formal immer mit der irischen Niederlassung, die dann Unteraufträge vergibt

Verhandlung mit einem Team von Freiwilligen nebenbei mit Fokus auf Beschaffung

LRZ als Vertragshalter

Stabsstelle IT-Recht wurde in die Verhandlungen mitgenommen

Adobe DPA mit Feedback-Option

- Fast kein Feedback zum LRZ oder der Stabsstelle gekommen

Keine Verhandlungsoption für den Rahmenvertrag mit Microsoft

- Fast kein Feedback wirksam zu Microsoft kommuniziert

Warum passt die DSK-Kritik in dieser Form nicht?

- Verträge müssen nur mit der Auftragsverarbeitung sondern auch mit Lizenzvertrag (teilweise Begründung für Datenverarbeitungen) und Dokumentation (sind Weisungen) geprüft werden.

In den Vertragsverwerken

Campus und School Vertrag

7. *Datenschutz und Einhaltung von Gesetzen.*

a. Die Einrichtung stimmt der Verarbeitung von persönlichen Informationen durch Microsoft und ihre Vertreter zur Förderung des Gegenstandes dieses Vertrags zu. Die Einrichtung holt alle erforderlichen Zustimmungen von Dritten (einschließlich Kontaktpersonen, Handelspartnern, Distributoren, Verwaltern und Mitarbeitern der Einrichtung) nach den anwendbaren Privacy- und Datenschutzgesetzen ein, bevor er Microsoft persönliche Informationen zur Verfügung stellt.

b. Im Rahmen dieses Vertrages erhobene persönliche Informationen (i) können in die USA oder in jedes andere Land, in dem Microsoft oder ihre Serviceprovider Einrichtungen haben, übertragen, dort gespeichert und verarbeitet werden und (ii) unterliegen den in den Nutzungsrechten dargelegten Datenschutzbestimmungen. Microsoft wird die Anforderungen der Datenschutzgesetze des Europäischen Wirtschaftsraums und der Schweiz in Bezug auf die Erfassung, Nutzung, Übertragung, Aufbewahrung und sonstige Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum und der Schweiz einhalten.

Lizenzbestimmungen > Datenschutz- und Sicherheitsbestimmungen

Datenschutz- und Sicherheitsbestimmungen

Allgemeines | Core-Onlinedienste | EU-Datengrenzen-Dienste

Allgemeines

Die Datenschutz- und Sicherheitsbedingungen waren zuvor in Anlage 1 zu den Bestimmungen für Onlinedienste enthalten.

Der **Datenschutznachtrag** oder **DPA** (wie im Glossar definiert) regelt die Verpflichtungen der Parteien in Bezug auf die Verarbeitung und die Sicherheit von **Kundendaten**, **Professional Services-Daten** und **Personenbezogenen Daten** durch die Produkte Der **Datenschutznachtrag** kann hier unter https://aka.ms/DPA heruntergeladen werden. Bei Konflikten oder Widersprüchen zwischen den Bestimmungen des **DPA** und anderen Bestimmungen des Lizenzvertrags des Kunden (einschließlich der vorliegenden Bestimmungen) hat der **DPA** Vorrang.

Aus dem DPA ausgeschlossene Onlinedienste

Außer wie in den **Produktspezifischen Bedingungen** angegeben, gelten die Bedingungen des **DPA** nicht für: Bing Maps Mobile Asset-Management-Plattform, Bing Maps Transaktionen und Nutzer, Bing-Suchdienste, Kognitive Dienste in Containern, die auf der dedizierten Hardware des Kunden installiert sind, GitHub-Angebote, LinkedIn-Verkaufsnavigator, Microsoft Defender für IoT (mit Ausnahme aller mit der Cloud verbundenen Funktionen), Azure SQL Edge, Azure Stack HCI, Azure Stack Hub, Microsoft Graph Data Connect für ISVs, Microsoft Genomics und Visual Studio App Center-Test. Jeder dieser Onlinedienste unterliegt den Datenschutz- und Sicherheitsbestimmungen in den entsprechenden **produktspezifischen Bedingungen**.

Vom DPA ausgeschlossene Softwareprodukte

Außer wie in den **Produktspezifischen Bedingungen** angegeben, gelten die Bedingungen des **DPA** nicht für: Internetbasierte Funktionen in Softwareprodukten, Windows-Desktopbetriebssystemen, Windows-Servern und diesen Softwareprodukten als Teil anderer Produkte. Jedes dieser Produkte unterliegt den Datenschutz- und Sicherheitsbestimmungen in den entsprechenden **produktspezifischen Bedingungen**.

Nicht von Microsoft stammende Produkte

Für die Nutzung von nicht von Microsoft stammenden Produkten durch den Kunden gelten gesonderte Bestimmungen (wie in den Universellen Lizenzbestimmungen für Onlinedienste definiert).

Regionsausschlüsse in den DPA-Bestimmungen

Für die Onlinedienste von Dynamics 365 und Power Platform gelten die in Anhang A aufgeführten spezifischen Bestimmungen des **Datenschutznachtrags (DPA)**, die besagen, dass Microsoft Kopien von **Kundendaten** und Datenwiederherstellungsverfahren an einem anderen Ort speichert als dem der primären Computerausrüstung, die die **Kundendaten** verarbeitet, nicht für die folgenden Regionen: Vereinigte Arabische Emirate und Südafrika.

Produktbestimmungen

https://www.microsoft.com/licensing/terms/productoffering/WindowsServerStandardDatacenterEssentials/EES

EU-Datengrenzen-Dienste

Der Begriff „EU-Datengrenze“ bezeichnet die Computer, die Computerumgebung und die physischen Rechenzentren von Microsoft, die sich ausschließlich in der Europäischen Union (EU) und der Europäischen Freihandelsassoziation (EFTA) befinden. Der Begriff „EU-Datengrenzen-Dienste“ bezieht sich nur auf die in der nachstehenden Tabelle aufgeführten Onlinedienste, ohne jegliche Vorschauversionen.

Azure

Dynamics 365

Microsoft 365

Power-Plattform

Die Nutzung von EU-Datengrenzen-Diensten kann zu begrenzten Übermittlungen von Kundendaten außerhalb der EU-Datengrenze führen, … Solche Übermittlungen werden in Übereinstimmung mit dem Datenschutznachtrag und den Produktbestimmungen durchgeführt.

- **Remotezugriff**
- **Vom Kunden initiierte Übermittlungen**.
- **Schutz der Kunden**.
- **Verzeichnisdaten**.
- **Netzwerktransit**.
- **Dienstspezifische Übermittlungen**.

Big Tech von der EU – nur leider ohne Auftragsverarbeitung

Digital Europe
Language Tools

eTranslation	eSummary	Multilingual Tweet	Speech-to-Text
NLP Tools	Interactive Terminology for Europe	European Language Resource Coordination (ELRC)	
Digital Language Programme Building Block Information	Developer's Corner	https://language-tools.ec.europa.eu/	

Und wo gehen die Daten nur wirklich hin?

6. INTERNATIONAL DATA TRANSFERS

Transfer outside of the EU or EEA

Data is transferred to countries outside the EU or EEA

N/A

Transfer to international organisation(s)

Data is transferred to international organisation(s)

N/A

Comments

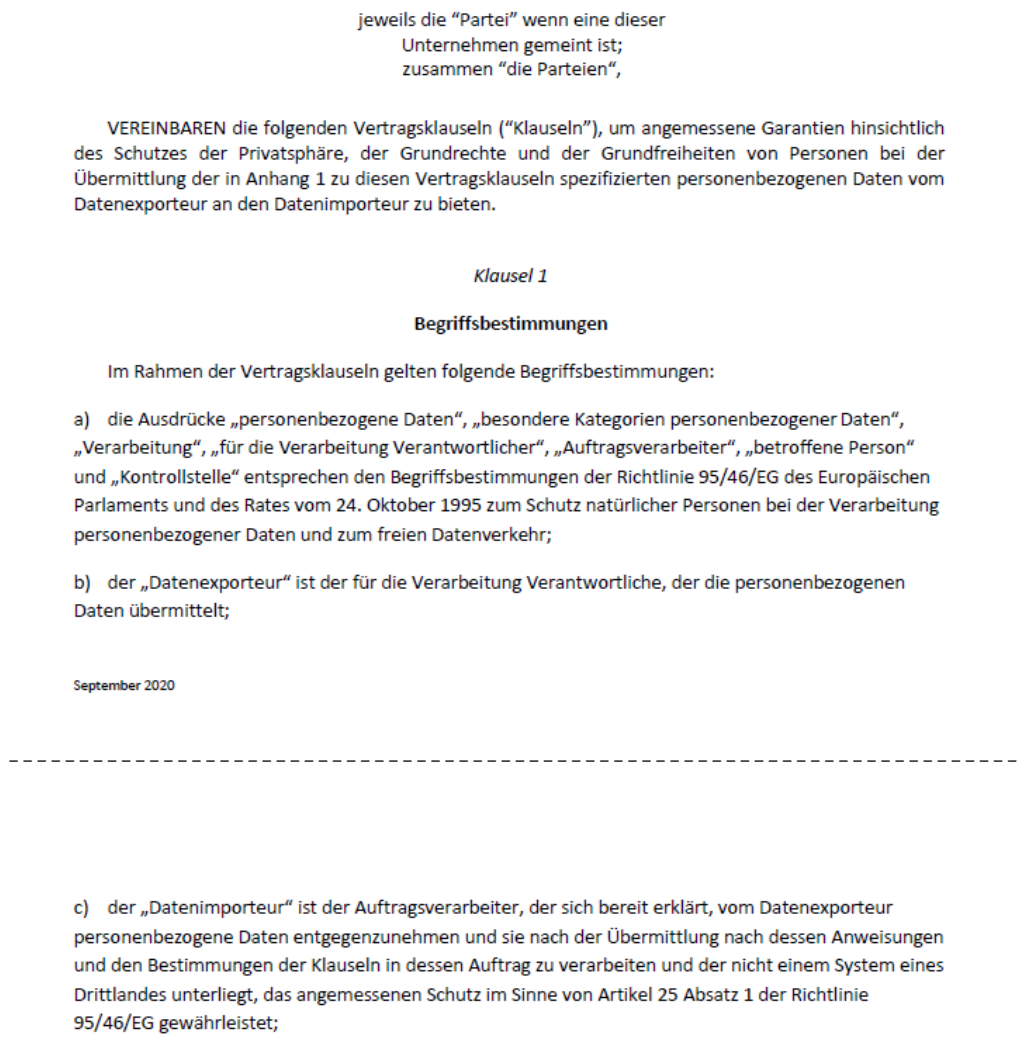
Comments/additional information on international data transfers

Personal data from EU Login is stored only in the data centre handled by DIGIT.

Microsoft Azure servers, which carry out the translation, are located in Amsterdam.

https://ec.europa.eu/dpo-register/detail/DPR-EC-00600.4

Was sehen Sie hier?



jeweils die "Partei" wenn eine dieser
Unternehmen gemeint ist;
zusammen "die Parteien",

VEREINBAREN die folgenden Vertragsklauseln ("Klauseln"), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten von Personen bei der Übermittlung der in Anhang 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur zu bieten.

Klausel 1

Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

a) die Ausdrücke „personenbezogene Daten", „besondere Kategorien personenbezogener Daten", „Verarbeitung", „für die Verarbeitung Verantwortlicher", „Auftragsverarbeiter", „betroffene Person" und „Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

b) der „Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

September 2020

---

c) der „Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

- Die Kopie der aktuell abgeschlossen Garantie …?
- Eine unnötige Garantie, da ein angemessenes Datenschutzniveau durch die EU-Kommission festgestellt worden ist, für das Sitzland …
- Die alten Standardvertragsklauseln …

… eines führenden Sicherheitslösungsanbieters

Microsoft 365 – November 2023 DPA aus der Ermöglichungsbrille

Auftragsverarbeitung

Wird den rechtlichen Mindestanforderungen bei einem praxisgerechten Verständnis von Clouddiensten gerecht

Verarbeitung zu eigenen Zwecken

Zwecke decken sich im Kern mit den von den Hochschulen selbst verfolgten Zwecken oder gesetzlichen Pflichten bzw. wären eine dauerhafte Aufgabe, soweit die Hochschulen die Lösung selbst betreiben und entwickeln würden

Internationaler Datentransfer

- Nunmehr Microsoft unter Data Privacy Framework
- Bloße Zugriffsmöglichkeit von Geheimdiensten und Ermittlungsbehörden in Drittstaaten ist noch keine Datenübermittlung im rechtlichen Sinne
- Noch kein Auskunftsersuchen an Microsoft von Behörden im Bereich Bildung bekannt
- Reduzierung weiterer Risiken durch das EU Data Boundary for the Microsoft Cloud
- Zusätzliche Schutzmaßnahmen: idR nur Verarbeitung von pseudonymen Daten, vertragliche Garantien von Microsoft

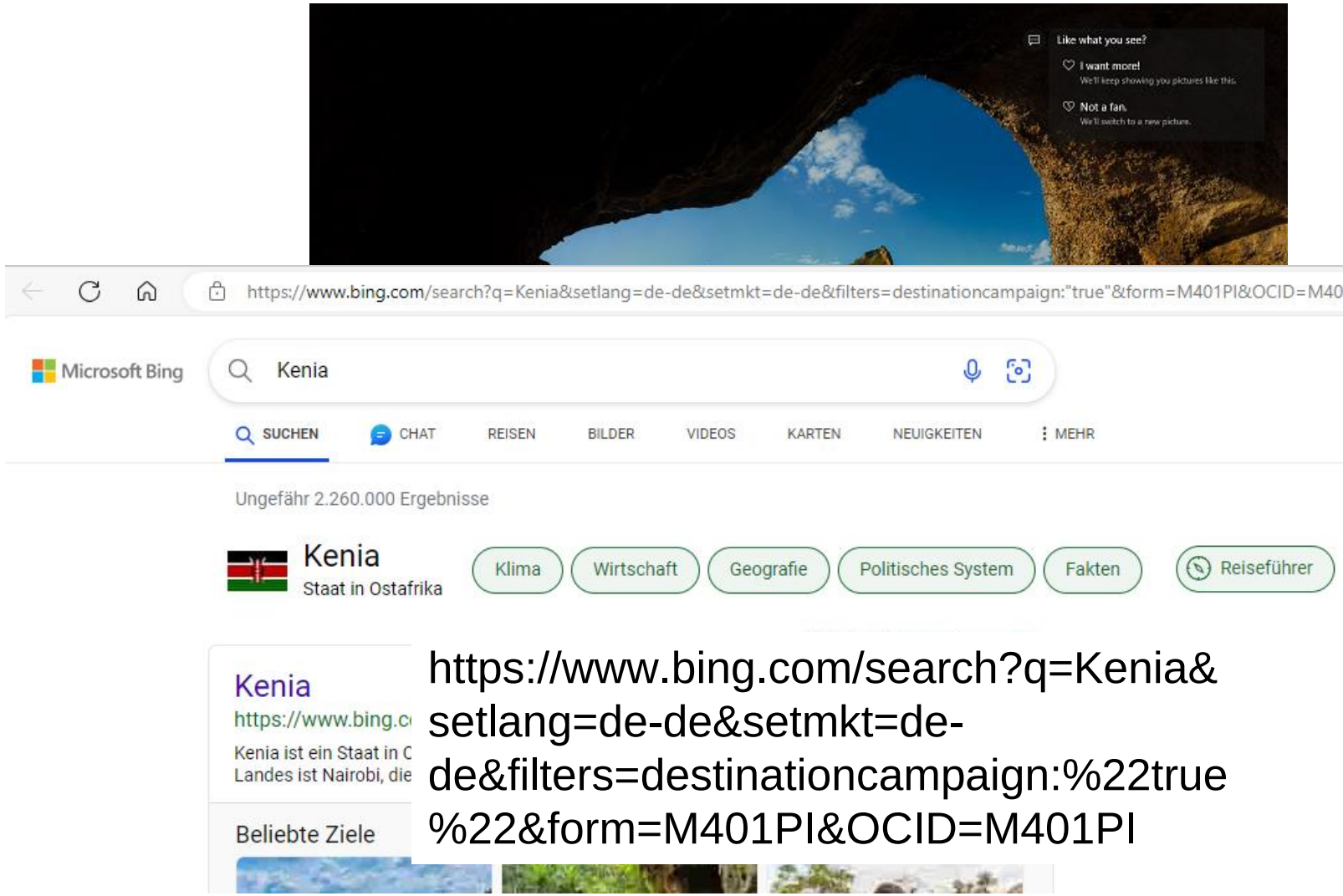
Datenschutzfolgenabschätzung

Für jeden Preis auf dem Markt erhältlich (200 € bis sechsstellig)

Verkettung – Blickpunkte in Windows

Dienst Blickpunkte

- Abwechslungsreiche Willkommensbildschirme
- User landen bei Klick auf Bing
- URL deutet Tracking an
- Bing läuft unter den dem allgemeinen Microsoft Servicevertrag
- Datenverarbeitung nach allgemeiner Datenschutzerklärung
- Technisch nun Verknüpfung von Unternehmensprofil und Bingnutzungsprofil möglich



Microsoft Search in Bing und Bing Chat Enterprise / Copilot

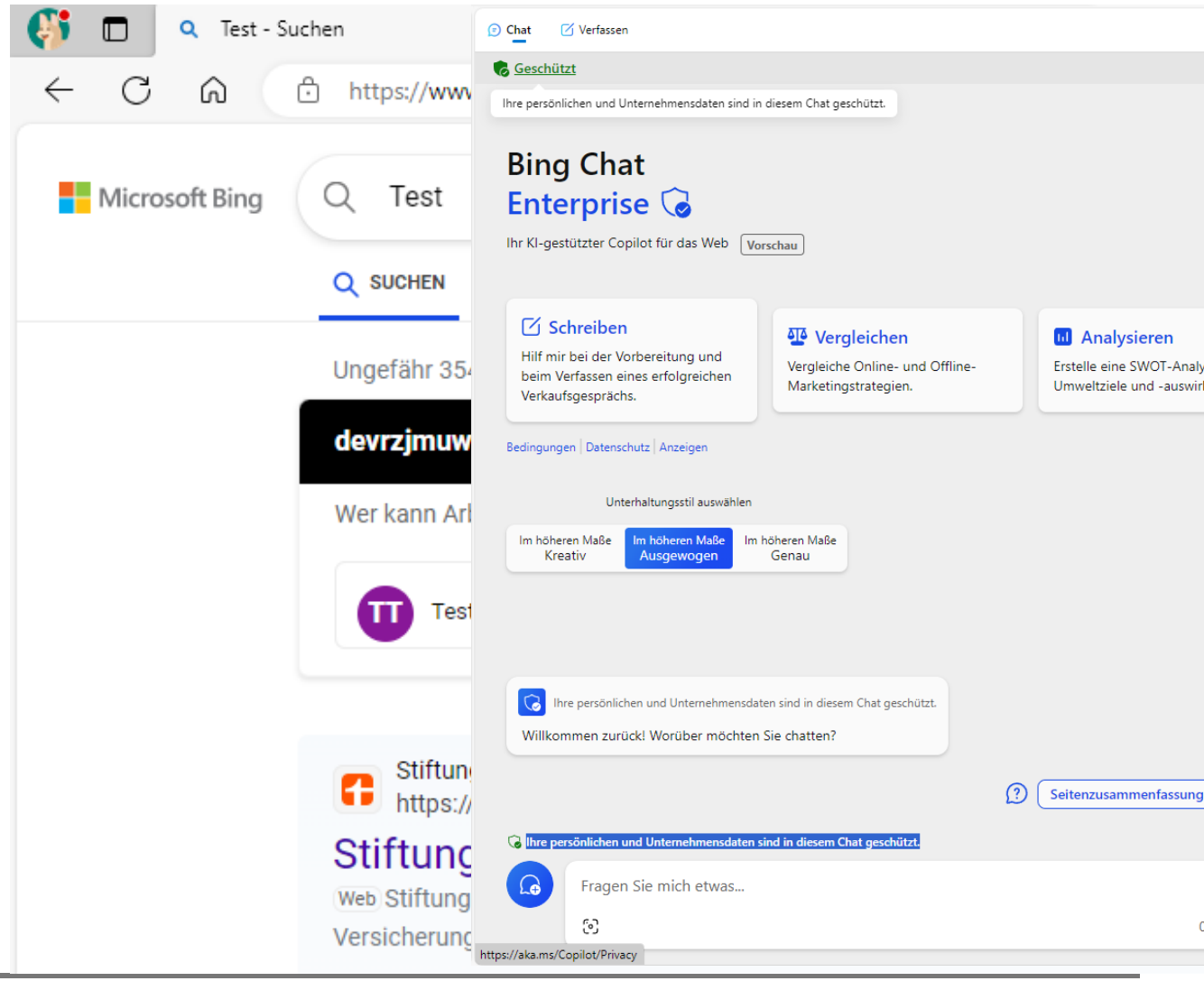
„Wenn ein Benutzer eine Suchabfrage in Microsoft Search in Bing eingibt, treten zwei gleichzeitige Suchanforderungen auf:

- Eine Suche nach den internen Ressourcen Ihrer Organisation.
- Eine separate Suche nach öffentlichen Ergebnissen von Bing.com.

Da Arbeitsplatzsuchen möglicherweise vertraulich sind, hat Microsoft Search eine Reihe von Vertrauensmaßnahmen implementiert, die beschreiben, wie die separate Suche von öffentlichen Ergebnissen von Bing.com behandelt wird.“

https://learn.microsoft.com/de-de/microsoftsearch/security-for-search

https://learn.microsoft.com/de-de/bing-chat-enterprise/overview



Copilot für Microsoft 365 oder Copilot für Microsoft 365 mit Internet (Bing)

„Wenn Microsoft Copilot für Microsoft 365 feststellt, dass Webinhalte eine relevantere Antwort liefern können, wird eine Suchabfrage generiert, die an Bing gesendet werden soll. Diese Suchabfrage basiert auf der Eingabeaufforderung des Benutzers, dem Copilot-Interaktionsverlauf und den Daten, auf die der Benutzer in Microsoft 365 Zugriff hat. Diese Abfrage kann die Daten Ihrer Organisation enthalten, aber das Konto des Benutzers und seine Mandanten-ID sind in der an Bing gesendeten Suchabfrage nicht enthalten.“

„Microsoft Bing ist ein separates Unternehmen von Microsoft 365, und Die Daten werden unabhängig von Microsoft 365 verwaltet. Die Verwendung von Bing ist durch den Microsoft-Servicevertrag zwischen jedem Benutzer und Microsoft sowie durch die Microsoft-Datenschutzerklärung abgedeckt. Der Nachtrag zum Datenschutz von Microsoft-Produkten und -Diensten (DPA) gilt nicht für die Verwendung von Bing.“

https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

https://learn.microsoft.com/de-de/microsoft-365-copilot/manage-public-web-access

Exkurs: Wer pflegt die Liste der Unterauftragsverarbeiter?

Adobe https://www.adobe.com/de/privacy/sub-processors.html

Microsoft Azure	Cloud computing and hosting services	Adobe Cloud Services (Experience Cloud, Creative Cloud and General Document Cloud)	Worldwide	Duration of Contract	Adobe TOMs
Amazon Web Services, Inc.	Hosting services	Adobe Cloud Services (Experience Cloud, Creative Cloud and General Document Cloud)	Worldwide	Duration of Contract	Adobe TOMs

Microsoft https://servicetrust.microsoft.com/DocumentPage/298b6d98-b8e8-4a8e-b3c2-3b3fc45e295c

Microsoft

Microsoft Online Services Subprocessors

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	DnB Registered Number	Parent Company
				USA			
Intercom, Inc. *	Visual Studio App Center	Customer chat and support	United States	18-21 St Stephen's Green 2nd Floor Dublin, Ireland	Ireland	985587563	Intercom, Inc.

Einschätzung

- Wahl zwischen Komfort und Produktivität oder besserem Datenschutzdesign
- Die Verzahnung Dienste von Microsoft 365 mit Bing von Microsoft ist für den normalen Nutzer nicht durchschaubar.
- Copilot für Microsoft 365 ohne Internet wäre aus Datenschutzschutzsicht (abseits der allgemeinen offenen Fragen zum DPA von Microsoft) dank Auftragsverarbeitung nutzbar
- Microsoft Search in Bing und Bing Chat Enterprise sollten tendenziell nicht zusammen mit Microsoft 365 genutzt werden
- Weitere Verknüpfungen mit Bing nur nach Optin der Nutzerinnen und Nutzer
- Aufbau von Alternativen

Ein Vertrag sie zu knechten …

Für Betroffene - Klausel Transparenz (M1 8.2, M2 8.3, M3 8.3, M4 -)

„Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung.“

Für den Verantwortlichen

Klausel Dokumentation und Einhaltung der Klauseln

„Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten Pflichten erforderlich sind, und der Datenexporteur stellt diese Informationen wiederum dem Verantwortlichen bereit.“

Klausel Transparenz M3 9c

„Auf Verlangen des Datenexporteurs oder des Verantwortlichen stellt der Datenimporteur eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.“

Eine Nachfrage zu Zoom X

Ausgangslage: EU-Standardvertragsklauseln werden mit Telekom abgeschlossen

Anfrage

- Kopien der Garantien für den internationalen Datentransfer der Unterauftragsverarbeiter von Zoom
- Das Data Transfer Impact Assessments (D)TIA für alle Empfängerländer außerhalb des EWR

Was kam?

- Die SCC von der „Telekom“ mit „Zoom“
- „Kurzfristig werden uns die vom Kunden geforderten Dokumente in keinem Fall zur Verfügung stehen, wenn überhaupt. Dazu wären Verhandlungen mit Zoom erforderlich, nach meinem Kenntnisstand sind die Beziehungen von Unterauftragnehmern zu deren Unterunterauftragnehmern nicht Teil des bei Zoom/Zoom X angewendeten internationalen Einkaufsprozesses. Bei der Ausschreibung des DFN in deren Rahmen hier der Vertragsschluss erfolgt, wurden solche Zusagen nicht vereinbart.

Und bis heute?

- Immerhin die SCC mit „AWS“

Wie weit kommt man, wenn man nach den Kopien der Garantien fragt?

Anbieter	AVV	Kopie der Garantien	TIA für Drittstaaten
Adobe	Verhandelbar, solide	Ja, aber …	Ja
Citavi	Geht so	Ja	Ja
Dropbox	Sportlich	Link zu EUR-Lex	Nein
Telekom (Zoom X)	Langweilig	Nach einem Jahr*	Nein
Microsoft	Umstritten	Teilweise, sonst nur Mustervertrag	Nein
Zoom	Verhandelt	Mustervertrag bzw. Links bei „Subs“	Über SURF

Fazit

Nicht immer Beraterinnen und Berater fragen, was man dürfte oder nicht.

Wägen Sie für sich selbst ab, über den Datenschutz hinaus, wenn man dem Anbieter vertraut, etwa

- Arbeitssicherheit
- Barrierefreiheit
- Digitale Souveränität
- Geheimnisschutz
- Haushaltsrecht
- Informationssicherheit
- Lizenz- und Patentrecht
- Mitbestimmung
- Nachhaltigkeit

Bonus - Vorschlag für Nutzungsregeln für Clouddienste

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.

Bonus - Vorschlag für eine Basisrisikoklassifikation Clouddienste

Dienste-klasse	I	II	III	IV	V
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 oder sind	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
Digitale Souveränität	Es besteht nur eine besonders geringe Abhängigkeit	Es besteht eine geringe Abhängigkeit vom Dienst	Es besteht eine gewisse Abhängigkeit	Es besteht eine relevante Abhängigkeit, parallel sollten Alternativen angeboten werden	Es besteht eine hohe Abhängigkeit, ein Ausstiegsplan ist erforderlich
Datenschutz	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
Informations-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 und Prozessen
Beispiel	Microsoft eigene Onlinebilder in Office einfügen Adobe Stock Bilder	Automatische Updates	Übersetzer in Microsoft Office, Dropbox jedoch mit vorab verschlüsselten Daten	Microsoft OneDrive, Zoom Cloudaufzeichung und Whiteboard	Automatisierung von Workflows mit PowerAutomate in Microsoft 365

Datenübermittlungen – Beispiel Microsoft

Region	Emissions ($mtCO_2e$)	% of total
EMEA	[redacted]	96.89%
France		1.6%
United States		<1%
Austria		<1%
Asia Pacific		<1%
United Kingdom		<1%
South Korea		<1%
Sweden		<1%
South Africa		<1%
Australia		<1%
Japan		<1%
Brazil		<1%
India		<1%
United Arab Emirates		<1%
Canada		<1%
Germany		<1%

Vielen Dank für Ihre Aufmerksamkeit!

Johannes Nehlsen

Tel.: 0931/31-84217

johannes.nehlsen@uni-wuerzburg.de
it-recht@digitalverbund.bayern

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

X/Mastodon/Bluesky: @JoNehlsen

Nehlsen – Big Tech - Vertragswerk zum Datenschutz vs. Realität