FH JOANNEUM
University of Applied Sciences

DSGVO, Google + Privacy: Verwenden Sie auch Google Dienste? Was sich bei IT-Dienstleister aus Drittstaaten (wie USA) zu beachten lohnt

DIHSÜD
Digital Innovation Hub

Johannes Feiner und Sabine Proßnegg
Fachhochschule JOANNEUM Kapfenberg

FFG Forschung wirkt.
Das Land Steiermark
LAND KÄRNTEN

30. November 2022

Bildquellen: Pexels / Pixabay https://www.pexels.com/search/microphone/

1

Kurze Einstiegsrunde

Vorstellung

Wissen / Erfahrung Datenschutz / IT

Erwartung(en) an den heutigen Vormittag

https://www.pexels.com/search/microphone/

FH | JOANNEUM
University of Applied Sciences

Zu uns

Sabine Proßnegg
Rechtswissenschaften (KFUG und Glasgow)

Mediatorin (ARGE Bildungsmanagement Wien)
Projektcoach (next level, Wien)

Johannes Feiner
TU Graz, Telematik

IICM/TU, HMS/JOANNEUM Research, Infonova
SWE, Mobile, UX

Disclaimer

Sämtliche Angaben und Aussagen in diesem Vortrag erfolgen trotz sorgfältiger Bearbeitung, Recherche und Kontrolle ohne Gewähr. Die Unterlage oder der Vortrag ersetzt keinesfalls eine rechtsfreundliche Beratung bei Ihren konkreten Fragestellungen.

Agenda

	Agenda	
09:00	**Einleitung**	JF
09:30	**Grundlagen DSGVO**	SP
10:00	*Pause*	
10:15	**Wo landen meine Daten**	JF
12:00	**Drittstaaten, USA und aktuelle Entscheidungen**	SP
12:40	**Sensible Daten sichern**	JF
12:55	**Zusammenfassung / Diskussion**	sp+jf
13:00	*Ende*	

Heute ist es das Cloud-Kapital, das seinen Besitzern unvorstellbare Macht verleiht.

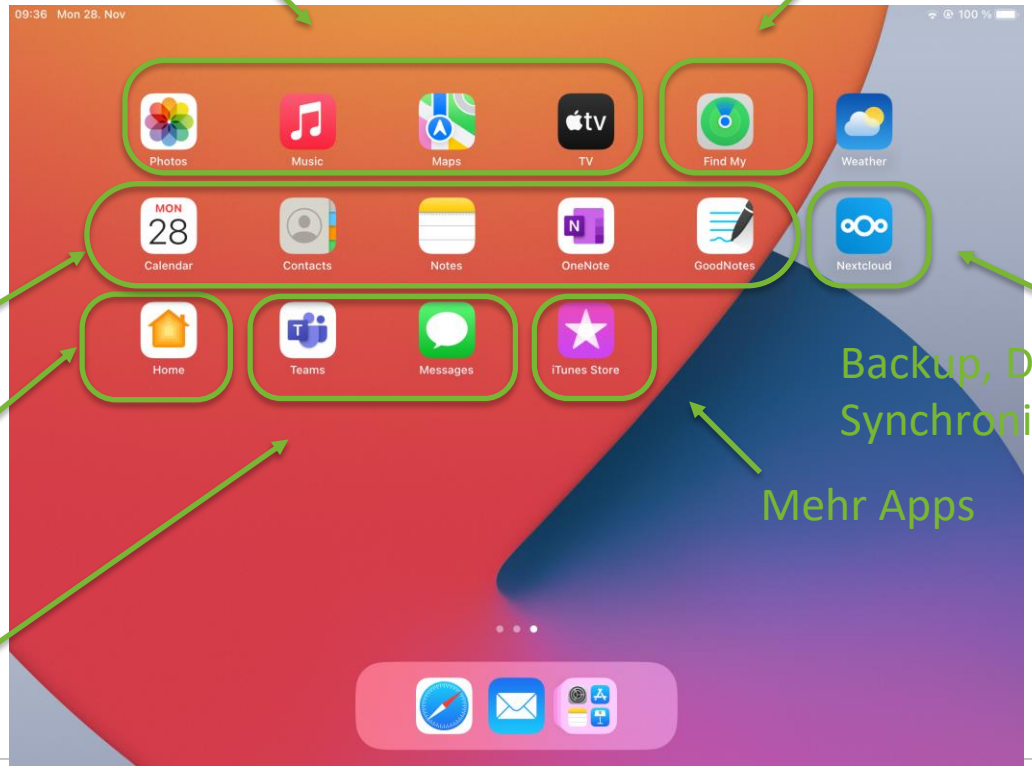
Yanis Varoufakis,
2022-11-20 DerStandard

Cloud Dienste

am Handy,
am Tablet

Bilder, Musik,
Karten, Streaming

Tracking



Backup, Daten
Synchronisation

Mehr Apps

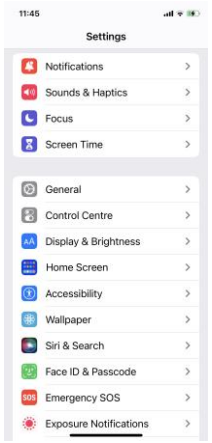
Kalender, Kontakte,
Notizen

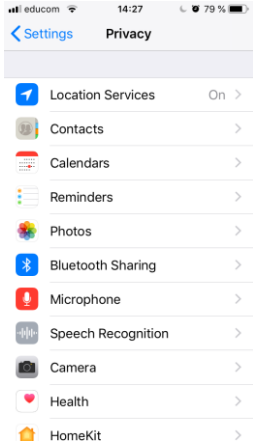
Fernwartung,
Heizung

(Video-)Chats

Cloud Dienste

am Handy



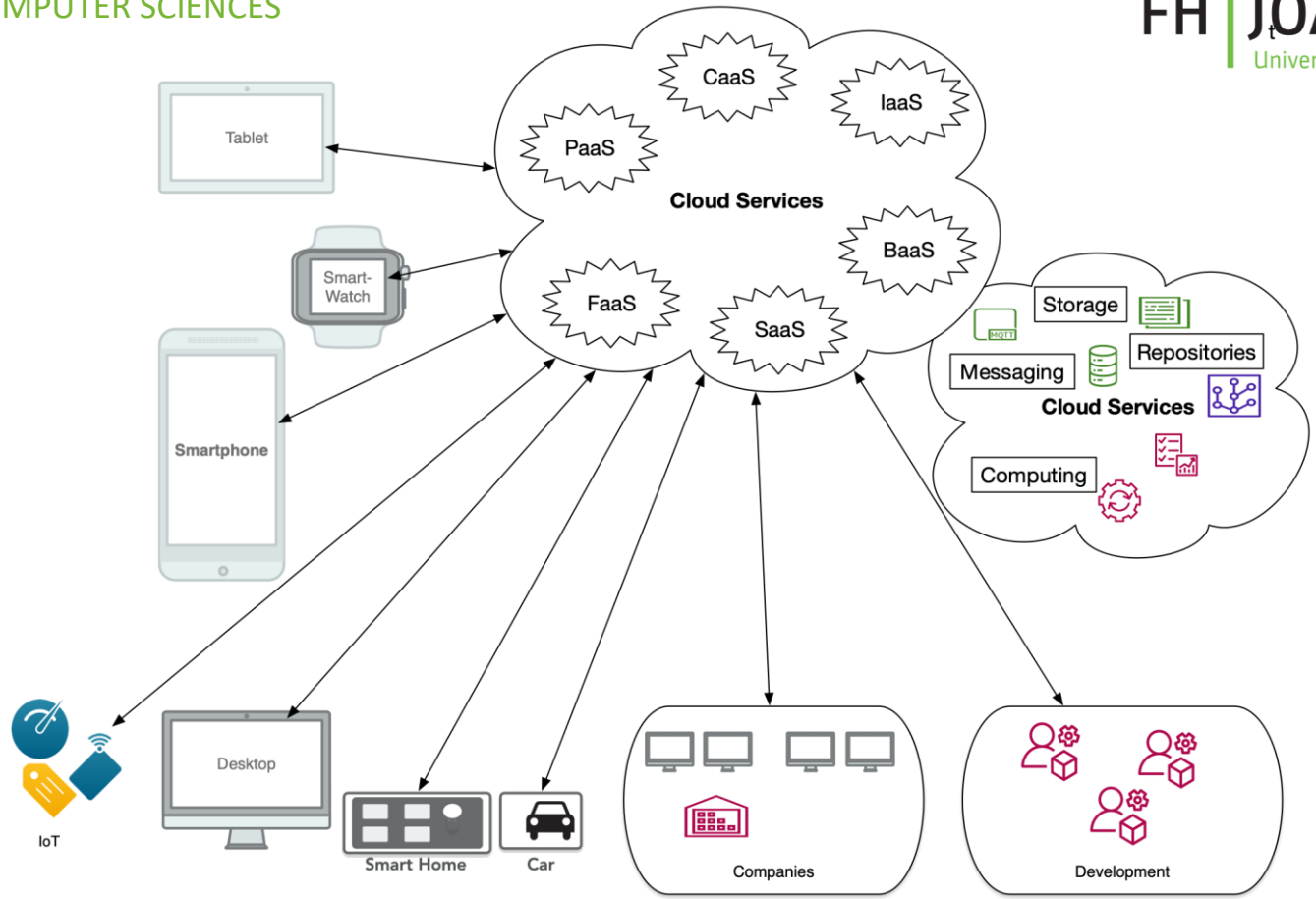


System Status

Available

App Store	Find My	iWork for iCloud
Apple Account Card	Game Center	Mac App Store
Apple Arcade	Global Service Exchange	macOS Software Update
Apple Books	Health sharing with provider	Mail Drop
Apple Business Essentials	HomeKit	Maps Display
Apple Business Manager	HomeKit Secure Video	Maps Routing & Navigation
Apple Card	iCloud Account & Sign In	Maps Search
Apple Cash	iCloud Backup	Maps Traffic
Apple Fitness+	iCloud Bookmarks & Tabs	News
Apple ID	iCloud Calendar	Photos
Apple Messages for Business	iCloud Contacts	Podcasts
Apple Music	iCloud Drive	Radio
Apple Music for Artists	iCloud Keychain	Schooltime
Apple Music radio	iCloud Mail	Schoolwork
Apple Music Subscriptions	iCloud Notes	Screen Time
Apple Online Store	iCloud Private Relay	Sign in with Apple
Apple Pay & Wallet	iCloud Reminders	Siri
Apple School Manager	iCloud Storage Upgrades	Spotlight suggestions
Apple TV Channels	iCloud Web Apps (iCloud.com)	Stocks
Apple TV+	iMessage	Volume Purchase Program
AppleCare on Device	iOS Device Activation	Walkie-Talkie
Device Enrollment Program	iTunes Match	Weather
Dictation	iTunes Store	
FaceTime	iWork Collaboration	

https://www.apple.com/support/systemstatus/


Tablet
Smart-
Watch
Smartphone
CaaS
IaaS
PaaS
Cloud Services
BaaS
FaaS
SaaS
Storage
Repositories
Messaging
Cloud Services
Computing
IoT
Desktop
Smart Home
Car
Companies
Development

Cloud Dienste

im Web

Suche

Gmail

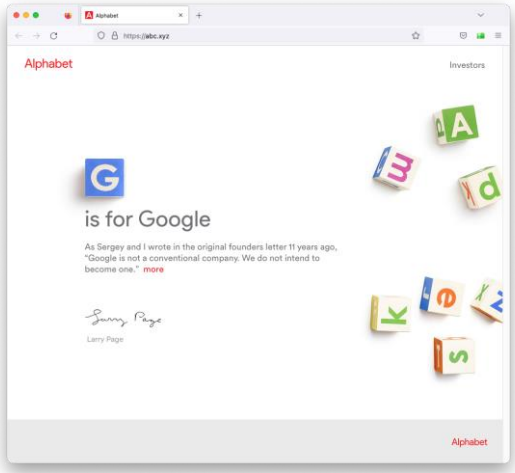
Maps

Photos

Google Docs

Chrome Browser

Beispiel Alphabet



Google Ads

Android

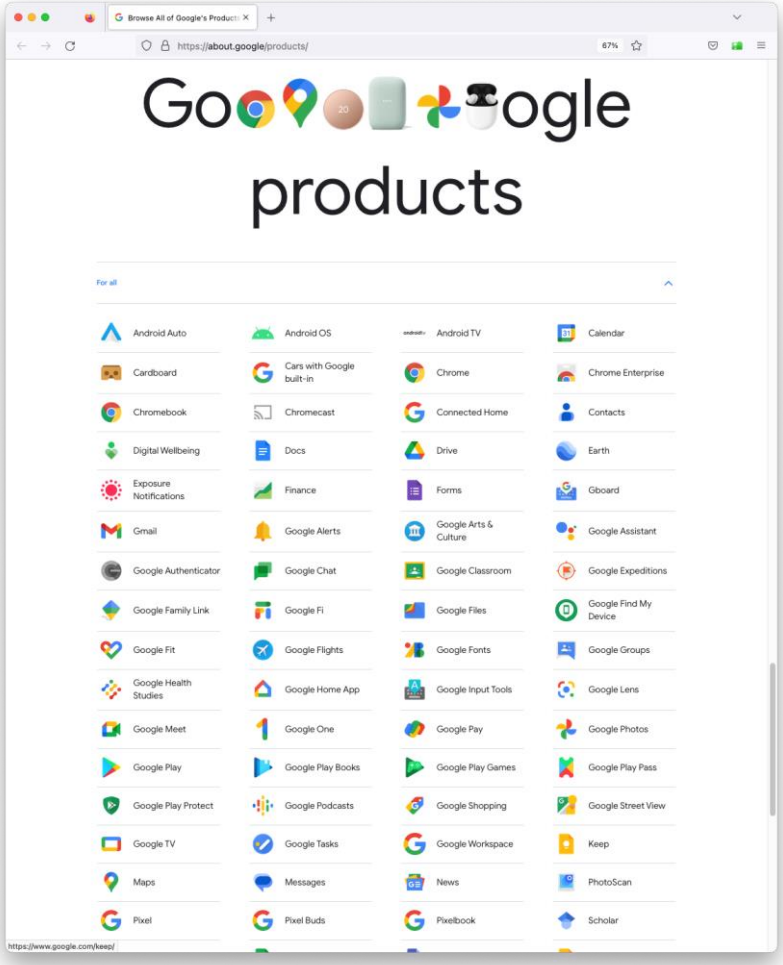
+ 250 Firmen gekauft:
Keyhole, YouTube,
DoubleClick, VirusTotal,
Kaggle, ...Fitbit

https://en.wikipedia.org/wiki/List_of_Google_products

Cloud Dienste

"Google weiß mehr über mich als meine Freundin"

Benedikt Fuest
(welt.de Google Selbstversuch), 2014



https://about.google/products/#all-products

Cloud Dienste

Zeitliche Nutzung

Average daily social media use via any device in selected European countries during the 3rd quarter of 2020 (in minutes)

https://www.statista.com/statistics/719966/average-daily-social-media-use-in-selected-european-countries/

Number of hours spent per day using apps worldwide from 2019 to 2021, by country

https://www.statista.com/statistics/1269704/time-spent-mobile-apps-worldwide/

Website and online service usage by type in Austria in 2022

https://www.statista.com/forecasts/1001336/website-and-online-service-usage-by-type-in-austria

Cloud service usage in Austria in 2022

https://www.statista.com/forecasts/1001229/cloud-service-usage-in-austria

Cloud Dienste mit unserer Zustimmung

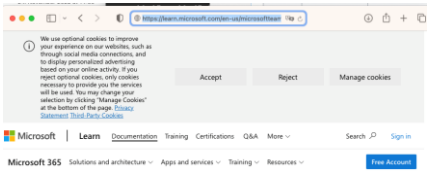
Länge?

Terminologie?

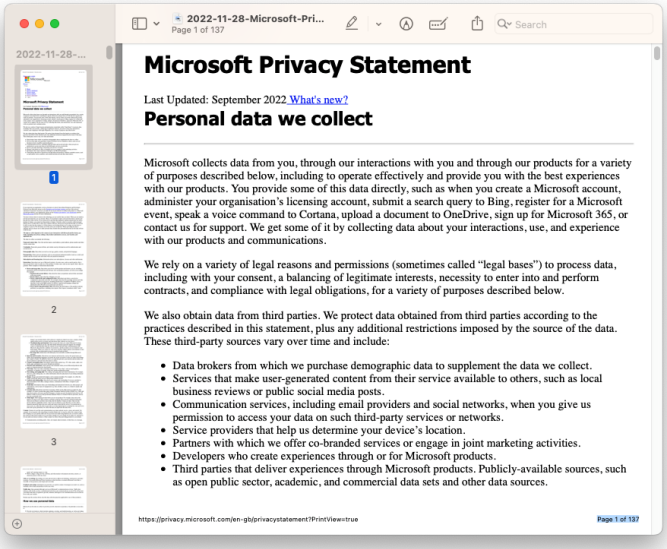
Lesbarkeit?

...

Gerichtsstand?

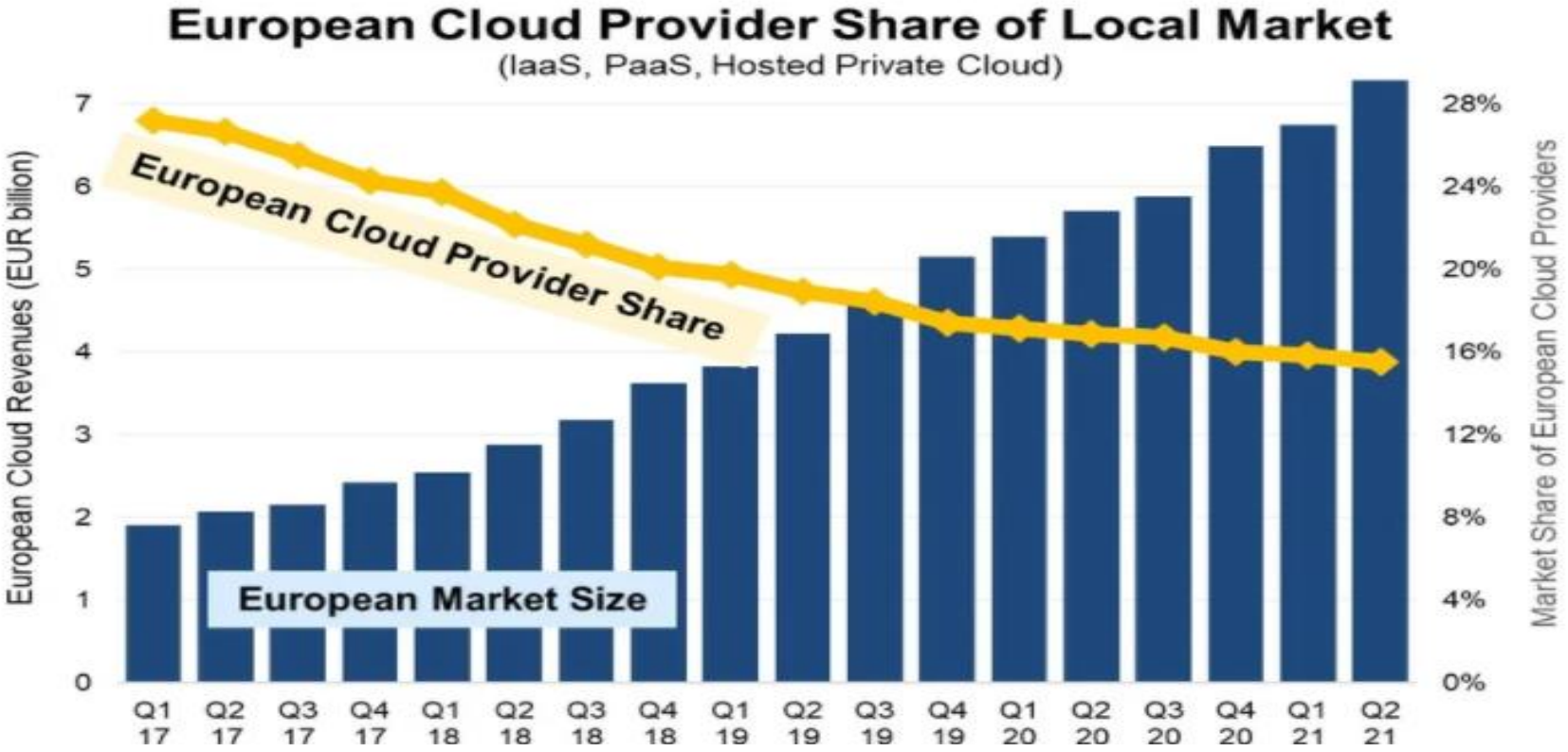


Microsoft Privacy Statement



https://learn.microsoft.com/en-us/microsoftteams/teams-add-on-licensing/microsoft-teams-add-on-licensing

The main beneficiaries of the cloud market growth in Europe have been Amazon Web Services, Microsoft Azure and Google Cloud. These three leading global cloud providers now account for 69% of the regional market, and their share continues to rise.



European cloud providers take hit from AWS, Google, Azure, says Synergy | Fierce Telecom*on Cloud Services and Infrastructure | Synergy Research Group (srgresearch.com), 16.03.2022.*

Datenschutzrecht Grundlagen

Agenda

VO (EU) 2016/679 des EP und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbez. Daten […] (Datenschutz-Grundverordnung)

Datenschutzgesetz 2000 (DSG)

Der Strafrahmen hat sich deutlich verändert:

bis € 25.000 -> bis zu €10 Mio./20 Mio. oder 2%/4% des weltweiten Umsatzes

Bildnachweis: https://www.pexels.com

Grundsatz der Datenverarbeitung DSGVO / Main Principles of the GDPR

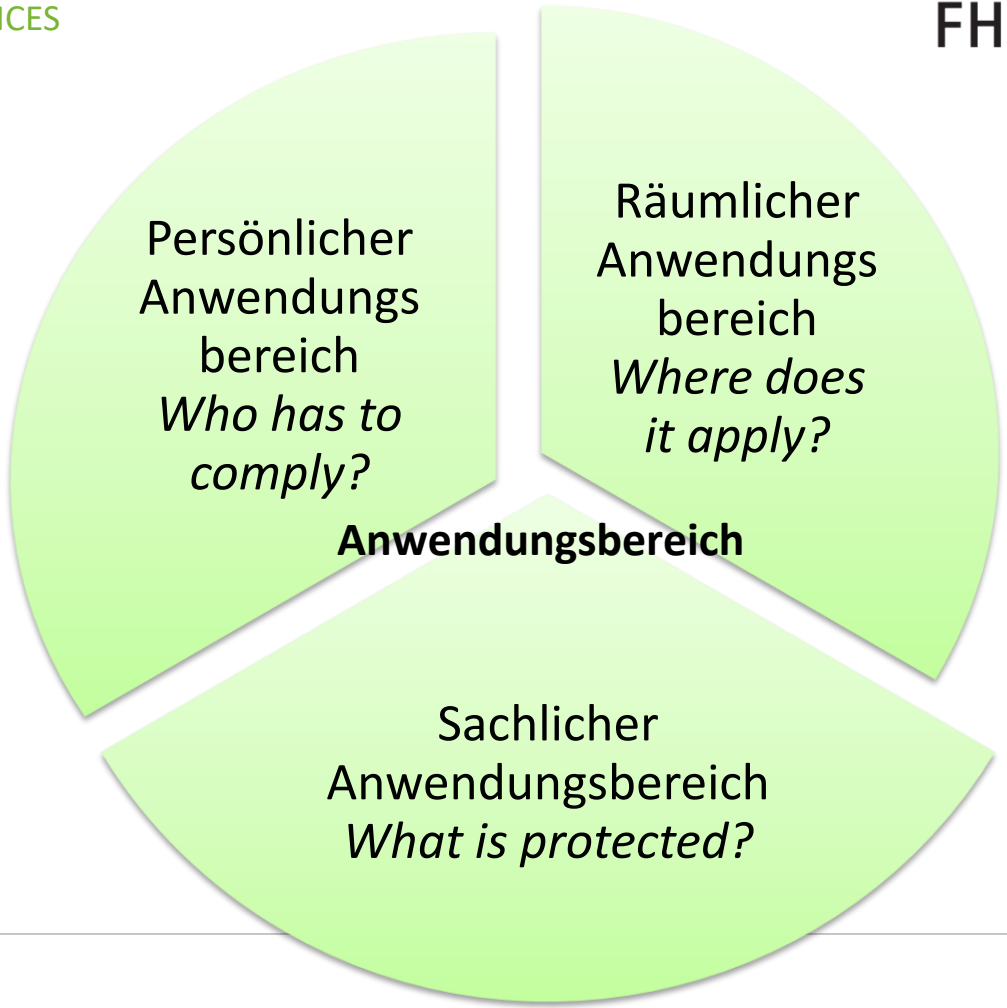
Pixabay.com

Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten.

Verbot mit Erlaubnisvorbehalt.

- ✓ **Informationelle Selbstbestimmung: wo gebe ich wem und wofür meine personenbezogenen Daten?**
- ✓ **Teil meiner Grundrechte**
- ✓ **Datenschutzrechtlich ok zB Corona App, aber Rechtstaatlichkeit allgemein?**

17

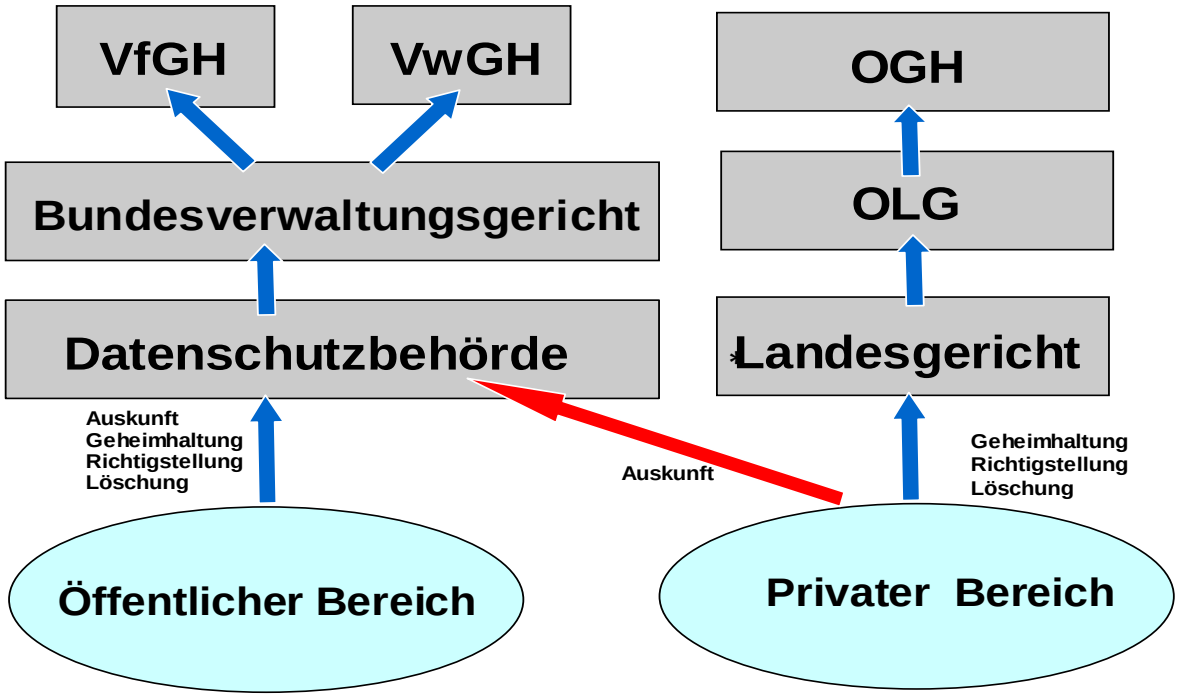

Persönlicher Anwendungs bereich
Who has to comply?
Räumlicher Anwendungs bereich
Where does it apply?
Anwendungsbereich
Sachlicher Anwendungsbereich
What is protected?

18

Grundsätze der Datenverarbeitung Art 5 DSGVO

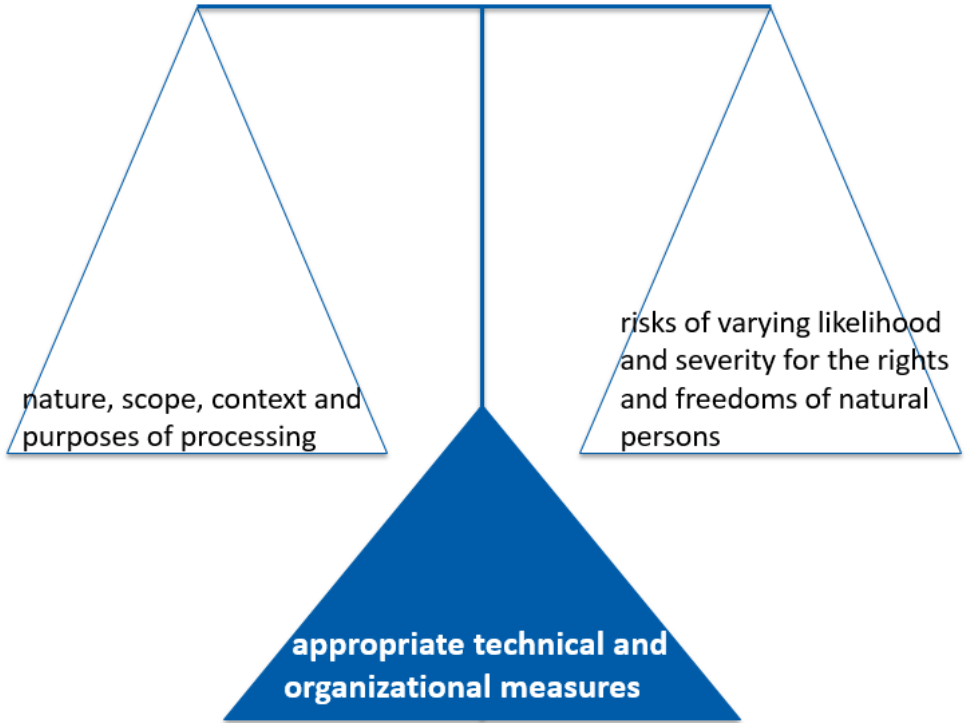
Grundsätze der Datenverarbeitung Art 5 DSGVO

Rechtsschutz nach dem DSG

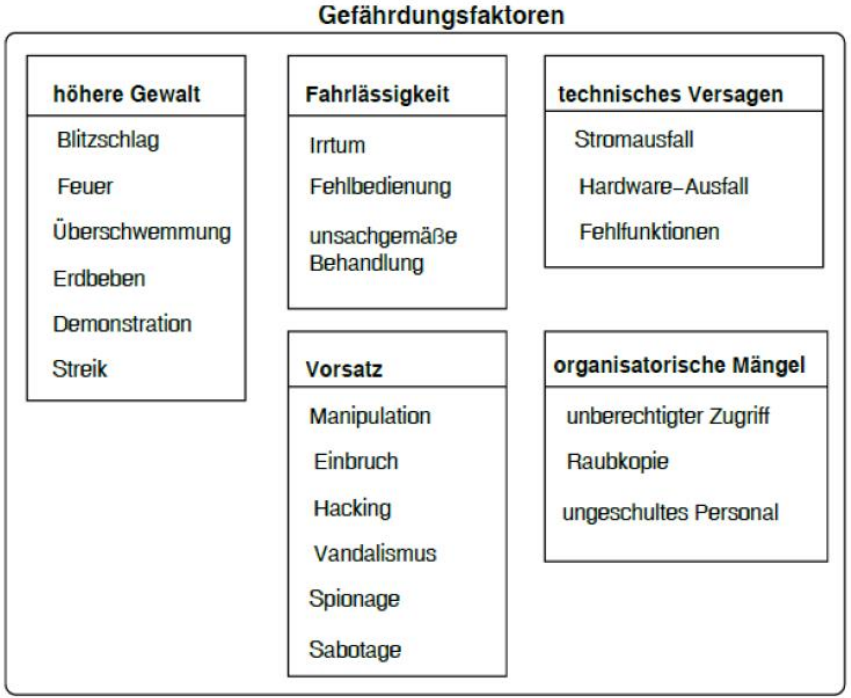


Darstellung: Prof. Jahnel

Art 24 DSGVO

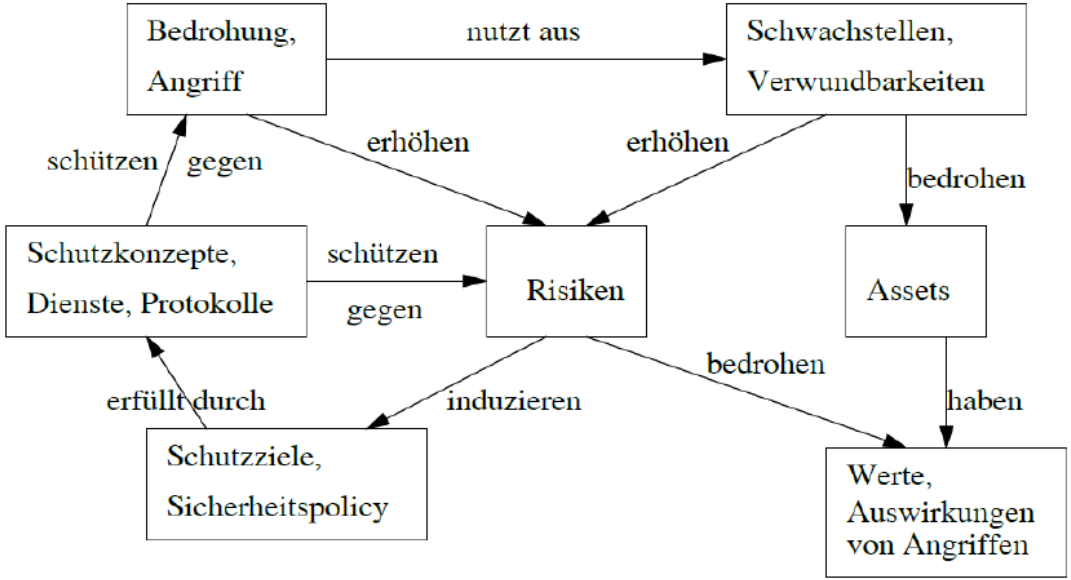

nature, scope, context and purposes of processing
risks of varying likelihood and severity for the rights and freedoms of natural persons
appropriate technical and organizational measures

Datensicherheit



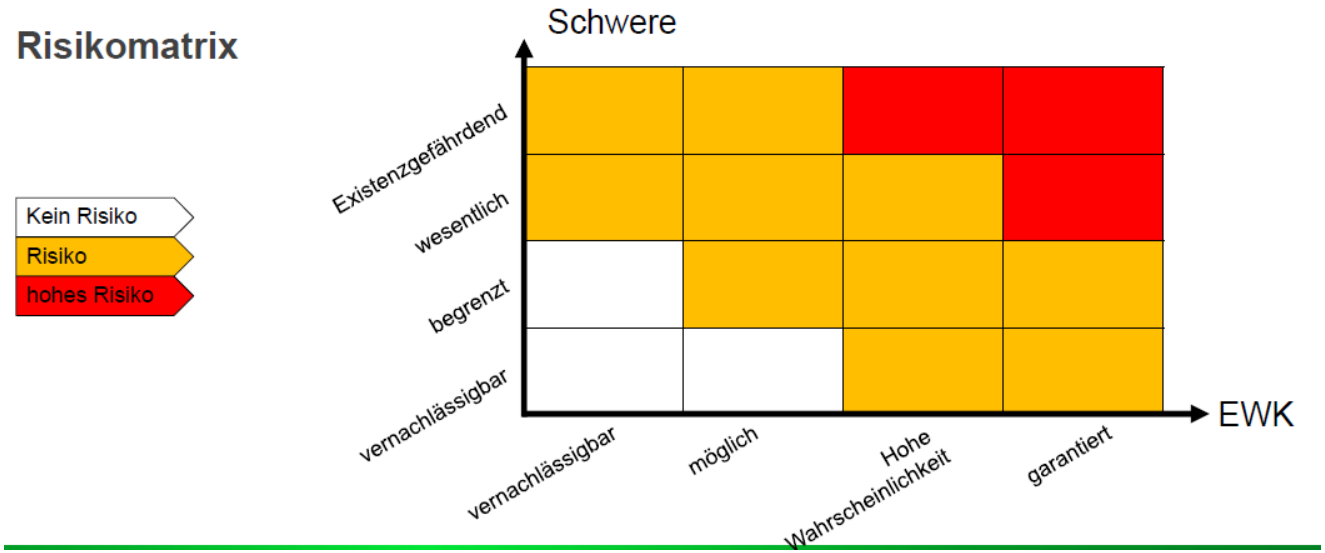
Eckert, Claudia (2013). IT-Sicherheit: Konzepte - Verfahren - Protokolle. Munich: Oldenbourg Verlag München. ISBN: 978-3-486-72138-6.

Datensicherheit / Risikoanalyse

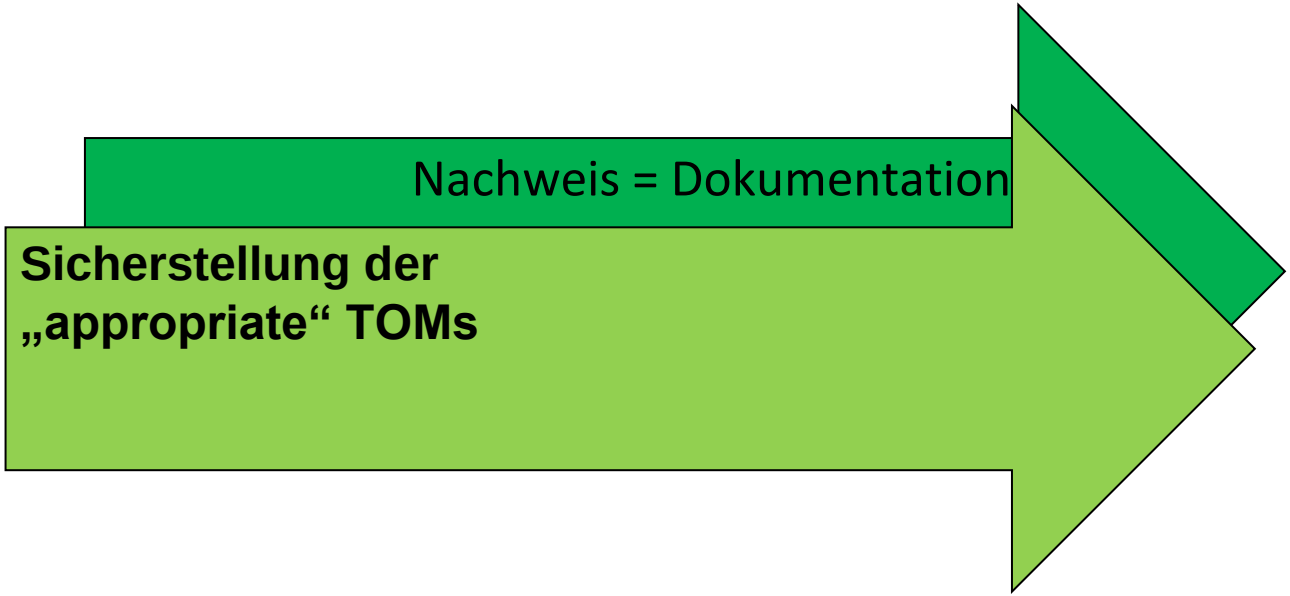


Eckert, Claudia (2013). IT-Sicherheit: Konzepte - Verfahren - Protokolle. Munich: Oldenbourg Verlag München. ISBN: 978-3-486-72138-6.

Risikomanagement



Art 24 ff DSGVO



Wo sind die Daten?

Unternehmen

TOMs

Auftragsverarbeitervertrag

Betroffenenrechte

Verantwortlicher

„Herr der Daten“

Betroffener

Auftrags-
verarbeiter

Vgl. Dohr/Pollirer/Weiss/Knyrim, DSG Kommentar

Google

Persönlichkeitsrechte – relative Rechte

Schutzwürdigkeit von Daten:

PERSONENBEZOGEN

Besondere Kategorie von Daten
strafrechtlich relevant
indirekt personenbezogen

ÖFFENTLICHE Daten
ANONYM / AGGREGIERT

hoch

SCHUTZWÜRDIGKEIT

niedrig

Umsetzung des DSR in ihrem Unternehmen

Recht – Organisation – Prozeß – IT

⇒Datenschutzcompliance Programm bzw Datenschutzstrategie

⇒ Privacy by Design und Privacy by Default

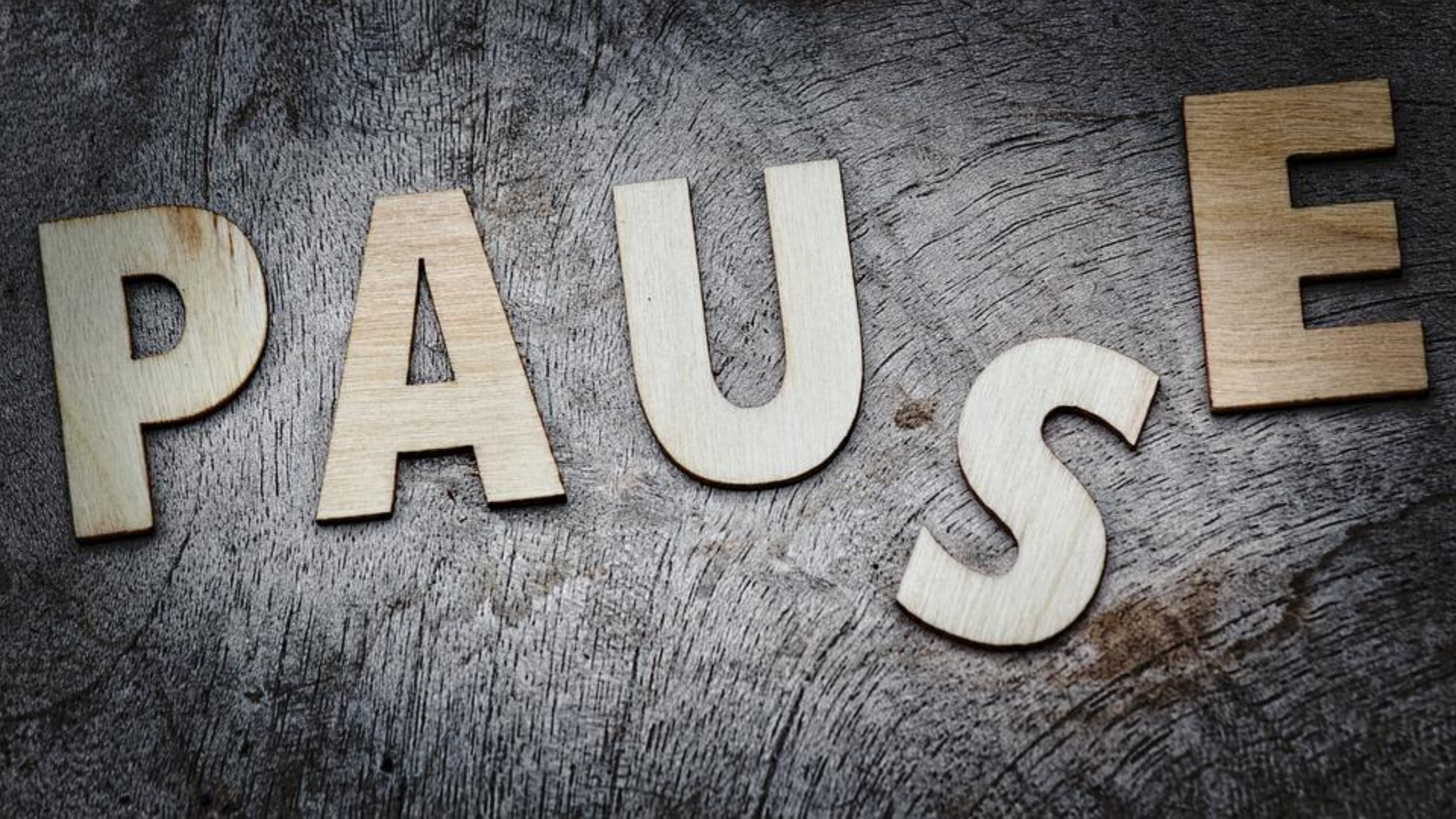
⇒ Führung eines Verarbeitungsverzeichnisses Art 30 DSGVO

⇒ ev. Datenschutzbeauftragter

⇒ umfassendes Datenschutzmanagement

Kein wenn dann, sonder je .. desto

⇒Angemessenheit, Risikoabwägung …


PAUSE

Agenda

Wo landen meine Daten?

„Sensible Daten“

"Ich habe ja Nichts zu verbergen"

Das stimmt hoffentlich nicht!

Ärztin / Krankheiten der Kinder,
Verdienst und Geld €,
24h Überwachung, Hobbies,...

"Ich habe ja Nichts zu verbergen"

Lesung der Chatprotokolle am Burgtheater

https://dietagespresse.com/regierungskrach-der-whatsapp-chat-zwischen-kurz-und-strache/

https://www.youtube.com/watch?v=jyof-WQQN58

"Ich habe ja Nichts zu verbergen"

Könnte aber Leben retten

Bradley Manning
deckt Angriffe von Drohnenpiloten im Irak auf
(vgl. WikiLeaks / Glenn Greenwald)
https://www.salon.com/2010/06/18/wikileaks_3/

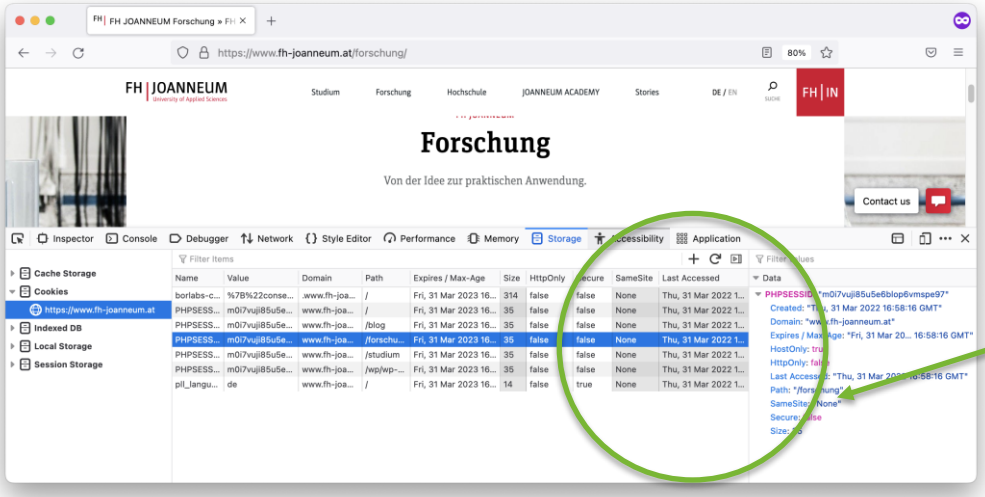
Tracking

Übertragung

Speichern (Datensenken)

Was bring Verschlüsselung? (https, SSL, TSL... end-to-end

FH | JOANNEUM
University of Applied Sciences



Typische FHJ Webpage

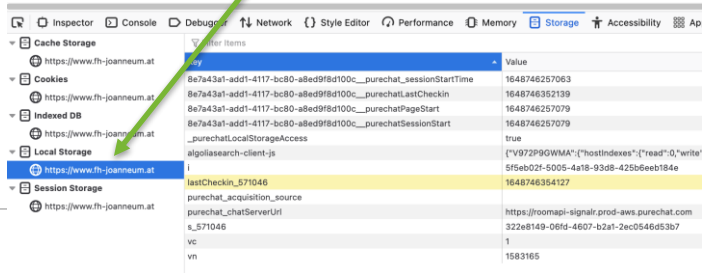
Verwendet auch bei Einstellung
"nur essentielle Cookies"
eher "suboptimale" Einstellungen...

...und weites viele, viele Daten (im LocalStorage).

https://www.fh-joanneum.at/forschung

Erklärung zu Cookies:

- **HttpOnly**: wenn *true*, dann dürfen Cookies nicht im Hintergrund (über JavaScript/AJAX) weitergesendet werden
- **Secure**: HTTPS muss verwendet werden (verschlüsselte Verbindungen)
- **SameSite**: wenn nicht "strict" angegeben wurde, dürfen Cookies *überallhin* (3rd Party Cloud Servers) gesendet werden



Try it out

https://feine.yaka.fh-joanneum.at/

1 Cookies → 2 Fingerprinting →

Try it out

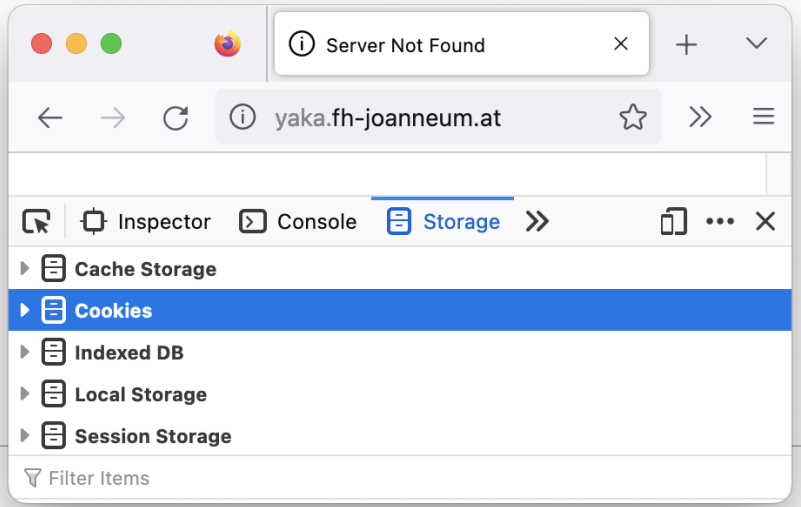
1 Check

Firefox

Cookies

... visit page again

https://feine.yaka.fh-joanneum.at/



Try it out

2 Fingerprinting

🐾 🐾 🐾 🐾

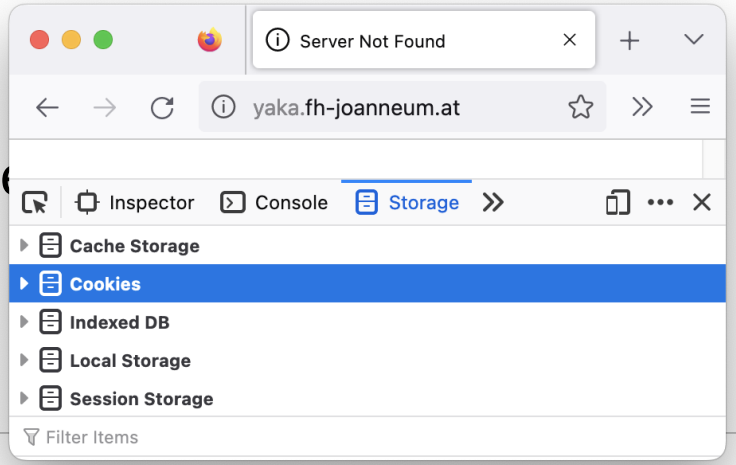
Tracking

without Cookie

... visit page

again

https://feine.yaka.fh-joanneum.at/



Bequemlichkeit vs. Privatsphäre

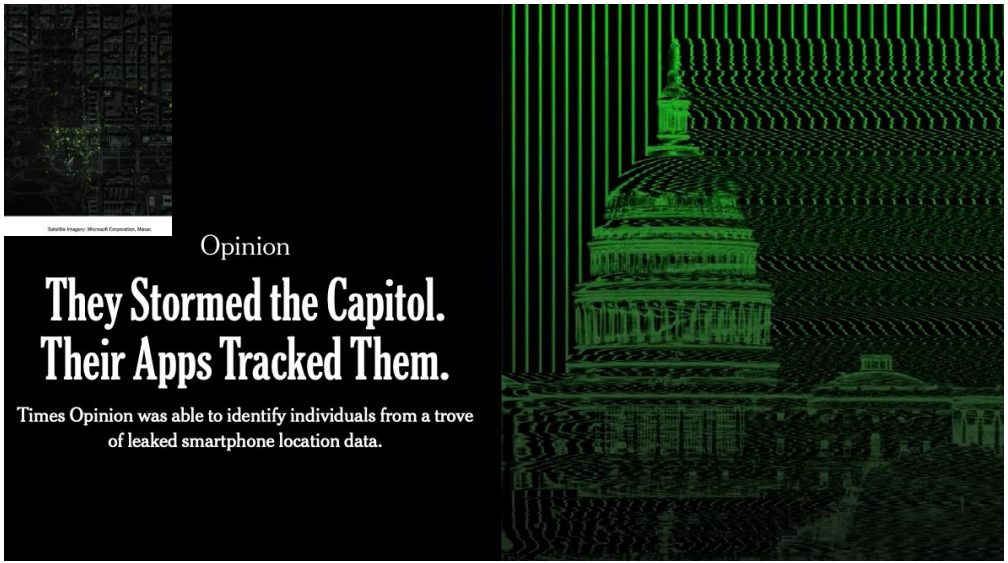
Tracking - Extrembeispiel

China: Vergehen (bei Rot über die Kreuzung) haben soziale Auswirkungen auf das Leben (Punkte Kreditwürdigkeit, Versicherung)

Google Maps: Routing Info inkludiert genaue Position anderer Google User

Versuche: NSA (Snowden), ... aber auch Apple "Bilder Filter" gegen Mißbrauch

Kapitolstürmer: zurückverfolgt durch Apps



Opinion

They Stormed the Capitol. Their Apps Tracked Them.

Times Opinion was able to identify individuals from a trove of leaked smartphone location data.

How "Anonymous" Pings Could Be Identifiable

The "anonymous" mobile advertising ID can be matched across databases ...

MARKETING DATABASE	APP DATABASE	ANONYMOUS LOCATION DATABASE
First name	Phone number	**Mobile Ad ID**
Last name	**Mobile Ad ID**	Precise location
Home address	Email address	Date
Mobile Ad ID	App name	Time

... creating a new deanonymized database

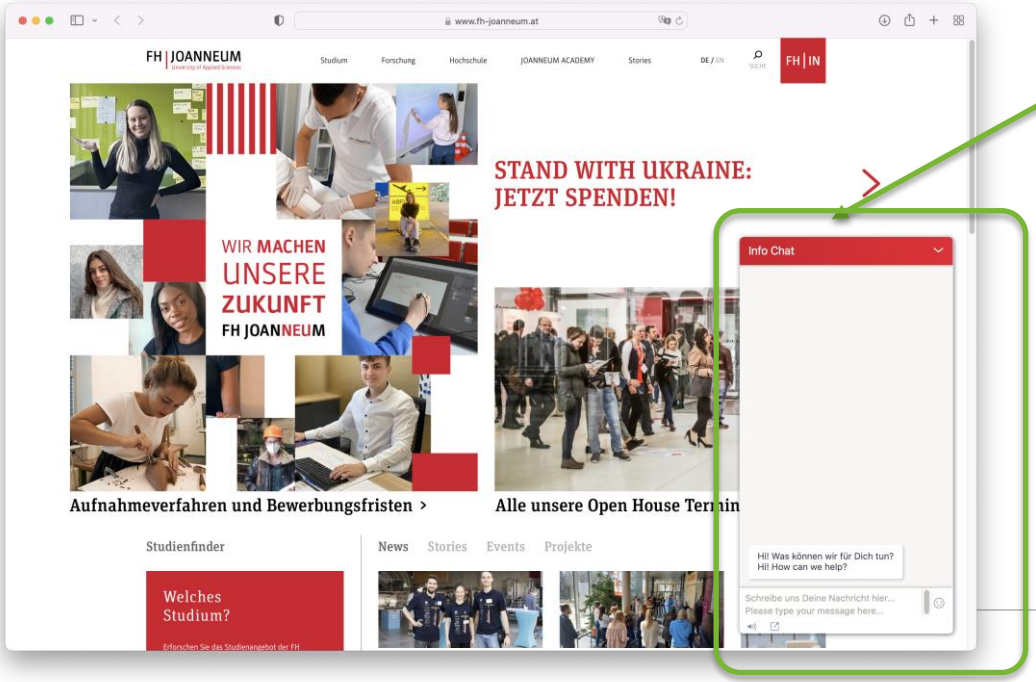
NEW DATABASE
Mobile Ad ID
First name
Last name
Home address
Phone number
Email address
App name
Precise location
Date
Time

By The New York Times

https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html

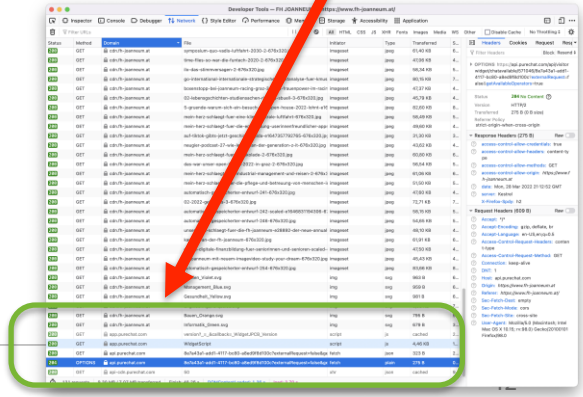
FH | JOANNEUM
University of Applied Sciences

Tracking - Minimalbeispiel



Chatbot

Problem: Sendet alle paar Sekunden zu purechat.com



Bekannte "Datensenken"

Fonts

https://fonts.googleapis.com

Javascript libs, (web-)fonts

https://fonts.gstatic.com

Web-fonts, stylesheets

https://use.fontawesom.com

Cloudflare - CDN Content Distribution Network

IP .... Lookup on Map: Brasil

188.114.97.20:443

https://www.ip2location.com/demo/188.114.97.20:443

FH | JOANNEUM
University of Applied Sciences

Bequemlichkeit vs. Privatsphäre

Tracking - Minimalbeispiel

Server Logs

Ein Click im Browser

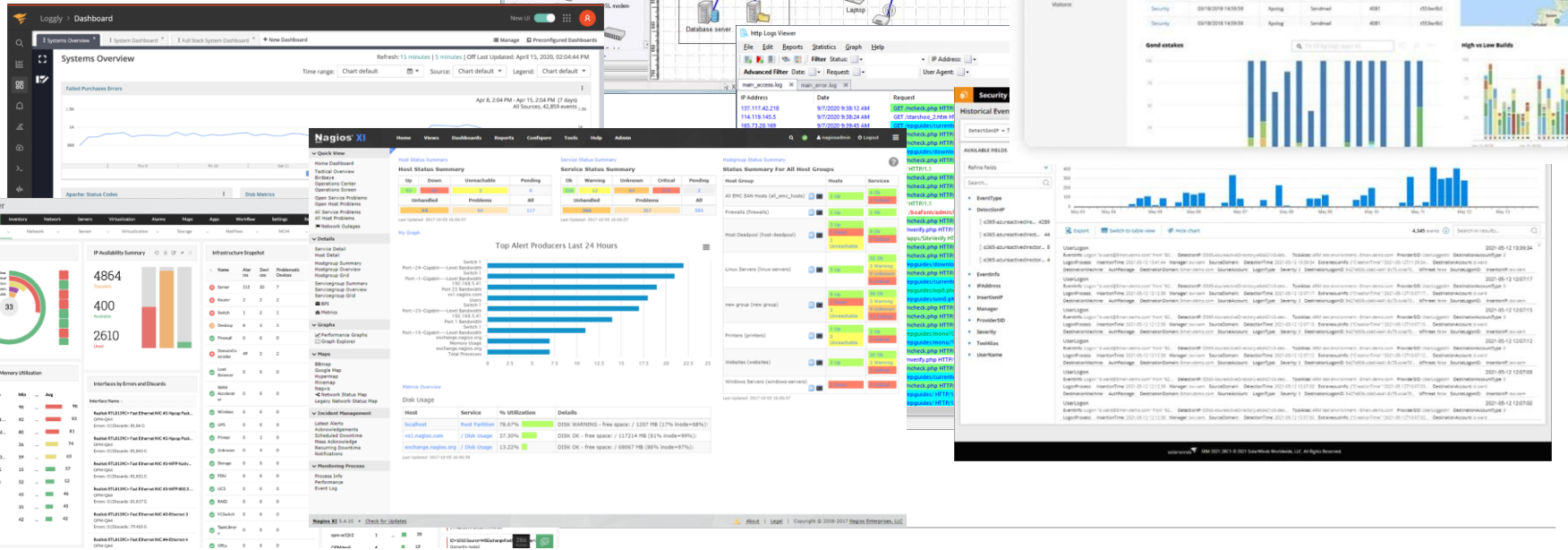
Problem: Typischerweise gespeicherte Details:

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html" "Mozilla/4.08 [en] (Win98; I ;Nav)"
```

start... "http://www.example.com/start.html"

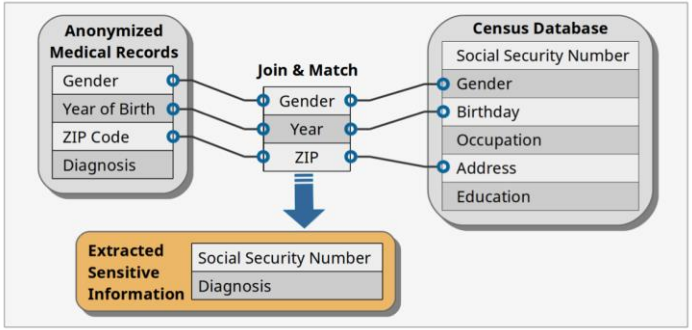
https://httpd.apache.org/docs/current/logs.html

Log-Daten Auswertungen



https://www.dnsstuff.com/apache-log-analyzer-tools

Sensible Daten



Was ist sensibel

Kombination v. Datenbanken

Was "hilft" beim Tracken? Z.B. IP, Device ID, Tracking ID, Google Fonts, Fingerprinting

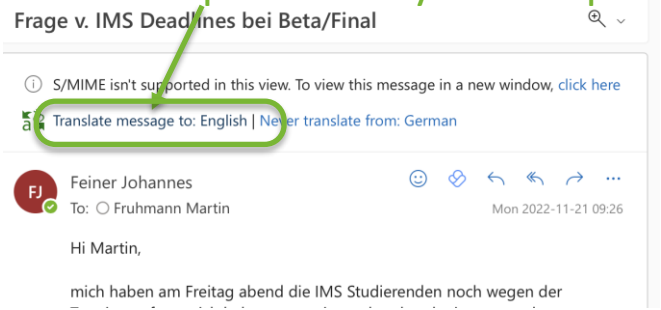
Bequemlichkeit vs. Privatsphäre

Datenanalyse - Aktuelle Beispiele

Beispiel MS Office 365

Mein "Verhalten"
+ Daten der Mail
+ Termine
+ ...

Bequem: Analyse der Sprache



Problem: Jemand liest alle deine Mails!

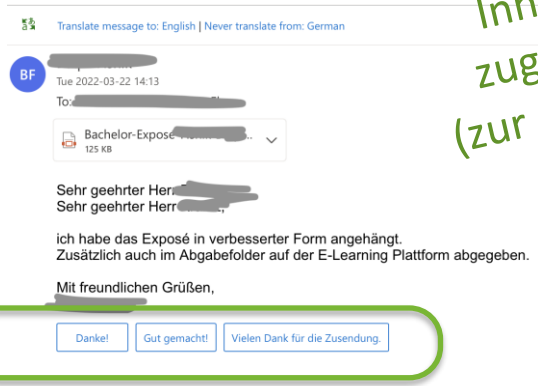
Beispiel Mail

Vorschläge in Office 365

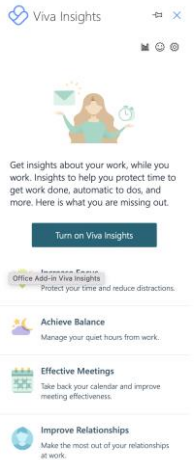
Mit ML
Sentiment - Analysis
(Stimmung)

Mit ML
Textanalyse (Sprache)

Inhaltsanalyse:
zugehörige Mails
(zur Kontakt-Person)



Die Mail-Antworten werden vorgeschlagen

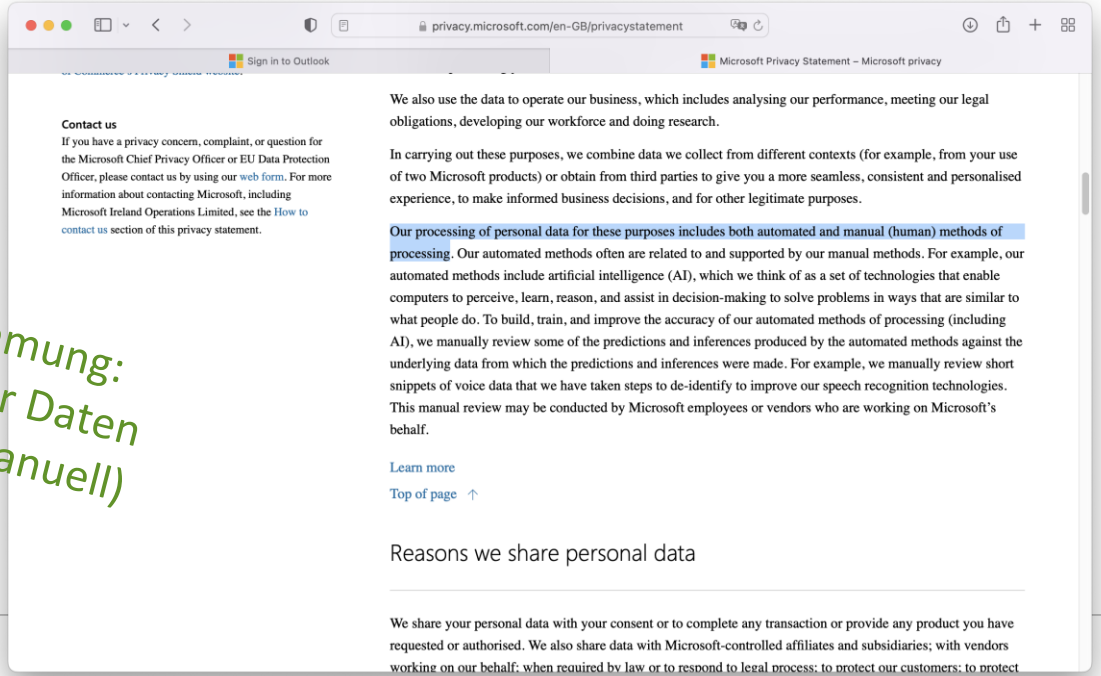


Optional sind
"Viva Insights"
aktivierbar

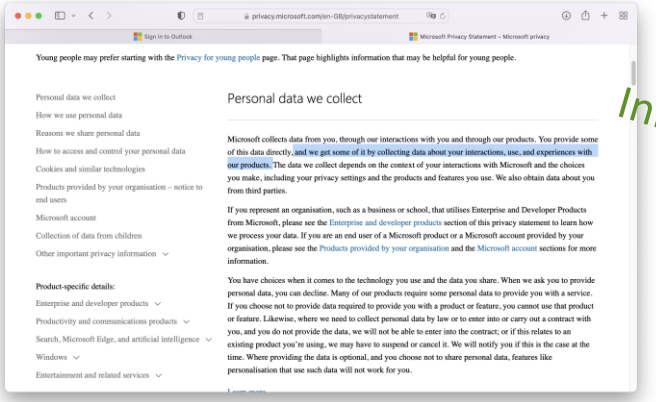
Default: "Productivity inline suggestions" waren eingeschalten.

Vermutlich haben wir zugestimmt....

Lizenzbestimmung:
Verwertung der Daten
(AI und/oder manuell)



Vermutlich haben wir zugestimmt....



Datenverknüpfung:
Inkludiert auch Daten externer (3rd Party) Dienste

Zentrale Speicherung und Verarbeitung (möglicherweise in den USA)

Try it out

https://feine.yaka.fh-joanneum.at/A

https://feine.yaka.fh-joanneum.at/B

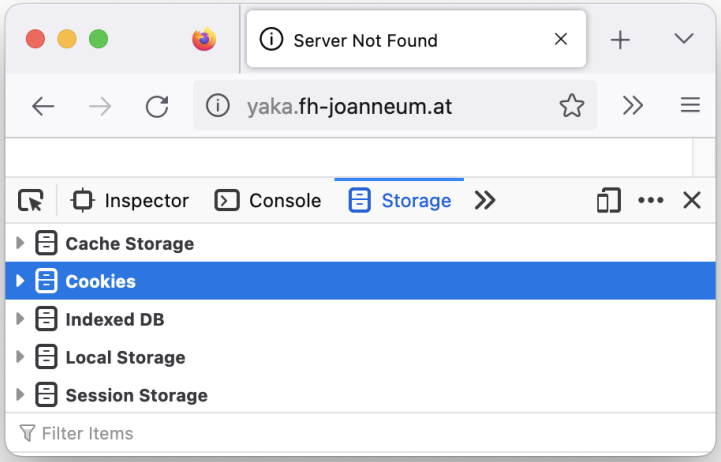
https://feine.yaka.fh-joanneum.at/C

1 Enter data in A,
2 then enter data in B.
3 Visit C to see combined data from A and B

Try it out

1 Enter Data at "A"

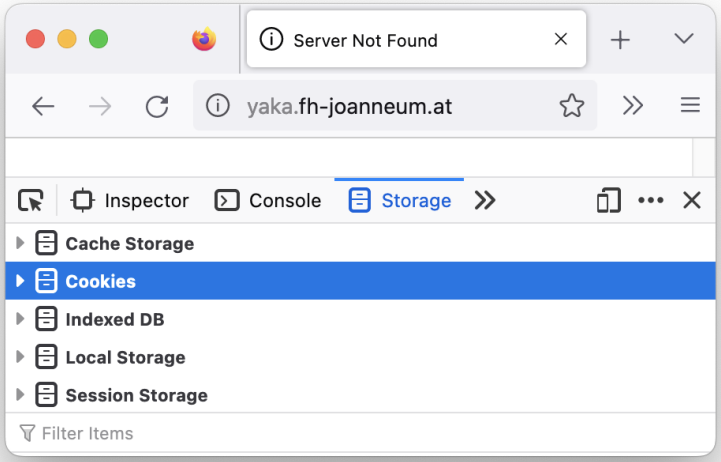
https://feine.yaka.fh-joanneum.at/A



Try it out

2 Enter Data at "B"

https://feine.yaka.fh-joanneum.at/B

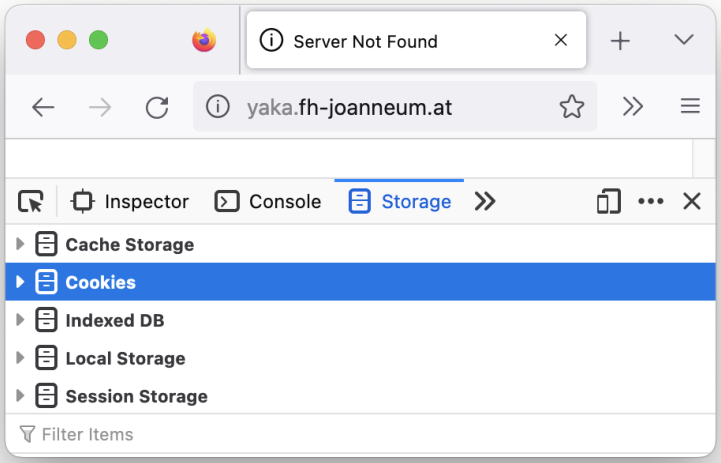


Try it out

3 Combined

Data at "C"

https://feine.yaka.fh-joanneum.at/A

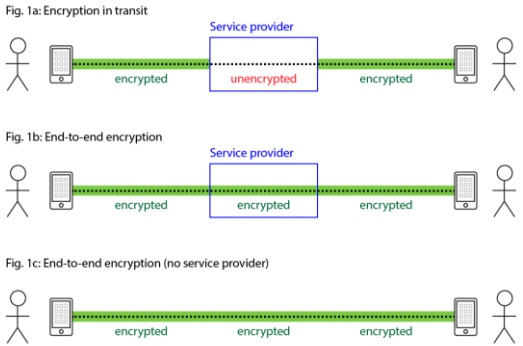


Sensible Daten in der Cloud schützen

Daten (auch Backups) verschlüsseln

Achtung:

Nur End-To-En



Beispiel:
Instant Messages

https://heimdalsecurity.com/blog/wp-content/uploads/data-stored-in-instant-messages.png

Exkurs: Snowden und die NSA

Vor Snowden:

Gerüchte
(Verschwörungstheorie)

Nach Snowden:

Es ist real
(und schlimmer als erwartet)

Update:
Viele Daten = Bessere Algorithmen
(Machine Learning)

Agenda

Drittstaatentransfer

USA

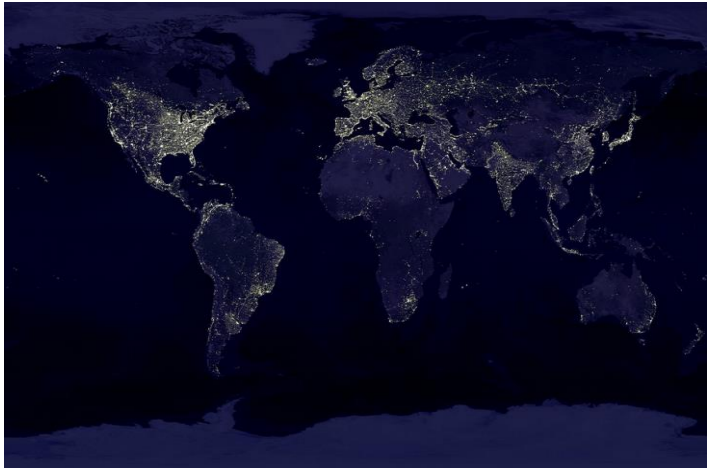
Problemstellung

Integrität und Vertraulichkeit 5 Abs 1 DSGVO

NEUM
of Applied Sciences

Bei Transfer in Drittstaaten:

- Risiko steigt
- Kontrollverlust



Häufige Anwendungsfälle:

Cloud Computing,

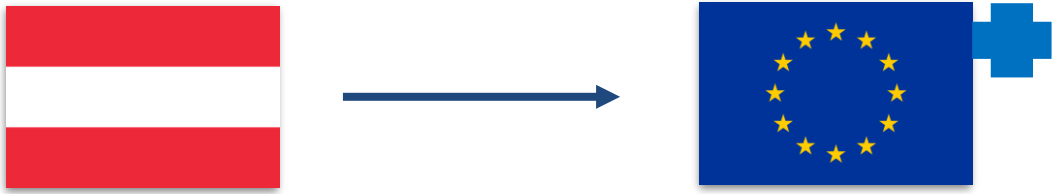
gängige Programme wie Microsoft- Teams, Google, WhatsApp, Zoom …

Datentransfer innerhalb eines Konzerns

59

Datentransfer innerhalb der EU+

- Grundsätzlich keine Einschränkungen
- Sofern DSGVO eingehalten wird
- inklusive **Norwegen, Island, Liechtenstein** (EWR)
- Rechtlich gleichgestellt mit Datentransfer im Inland



Datentransfer in Drittstaaten Art 44ff DSGVO

- **Kapitel V** (Art. 44 bis 50) DSGVO; vormals Kapitel IV RL 95/46EG
- Art. 44 DSGVO als Grundnorm des IDVK:

„Jedwede ***Übermittlung personenbezogener Daten****, […] an ein Drittland oder eine internationale Organisation […] ist* ***nur zulässig****, wenn der Verantwortliche und der Auftragsverarbeiter* ***die in diesem Kapitel niedergelegten Bedingungen*** *einhalten und auch die* ***sonstigen Bestimmungen*** *dieser Verordnung eingehalten werden; dies gilt auch für die etwaige* ***Weiterübermittlung*** *personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation.* ***Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird****.“*

61

Datentransfer außerhalb der EU+

- Sorgfalt bei der Auswahl des Auftragsverarbeiters
- Sicherheitsvorkehrungen und Nachweise
- Provider hat die Pflichten eines Auftragsverarbeiters gem Art 28f DSGVO (Vertrag)
- darf Daten nicht für eigene Zwecke verwenden und
- muss Mindestanforderungen an Datensicherheit erfüllen gem Art 32 DSGVO
- **Angemessenes Schutzniveau**, Einhaltung der Vorgaben **Art 44-50 DSGVO ->** Haftung / Betroffenenrechte

- **WIE?**

Datentransfer in Drittstaaten

- **Rechtsgrundlagen für Datenübermittlungen**
  - Art. 45 → **Angemessenheitsbeschluss** der EK (partiell/vollumfänglich)
  - Art. 46 → **Geeignete Garantien**
    Standarddatenschutzklauseln
    Verbindliche interne Datenschutzvorschriften
    Verhaltensregeln (Codes of Conduct), Zertifizierungen
    weitere
  - Art. 49 → **Ausnahmen** für bestimmte Fälle
    restriktive Auslegung (Leitlinien 2/2018 des EDPB)

Datentransfer in Drittstaaten

Datenübermittlungen auf der Grundlage eines **Angemessenheitsbeschluss der Kommission (Art 45 DSGVO)** bedürfen keiner besonderen Genehmigung durch die Aufsichtsbehörde.

- Mechanismus für eine regelmäßige Überprüfung, die mindestens alle 4 Jahre zu erfolgen hat.

derzeit die Staaten **Andorra, Argentinien, Färöer Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay, Japan, Südkorea,**

UK

~~**USA**~~

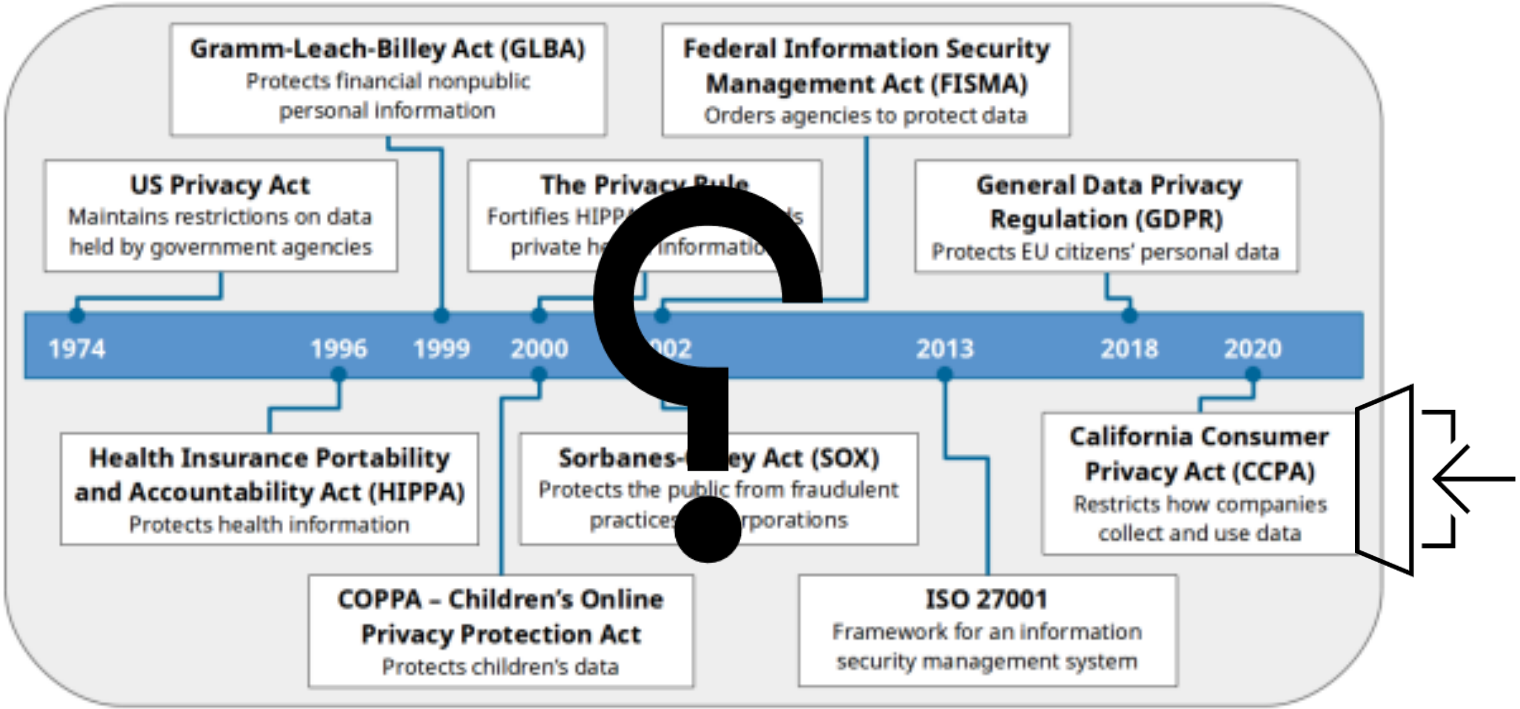
https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

Exkurs: Take a Guess where (country?) you can read this:

In the 21st century, we share and store our most sensitive personal information on phones, computers and even in "the cloud." Today more than ever, a strong privacy program, which includes data security, is essential to the safety and welfare of the people of [redacted] and to our economy.

State of California Department of Justice, Attorney General Xavier Becerra

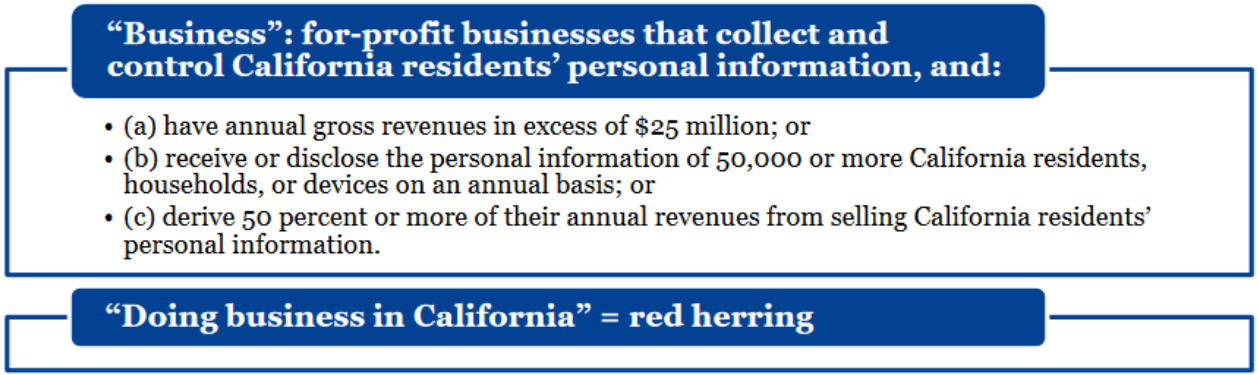
- - > Privacy in der EU und den USA



Petters, 2020.

California Consumer Privacy Act (CCPA)

- Grants rights to Californian residents over their personal information and the data they generate on websites, through devices, online and offline.
- Consumer rights – Business?



https://oag.ca.gov; https://calawyers.org, 25.02.2020; Morrison & Foerster LLP

California Consumer Privacy Act (CCPA)

- **Rights**
  - Disclosure / information
  - Deletion
  - Opt-out of sale
    (children must opt-in)
  - Right to non-discrimination
  - Right to sue

Obligations

Provide notice and keep records

„ Do not sell my Information.“ Info about consumers‘ rights

Create procedures (ie. information, respond to requests, data deletion)

Disclose purpose, source, financial incentives for retention/ sale of customers personal info

„**T**OM“, notify data breach

https://oag.ca.gov; https://calawyers.org, 25.02.2020.

CCPA and Financial Incentives

If businesses through its website make available to third parties (e.g. through cookies and social media plugins) data on Californian residents that is either not anonymized or has the potential to be re-identified, the **businesses might be categorized as a business "selling"** personal information.

- making available
- transferring
- otherwise communicating

The personal information of more than fifty thousand Californian residents per year.

https://calawyers.org, 25.02.2020.

CCPA and Financial Incentives

Right to know:

- what personal information a business has collected about them,
- where it was sourced from,
- what it is being used for, whether it is being disclosed or sold, and
- to whom it is being disclosed or sold;

Right to “opt out”:

- A business selling their personal information to 3rd parties;

⇒ Privacy policy/notices must use Personal Information categories,
⇒ Provide notice of whether Personal Information is sold
⇒ Listings of categories of Personal Information collected, sold, or shared with third parties for business purposes
⇒ Businesses that sell PI must include a “Do Not Sell My Personal Information” link on their homepage and web pages

CCPA and cookies

Third party cookies for **analytical** and **marketing** purposes collect information on users through unique IDs and similar tracking technologies are classified as **unique identifiers** that form part of the law's definition of personal information (1798.140.x).

Cookies are very important for CCPA compliance, since they are one of the most widely used tracking technologies for websites that can make a business liable under the CCPA.

Such third-party cookies are seen as a threat to privacy and autonomy.

Any information *"that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked"* with a *"consumer or household"* is potentially personal information under CCPA.

https://www.cookiebot.com/de/was-ist-ccpa; https://calawyers.org, 25.02.2020.

Anderer Zugang und anderer Umgang mit personenbezogenen Daten

FH | JOANNEUM
University of Applied Sciences

Problemstellung

EO 12333

While FISA generally covers surveillance activities inside the US, the government may also conduct surveillance **outside the US** under the authority of Executive Order 12333 (EO 12333). In broad terms, EO 12333 provides the foundational authority by which US intelligence agencies collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means.

Unlike FISA, surveillance under EO 12333 does not rely on the compelled assistance of electronic communications service providers. The technical details remain classified and obscure, but the NSA has confirmed it involves **exploiting vulnerabilities in telecommunications infrastructure**.

US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM | Fieldfisher, 4.11.2022.

FISA

Section 702 of FISA

The Foreign Intelligence Surveillance Act ("**FISA**") was enacted in 1978 to regulate US governmental electronic and physical surveillance of communications for foreign intelligence purposes. It has been amended, strengthened and reformed a number of times, including by the USA Patriot Act of 2001, the FISA Amendments Act of 2008 and the USA FREEDOM Act of 2015.

FISA authorises government surveillance through various means: electronic surveillance, physical searches, pen register and trap and trace surveillance and business record searches. All FISA activities are overseen by the Foreign Intelligence Surveillance Court ("**FISC**"), which sits in a secure courtroom in Washington D.C. Decisions by the FISC may be appealed to the Foreign Intelligence Surveillance Court of Review ("**FISC-R**").

FISA was originally intended to govern surveillance activities targeting individuals inside the US. In 2008, however, s702 (50 USC §§ 1881a et seq) was enacted to authorise the acquisition of foreign intelligence information about **non-US persons located outside the US**. A non-US person is anyone who is not a US citizen or permanent US resident.

US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM | Fieldfisher, 4.11.2022.

FISA

- Unlike the "traditional" FISA provisions, which require the government to obtain orders on an individualised basis and demonstrate probable cause, the Attorney General ("**AG**") and Director of National Intelligence ("**DNI**") submit **written certifications** to the FISC that jointly authorise surveillance activities for up to one year. **The government does not have to specify which non-US persons will be targeted or demonstrate probable cause. It merely needs to attest that a significant purpose** of the activities is to obtain foreign intelligence information and certify that appropriate targeting and minimisation procedures will be implemented.

- Once the FISC has approved a certification, the government issues directives to US **electronic communications service providers** that compel the providers to “immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition” of communications. Service providers must comply with these directives in secret and are not allowed to notify their users.

- The term "electronic communications service provider" is defined broadly to include **telecommunications carriers** (e.g., AT&T, T-Mobile, Verizon), providers of **electronic communications services** and **remote computing services** (e.g., Facebook, Google and AWS), as well as **any other communications service providers that have access to wire or electronic communications** (either in transit or in storage). Any company that provides its employees with corporate email or a similar ability to send and receive electronic communications, regardless of the company's primary business or function.

US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM | Fieldfisher, 4.11.2022.

75

PRISM / UPSTREAM

PRISM and UPSTREAM. Both are conducted under s702 of FISA but operate in different ways:

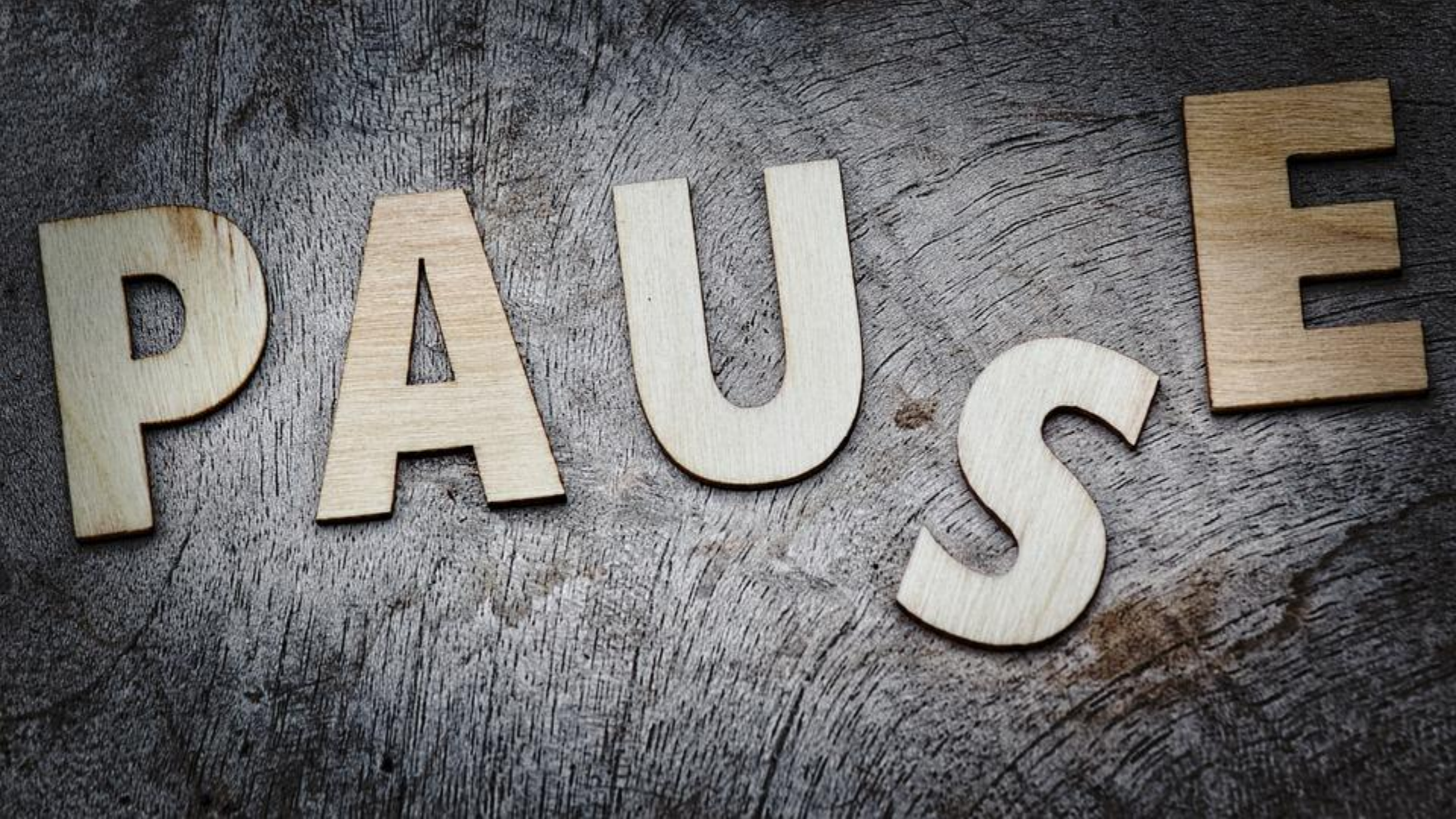
- PRISM involves the **direct 'downstream' collection of communications** by the NSA through the compelled assistance of electronic communications service providers. Effectively, the government sends a selector, such as an email address, to a US-based provider, and the provider is required to provide the government with all communications sent to or from that selector.

- As its name suggests, UPSTREAM involves the **indirect 'upstream' collection of communications** through the compelled assistance of **telecommunications providers that provide the backbone of the internet** (e.g. AT&T and Verizon). Essentially, the NSA copies and filters the vast quantity of data flowing through the network of cables, switches and routers that make up the Internet. Because the data is obtained **without the knowledge or assistance of downstream providers**, UPSTREAM has been described as a form of 'backdoor' surveillance.

US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM | Fieldfisher, 4.11.2022.

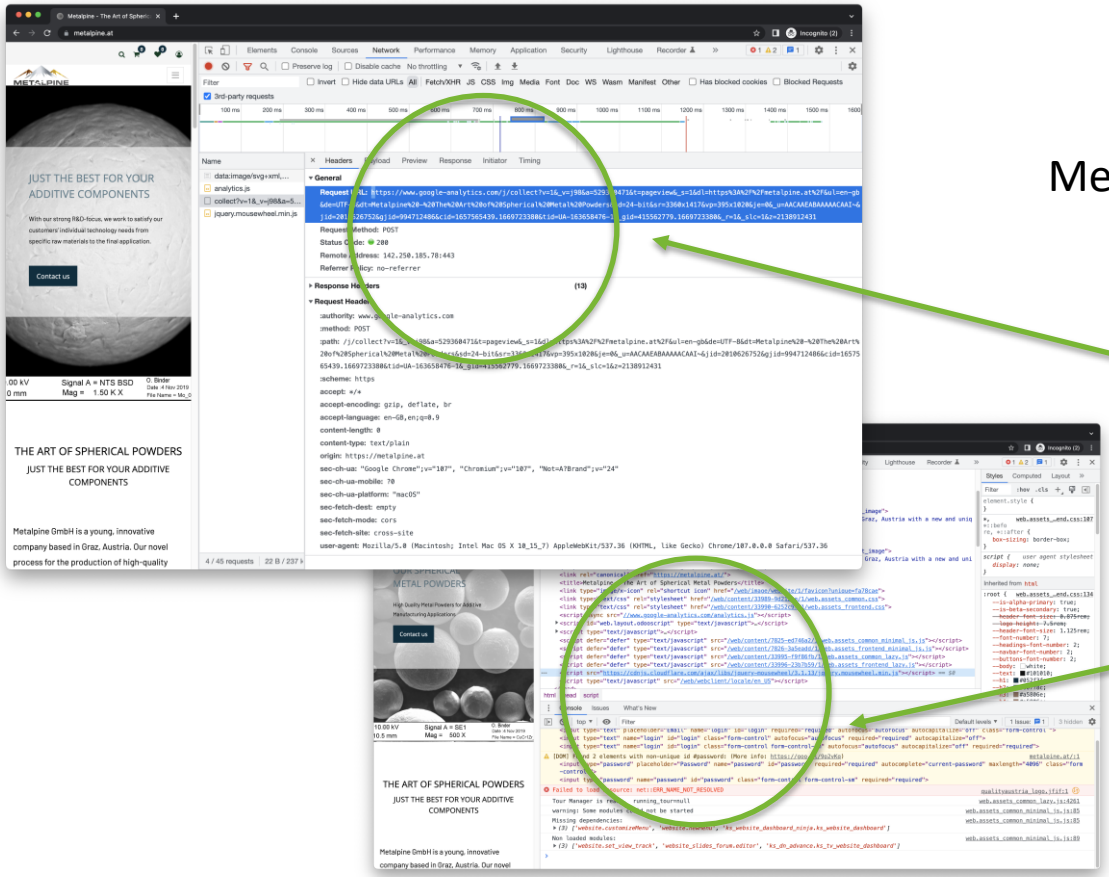
Pause

77


PAUSE

Problemstellung und Fälle

Agenda

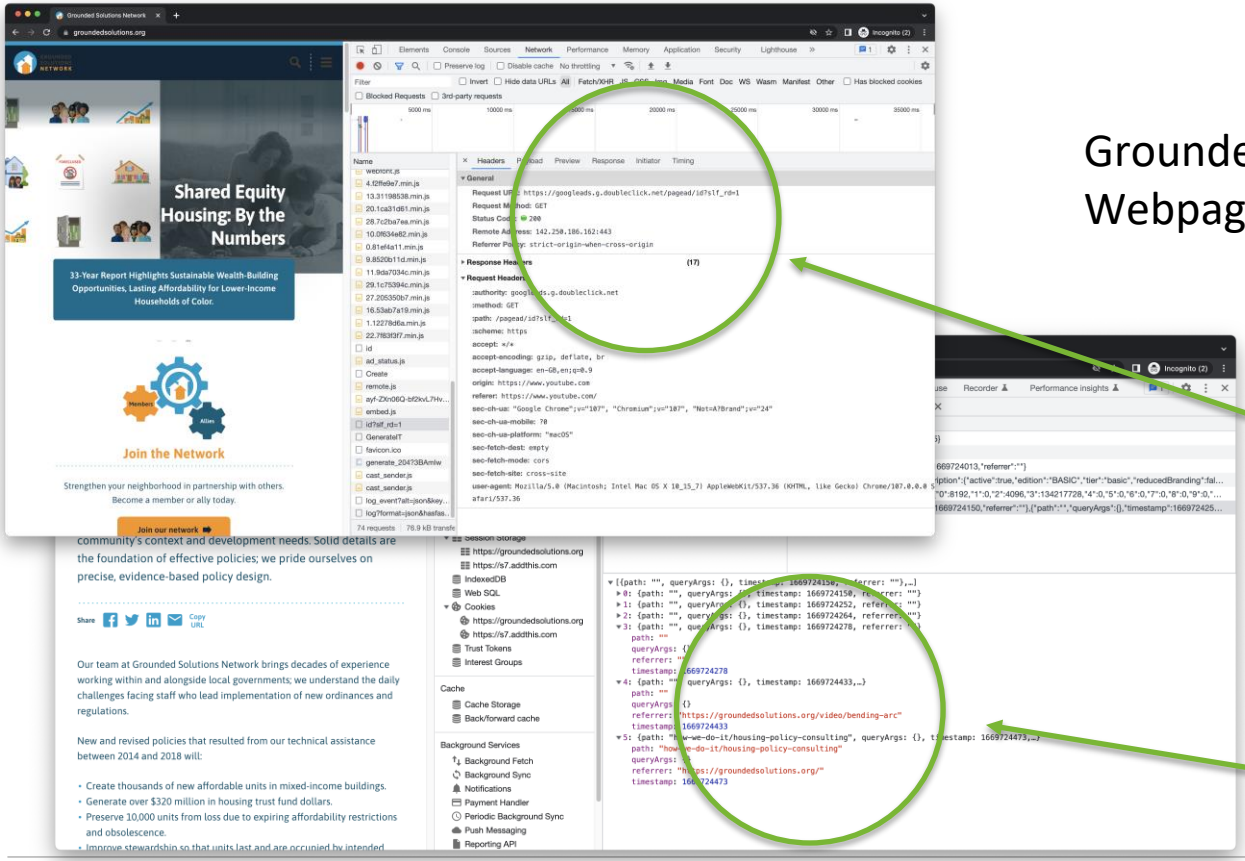


Metalpine Webpage

Verwendet
Google Analytics
Google Fonts

...und.. Cloudflare CDN

https://metalpine.at/



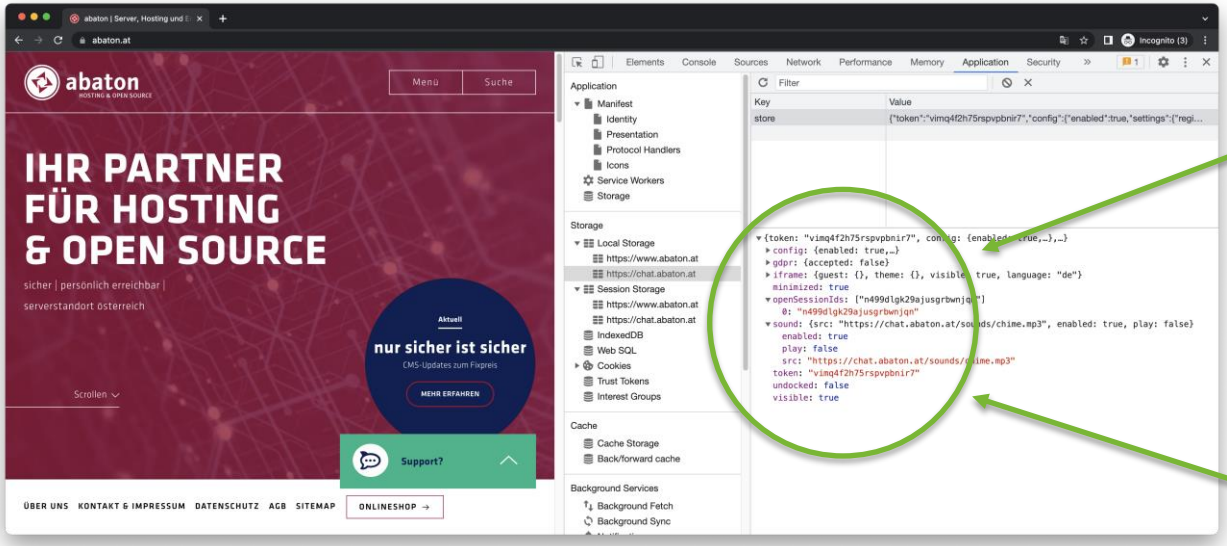
Grounded Solutions Webpage

Verwendet:
Google Ads DoubleClick,
External Sign-Upform
Recaptcha, ...

...und.. tracked auch den User Page Flow ....

https://groundedsolutions.org/

Abaton Webpage



Verwendet NUR
eigene Infrastruktur

... und das auch beim Chat ...

https://www.abaton.at/

Datentransfer in die USA

Angemessenheitsbeschluss „Safe Harbor“
-> EUGH 6.10.2015, C-362/14 (Schrems I) „Safe Harbor“

Angemessenheitsbeschluss (EU) 2016/1250 der EK als Nachfolgemodell „Privacy Shield“

- **partiell**
- **Selbstzertifizierungsmechanismus unter Aufsicht des MoC bzw der FTC**

-> EuGH 16.7.2020, C-311/18 (Schrems II) vor der irischen Aufsichtsbehörde (DPC), Vorabentscheidungsersuchen des Irishen High Courts, „Privacy Shield“

Datentransfer in die USA

„Schrems II“

DSB Republik Österreich Datenschutzbehörde

- **Maßgebliche Entscheidungsgründe**
  - **Vorrang** U.S.-amerikanischer Rechtsnormen im Zusammenhang mit nationaler Sicherheit, öffentlichen Interesse, oder Durchführung von anderweitigen Gesetzen
  - keine hinreichenden **Einschränkungen** für staatliche Eingriffe auf das unbedingt erforderliche Ausmaß iS. einer Verhältnismäßigkeitsprüfung
  - Keine hinreichend wirksamen und durchsetzbaren **Rechtsschutzmöglichkeiten** für Betroffene
- Insgesamt daher **kein ausreichender Schutz** der durch Art 7, 8 und 47 GrCH garantierten Rechte und Freiheiten

  (vgl. C-311/18, Rz. 168 ff)

Datentransfer in die USA

„Schrems II“

Republik Österreich
Datenschutz
behörde

- **Wesentliche Folgen**
  - „Privacy Shield“ **ungültig**, kann nicht mehr als Rechtsgrundlage für Datentransfers an (zertifizierte) Empfänger in den USA herangezogen werden
  - Datenübermittlungen bei Bestehen **anderer geeigneter Garantien** weiterhin möglich
  - SCC-P weiterhin grundsätzlich gültig, in bestimmten Fällen müssen aber **zusätzliche Maßnahmen** getroffen werden

    (vgl. C-311/18, Rz. 131 ff)
  - Obliegenheit für Verantwortliche zur **eigenständigen Beurteilung** eines entsprechenden Datenschutzniveaus im jeweiligen Zielort; Ausnahme: Angemessenheitsbeschluss (vgl. C-311/18, Rz. 134)

EDPB

Republik Österreich
Datenschutz
behörde

- **Wesentliche Dokumente bzgl. „Schrems II“**
  - **Erklärung** zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18
  - **Häufig gestellte Fragen** zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18
  - **Empfehlungen 01/2020** zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten
  - **Empfehlungen 02/2020** zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen

Datentransfer in die USA

EDPB

Republik Österreich
Datenschutz
behörde

- **Empfehlungen 01/2020** bzgl. zusätzlicher Maßnahmen

→ **Ergänzung** der Garantien, die bereits in dem in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrument enthalten sind (vgl. ErwGr. 109 DSGVO sowie C-311/18, Rz. 134)

- **Technische Maßnahmen**
  - z.B. Verwendung einer (Transport-)Verschlüsselung, Split-Processing
- **Vertragliche Maßnahmen**
  - Z.B. Verpflichtung zur Verwendung spezifischer techn. Maßnahmen
- **Organisatorische Maßnahmen**
  - Z.B. Schaffung interner Regeln für Datenübermittlungen, Datenminimierung

Datentransfer in die USA - Ausblick

- Annahme **neuer Standarddatenschutzklauseln** durch die EK
  - Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern, ABl. L 2001/199, S. 18 ff.
  - Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer, ABl. L 2001/199, S. 31 ff.

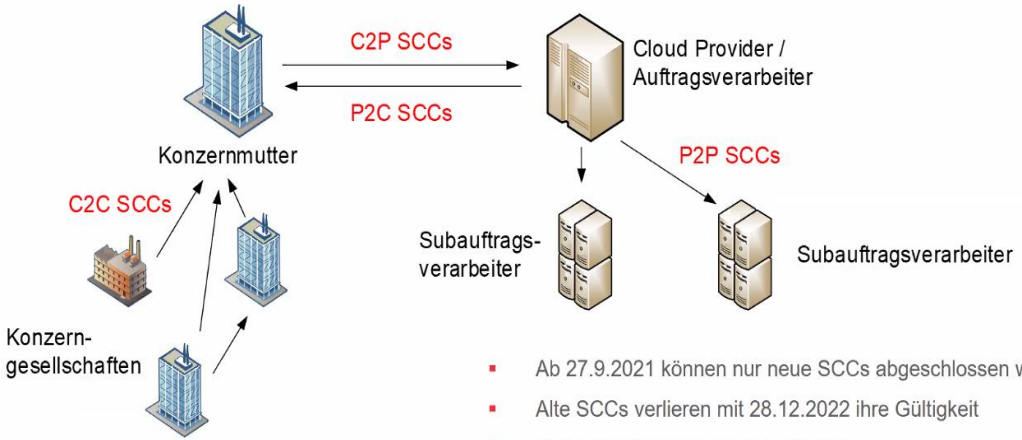
Datentransfer in Drittstaaten

Datenübermittlungen auf der Grundlage **geeigneter Garantien** können auch **ohne Genehmigung der Aufsichtsbehörde** erfolgen, wenn:

- **Standarddatenschutzklauseln**, die von der Kommission erlassen oder von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt worden sind.
- https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

Standardvertragsklauseln (SCC)

Die neuen SCCs



- Ab 27.9.2021 können nur neue SCCs abgeschlossen werden
- Alte SCCs verlieren mit 28.12.2022 ihre Gültigkeit
- Risiko-basierter Ansatz (ErwGr. 20)
- Dokumentierte Angemessenheitsprüfung (Art. 14(b)-(d) SCCs)
- Art. 28 DSGVO umgesetzt

Folie: Prof. Feiler

Standardvertragsklauseln

DURCHFÜHRUNGSBESCHLUSS (EU) 2021/915 DER KOMMISSION vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0915&from=EN

Durchführungsbeschluss vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung von Daten in https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914&from=DE

- Aber SCC+
  - TOMs
  - TIA

Transfer Impact Assessment (TIA)

Die Durchführung eines TIA ist in Klausel 14 der neuen SCC vorgeschrieben. Klausel 14 regelt den Umgang mit lokalen, im Drittstaat geltenden, Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der datenschutzrechtlichen Pflichten auswirken.

Die Parteien sichern zu, die Pflichten aus den SCC erfüllen zu können (Klausel 14.1 der SCC).

Transfer Impact Assessment (TIA)

Die SCC können jedoch nicht eingehalten werden, wenn die Rechtsvorschriften und Gepflogenheiten die Grundrechte der europäischen Grundrechte-Charta und Grundfreiheiten der europäischen Verträge missachten und über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft **notwendig und verhältnismäßig** sind, um eines der in Art 23 Abs 1 DSGVO aufgeführten Ziele sicherzustellen.

Betroffenenrecht
Verfahren

Datentransfer in Drittstaaten

Datenübermittlungen auf der Grundlage **geeigneter Garantien** können auch **ohne Genehmigung der Aufsichtsbehörde** erfolgen, wenn:

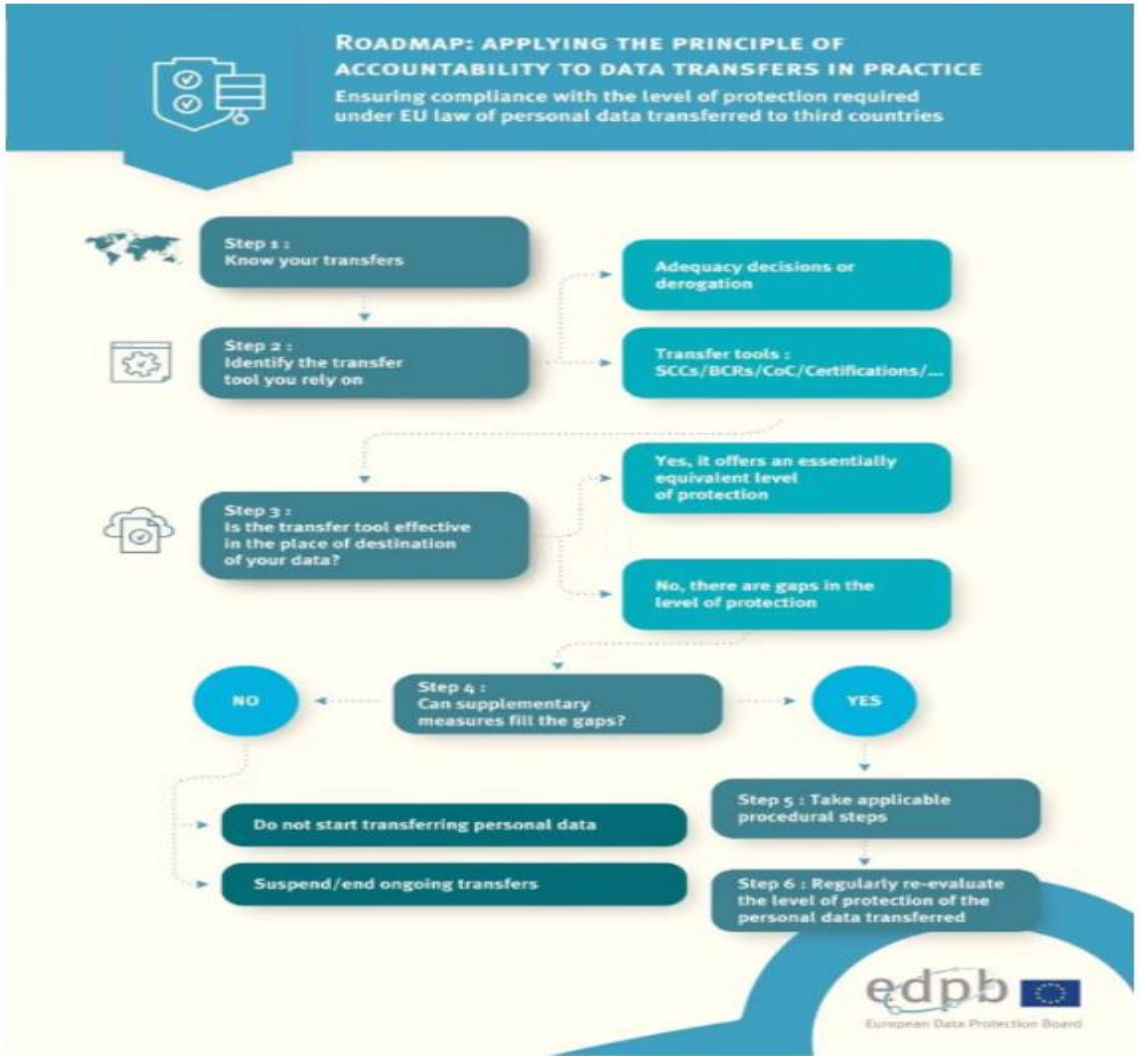
- Gesetzliche Grundlage
- Ausnahme

=> Sonst: Genehmigung der DSB

Datentransfer in Drittstaaten

Datenübermittlungen auf der Grundlage **einer Ausnahme für bestimmte Fälle** **ohne Genehmigung der Aufsichtsbehörde** erfolgen, wenn:

- eine **ausdrückliche Einwilligung** des vorliegt.
- für die **Erfüllung eines (Vor)Vertrages** (Hotelzimmer ..) erforderlich ist.
- zum Abschluss oder zur Erfüllung eines **im Interesse der betroffenen Person** von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist.
- zur Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen** erforderlich ist.
- zum Schutz **lebenswichtiger Interessen** der betroffenen Person oder anderer Personen erforderlich ist.
- aus wichtigen Gründen des **öffentlichen Interesses** notwendig ist oder erfolgt aus einem Register.


ROADMAP: APPLYING THE PRINCIPLE OF ACCOUNTABILITY TO DATA TRANSFERS IN PRACTICE
Ensuring compliance with the level of protection required under EU law of personal data transferred to third countries
Step 1 : Know your transfers
Step 2 : Identify the transfer tool you rely on
Adequacy decisions or derogation
Transfer tools : SCCs/BCRs/CoC/Certifications/...
Step 3 : Is the transfer tool effective in the place of destination of your data?
Yes, it offers an essentially equivalent level of protection
No, there are gaps in the level of protection
Step 4 : Can supplementary measures fill the gaps?
NO
YES
Do not start transferring personal data
Suspend/end ongoing transfers
Step 5 : Take applicable procedural steps
Step 6 : Regularly re-evaluate the level of protection of the personal data transferred
edpb
European Data Protection Board

(Quelle: EDPB)

US –EU Data Transfer: neuer Angemessenheitsbeschluss?

EO vom 7. Oktober 2022
EU-US Data Privacy Framework, Privacy Shield II

FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework | The White House

New US Executive Order unlikely to satisfy EU law (noyb.eu)

Questions & Answers: EU-U.S. Data Privacy Framework (europa.eu)

97

US –EU Data Transfer: neuer Angemessenheitsbeschluss?

EO vom 7. Oktober 2022
EU-US Data Privacy Framework, Privacy Shield II

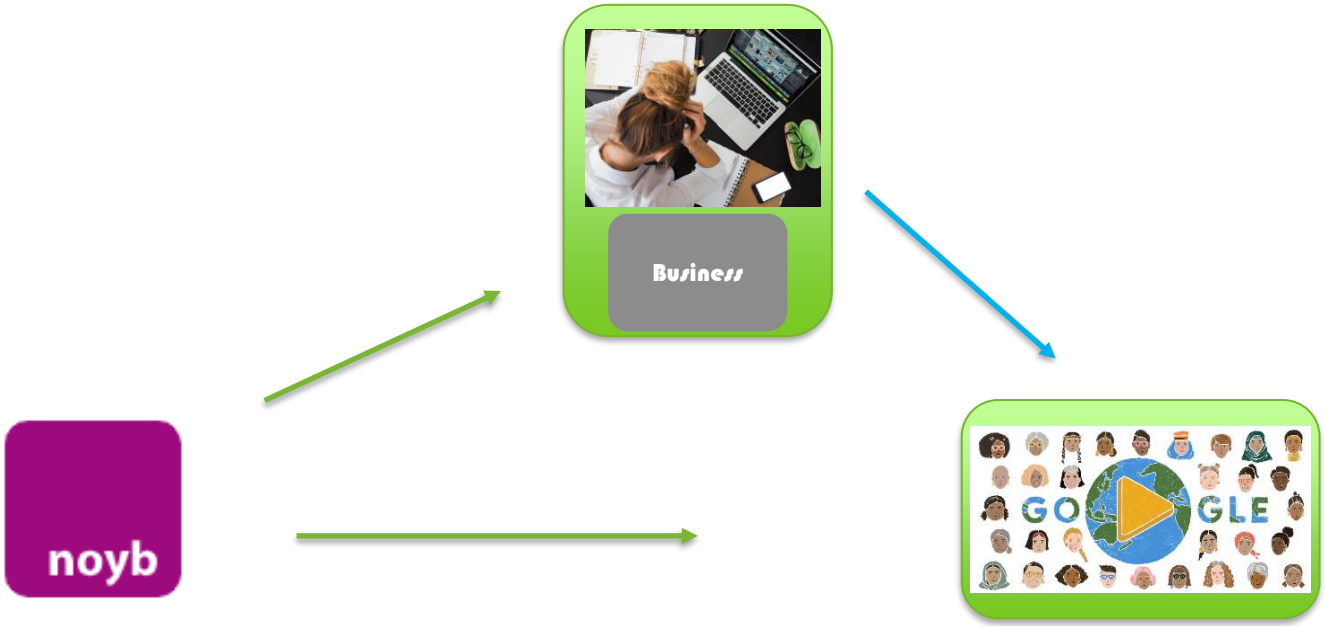
Die neuen Maßnahmen umfassen:

Die Stärkung der Privatsphäre und der Freiheitsrechte bei Aktivitäten der sog. **signalerfassenden Aufklärung** (Gewinn von Erkenntnissen aus elektromagnetischen Ausstrahlungen mit und ohne Kommunikationsinhalt, i.d.R. durch Nachrichtendienste)

Die Einrichtung eines zweistufigen, unabhängigen Rechtsmittelmechanismus hinsichtlich aus Betroffenensicht unrechtmäßigen Aktivitäten der Nachrichtendienste, durch den Abhilfemaßnahmen verbindlich angeordnet werden können

Die signalerfassende Aufklärung soll einer strengen, mehrstufigen Aufsicht unterstellt werden, um die Einhaltung der Beschränkungen der Überwachungsmaßnahmen sicherzustellen

Aktuell, dh 2021 / 2022 NOYB gegen Google Analytics



Datenverarbeitung in den USA Beispiel Google

The Google account is the red thread which connects how users' data is used across all Google services. Consumers can choose to create a Google account voluntarily or be obliged to create one when they use certain Google products and services. For example, they must create an account when they buy a smartphone that uses Google's Android system, which almost 7 in 10 phones worldwide (69%)1 depend on, if they want to download apps from the Google Play store.

Quelle: Google puts its users on a 'fast track to surveillance': EU and U.S. groups urge authorities to take action (tacd.org)

Weitere Fälle

Abmahnwelle in Österreich

Ausschluss von Unternehmen mit US Anbietern als Auftragsverarbeiter vom Vergabeverfahren in Deutschland

...

Agenda

Anonymisierung

… und andere Alternativen

Alternative Technologien (sensible Daten)

Weniger Daten generieren:

- Beispiel: coarse location
- Beispiel: text

Sensible Daten anonymisieren:

- Beispiel: Image blurring
- Beispiel: Differential Privacy

Zero Trust

- Beispiel: Homomorphic Encryption (HE)

We need:
Privacy by Design

Beispiel: Datenminimierung

Aktuelle Position (GPS)

https://appleinsider.com/articles/20/06/22/approximate-location-in-ios-14-limits-positioning-data-to-within-10-square-miles

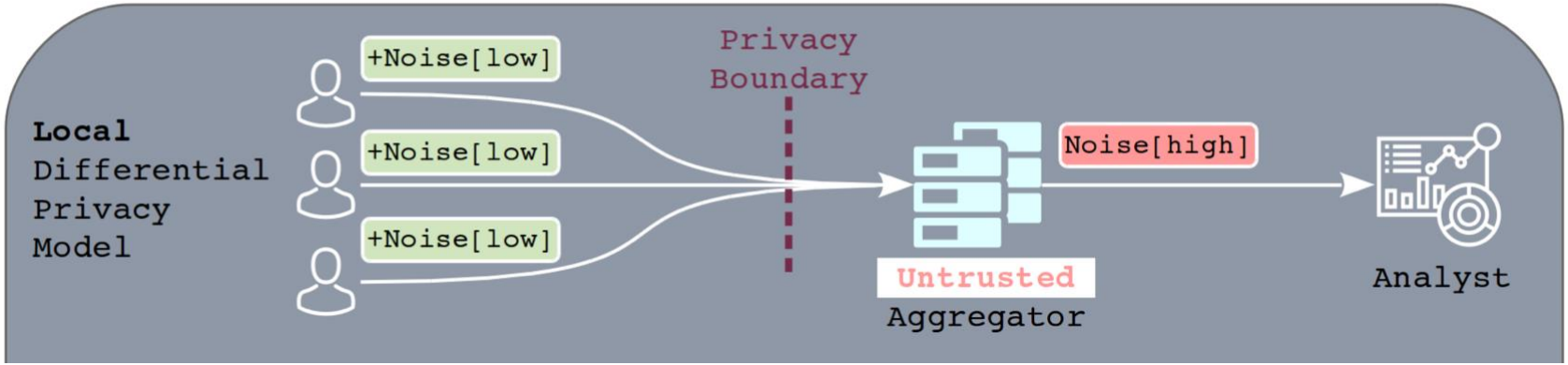
Beispiel: Sätze und "Sinn" entfernen

Stemming
Lemmatisation

```
Text: He glanced up from his computer when she came into his office
Stem: ['glanc', 'comput', 'came', 'offic']
Lemma: ['glance', 'computer', 'come', 'office']
```

https://www.analyticsvidhya.com/blog/2021/06/rule-based-sentiment-analysis-in-python/

Beispiel: Differential Privacy



Helmut Bierbaumer, IMS19

Beispiel: Unscharfe/Verpixelte Bilder

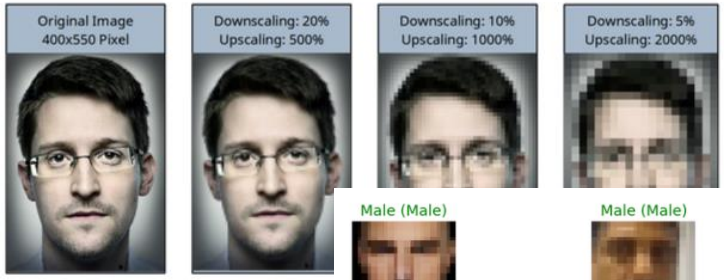


Figure 2.5: Exemplary results of imag

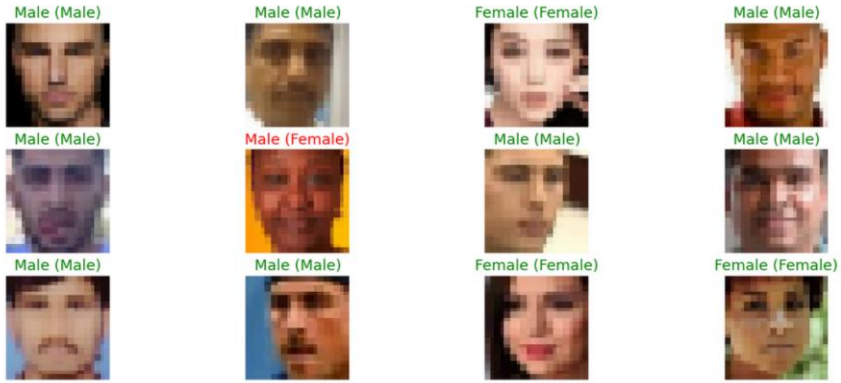
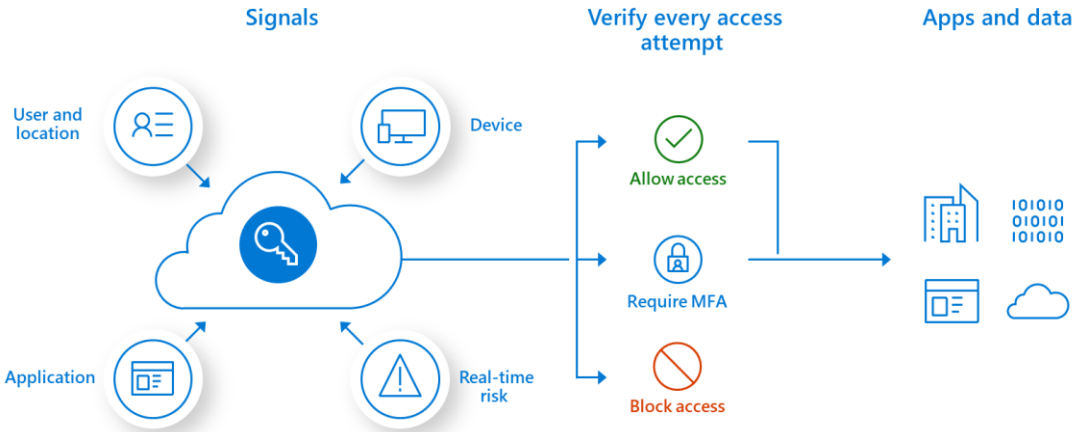


Figure 3.76: An exemplary test run demonstrates that a CNN trained with pixelated images only misclassifies one out of 12 sample pictures.

ML / Objekterkennung funktioniert trotzdem noch

Helmut Bierbaumer, MA 2021

Idee/Ansatz: "Zero Trust"



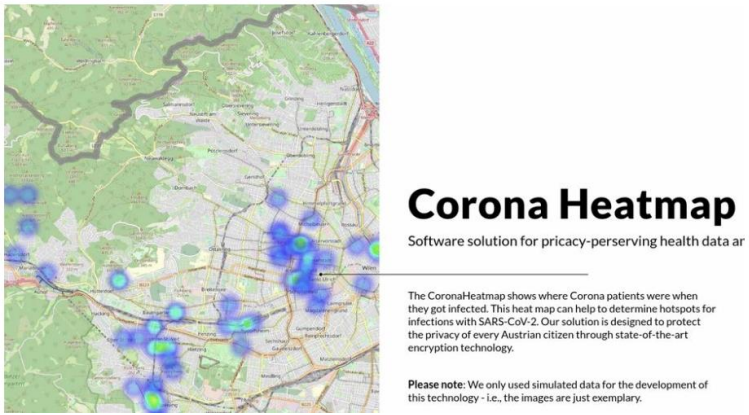
https://www.microsoft.com/en-ie/microsoft-365/blog/wp-content/uploads/sites/16/2019/09/Zero-trust-model-1.png

Aktuelle Forschung: Homomorphic Encryption

TU Graz kombiniert Gesundheits- und Bewegungsdaten datenschutzkonform

Konzept basiert auf homomorpher Verschlüsselung – Erstellte Softwarelösung für "CoronaHeatMap" – Ermöglicht mit Daten zu rechnen, ohne sie vorher entschlüsseln zu müssen

20. Mai 2021, 16:37



https://www.derstandard.at/consent/tcf/story/2000126812003/tu-graz-kombiniert-gesundheits-und-bewegungsdaten-datenschutzkonform

Alternativen für Cloud Dienste?

Ursprüngliche Idee:

verteiltes Internet

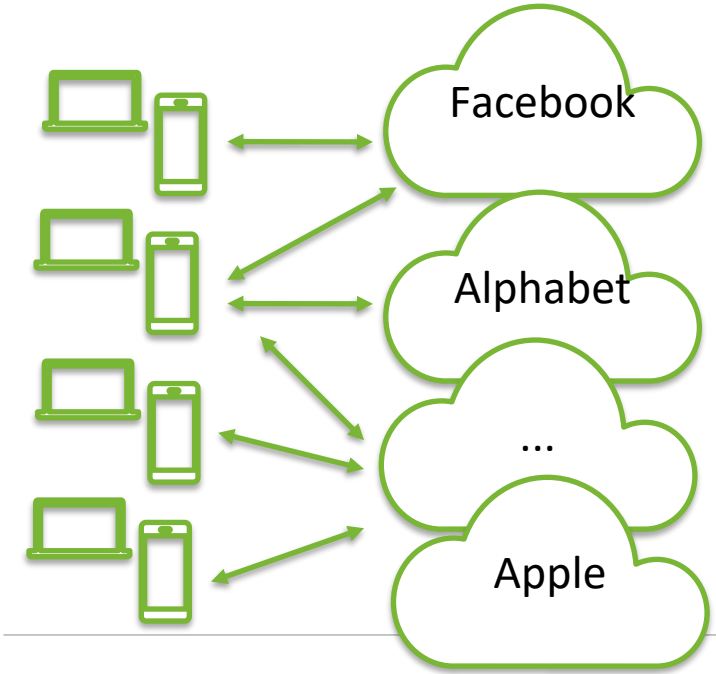
Aktuelle Trend:

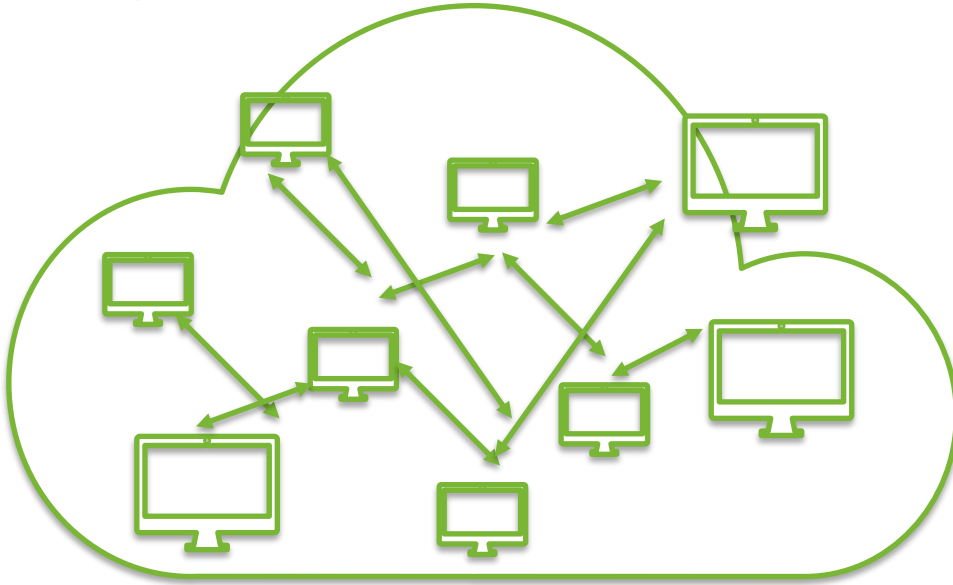
einzelne Firmen dominieren

(monopolartig, Locked-in)

(verteilt sind zwar deren Rechner und Daten)

Clouddienste versus ursprüngliches Internet

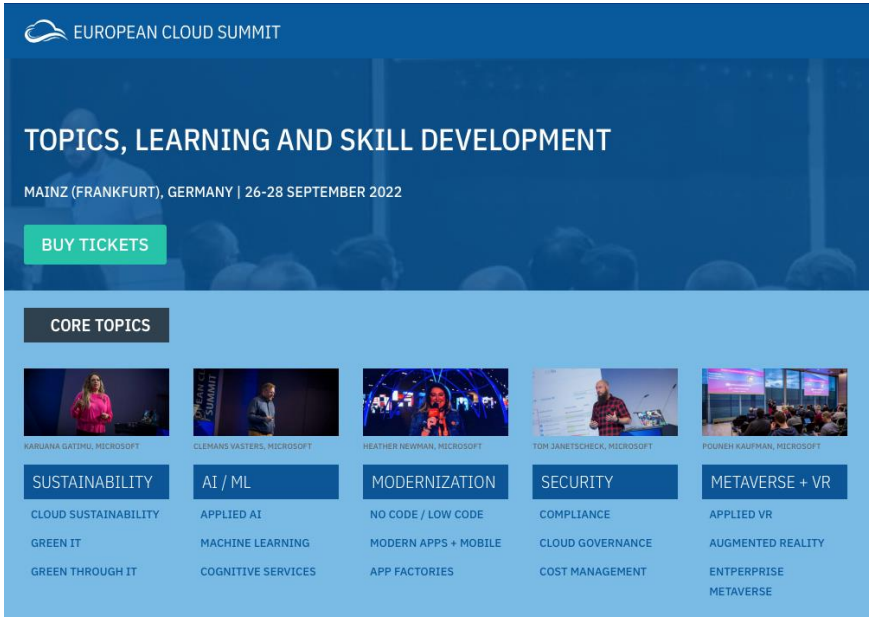




Alternativen für Cloud Dienste?

Sind europäische
Cloud Dienste
ein Thema?

Compliance



https://www.cloudsummit.eu/en/learning/

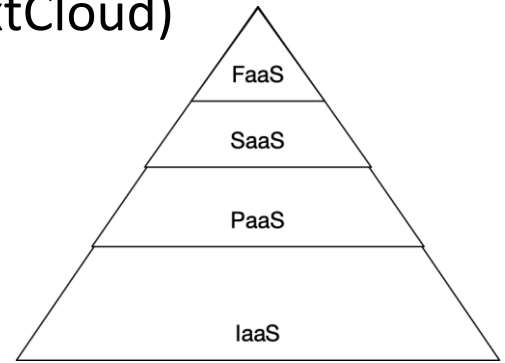
Alternativen für Cloud Dienste?

Open Source Tools & Services (IaaS, PaaS, SaaS, FaaS)

Backup (Verschlüsselung) & Synchronisation (NextCloud)

Virtualisierung (Kubernetes), DevOps

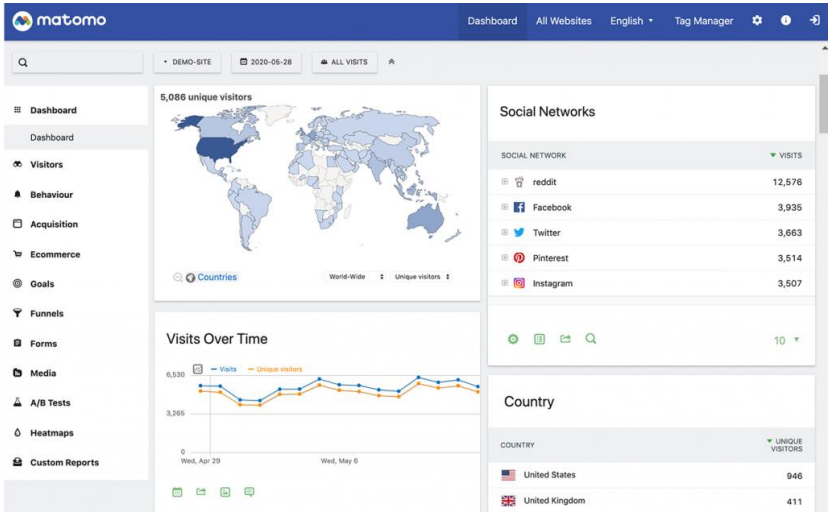
(auch Selbst-Hosten,
"Cloud native" Development)



Alternativen für Cloud Dienste

Statt Google Analytics

Matomo

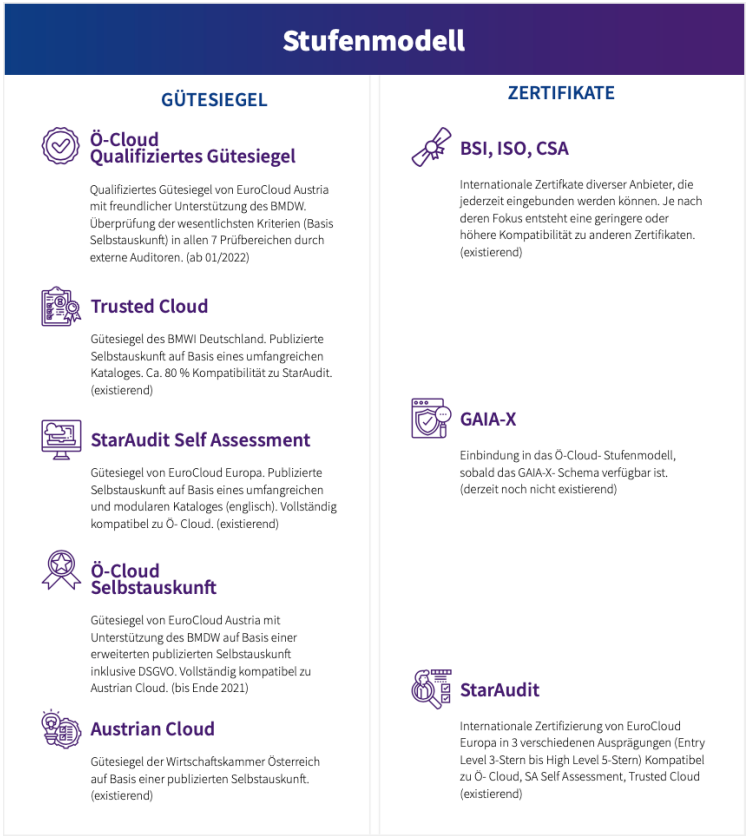


https://blog.runcloud.io/google-analytics-alternatives/#2-matomo

https://matomo.org/matomo-analytics-the-google-analytics-alternative-that-protects-your-data-variation/

Alternativen

Ö-Cloud Initiative



https://gaia-x.eu/what-is-gaia-x/

https://www.exoscale.com/

https://www.fabasoft.com/en/o-cloud-quality-seal

https://www.nextlayer.at/en/cloud/o-cloud/

https://oe-cloud.eurocloud.at/en/information/


Fazit

- Google Analytics ist jedenfalls unzulässig und sollte sofort von den Webseiten entfernt werden.
- Das gilt auch für von der Cloud geholte Dienste wie Schriftarten, die bereits vor der Zustimmung Daten übermitteln
- Alle Anbieter, Webseiten enthalten bis zu 50 solcher Dienste, sollten kritisch hinterfragt werden:

-notwendiger Dienst? Wenn nein, weggeben / ausschalten.

- Wenn ja und es handelt sich um US Anbieter:
  - ersetzbar durch alternative (europäische) Anbieter?
  - strengste Sicherheitseinstellung wählen.
  - Zustimmung einholen
  - TIA durchführen

Langfristig:
- solide datenschutzfreundliche Lösungen, europäische Cloud(s)
- faire und sinnvolle Digitalisierung
-

https://www.dsb.gv.at/

EDPB

- **Europäischer Datenschutzausschuss**
  - **unabhängige** europäische Einrichtung, Art. 68 ff DSGVO
  - Förderung und Beitrag zur **einheitlichen Anwendung** der Datenschutzvorschriften in der EU sowie zur **Zusammenarbeit** zwischen EU/EWR-Aufsichtsbehörden
  - Vertreter der nationalen Aufsichtsbehörden sowie Europäischer Datenschutzbeauftragter, EK Teilnahme- aber kein Stimmrecht
  - aktueller Vorsitz: Leiterin der DSB
  - **Plenum** sowie **Fachgruppen** („subgroups“)

Weiterführende Informationen

Unger, Kaja, Datenschutzrecht (2018)

Social Media, Rolf Schwartmann, Tobias Keber, Robin Mühlenbeck, Beck Verlag, 2. Auflage (2018)

Weitere Informationen auch auf Webseiten der WKO, der AK …

Saferinternet: https://www.saferinternet.at/
Epicenter.works: https://epicenter.works/

noyb.eu: https://noyb.eu/en
computer chaos club https://www.ccc.de/

https://www.youtube.com/watch?v=bPS3ojekcKw
(Explainity.com)

…

Weiterführende Informationen

Website der DSB: www.dsb.gv.at

Newsletter der DSB: erscheint vierteljährlich und kann unter dsb@dsb.gv.at bestellt werden

Datenschutzberichte jährlich: abrufbar auf der Website der DSB

Leitlinien der Art. 29-Gruppe -> abrufbar auf der Website der Kommission

Art 29 Datenschutzgruppe: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083, jetzt EDSB

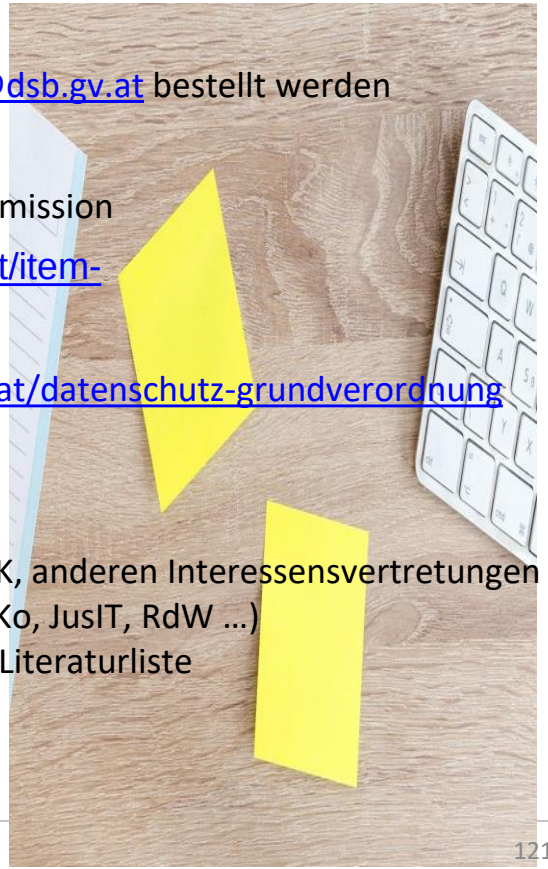
Leitfaden der DSB zur DSGVO abrufbar unter https://www.dsb.gv.at/datenschutz-grundverordnung

Grazer Datenschutzgespräche der Karl Franzens Universität Graz

einmal im Quartal (Prof. Staudegger, Prof. Bergauer)

Weitere Informationen auch auf Webseiten gv.at; der WKO, der AK, anderen Interessensvertretungen

- Kurze Artikel, Überblick / Praxistipps / Checklisten (DaKo, JusIT, RdW …)
- Lange Artikel mit Detailbetrachtung und umfassender Literaturliste (JBl, ZöR …)



Weiterführende Informationen

https://epicenter.works/
None of your business
https://www.univie.ac.at/RI/IRIS17/
https://www.infolaw.at/
https://www.it-law.at/

https://www.bsi.bund.de
https://www.iso.org/isoiec-27001-information-security.html

International:
Deutschland
https://www.datenschutz-wiki.de/Düsseldorfer_Kreis
CNIL
ICO

122

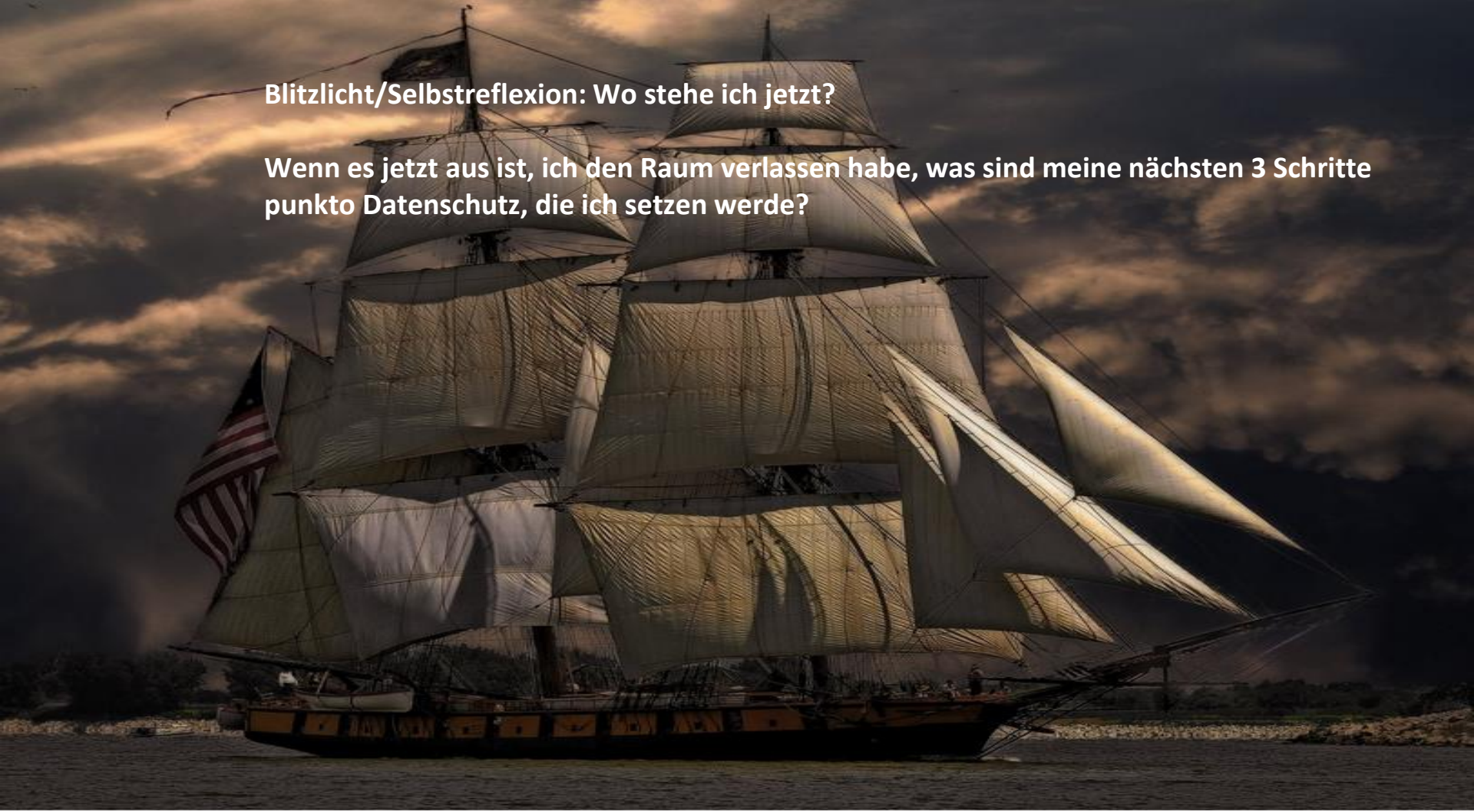
r. Jörn von Lucke - Wohin führt uns eigentlich das Internet der Dinge? @ IRIS2019

Datenschutzrecht
Menschenrecht

Data Science
Machtausgleich

Abschluss

Agenda



Blitzlicht/Selbstreflexion: Wo stehe ich jetzt?

Wenn es jetzt aus ist, ich den Raum verlassen habe, was sind meine nächsten 3 Schritte punkto Datenschutz, die ich setzen werde?

"Technology is a useful servant, but a dangerous master."

[Christian Lous Lange]

DIHSÜD Digital Innovation Hub

FFG Forschung wirkt.

Das Land Steiermark

LAND KÄRNTEN