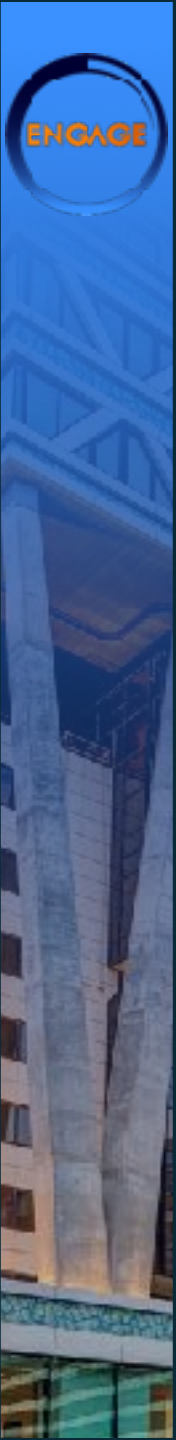


The ABC of Sovereign Cloud: Protect your data

Engage 2025 – The Hague





Sovereign Cloud

- 1) Intro
- 2) The boring part
- 3) Example galore
- 4) The future



Wannes Rams



ISW

 HCL Lifetime Ambassador



Thomas Hampel



HCLSoftware

Andreas Ponte



Belsoft
collaboration

 HCL Ambassador





Digital Sovereignty

1)‘ Digital sovereignty is control of our present and destiny as manifested and guided by the use of technology and computer networks ‘

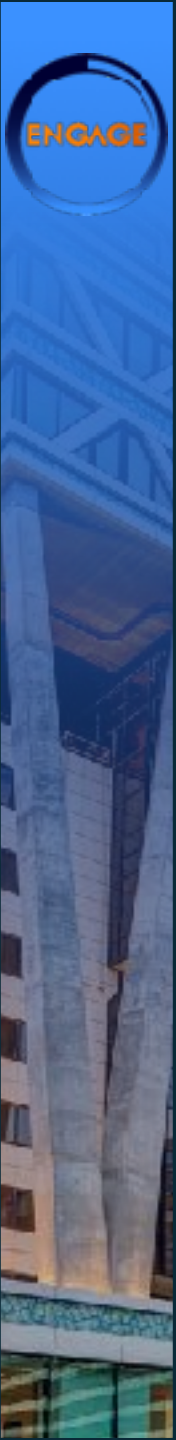
Pierre Bellanger, 2011

2)Digital sovereignty, cyber sovereignty, technological sovereignty and data sovereignty refer to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create.



Figure 1.1: Different approaches to governance of personal and non-personal data

Country/ bloc	Overall approach to digital sovereignty	Approach to personal data	Approach to non-personal data
U.S.	Does not adopt language of digital sovereignty, but has advocated for an open and unregulated cyberspace in which big tech plays a dominant role.	No unified approach to protection of personal data at the federal level; some states regulate personal data. The Clarifying Lawful Overseas Use of Data (CLOUD) Act authorises US authorities to demand access to data held by US companies overseas.	Free flow of both personal and non-personal data.
China	Promotes a government-led approach to digital sovereignty. Has put in place policies to control the internet.	Personal Information Protection Law (PIPL) has similarities with the EU's General Data Protection Regulation (GDPR) on extraterritorial application, principles on the processing of personal data, and rights of individuals. Additional requirements e.g. local storage of personal information by critical information infrastructure operators.	Non-personal data classified according to national security and public interest considerations. 2017 Cybersecurity Law and 2021 Data Security Law with specific requirements for security assessment before data is transferred abroad.
E.U.	Third way between the US (unregulated surveillance capitalism) and the Chinese (surveillance-heavy) models with a strong focus on individual rights.	Protection of personal data is a fundamental right with mandatory requirements under the GDPR for processing personal data. Extrajurisdictionalisation of the GDPR as entities outside the EU/EEA apply these principles to retain access to EU data. Restrictions on transfers of personal data and requirements on how personal data is treated once it has left the EU/EEA.	Free flow of non-personal data with rules on fair access, use of non-personal data, and mechanisms to increase data availability.



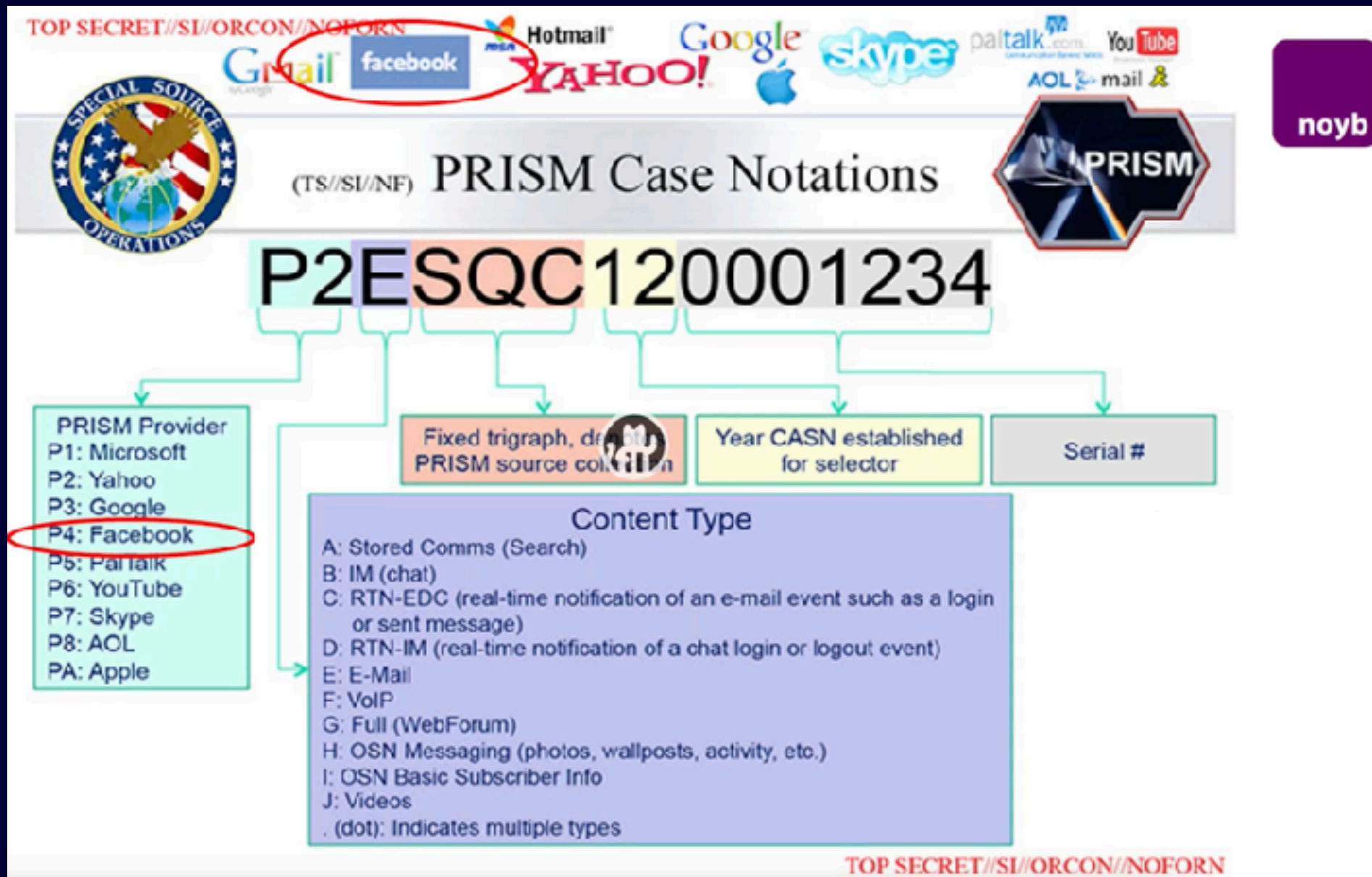
Safe Harbour Agreement (2000)

1) Comply with the European Data Directive 1995

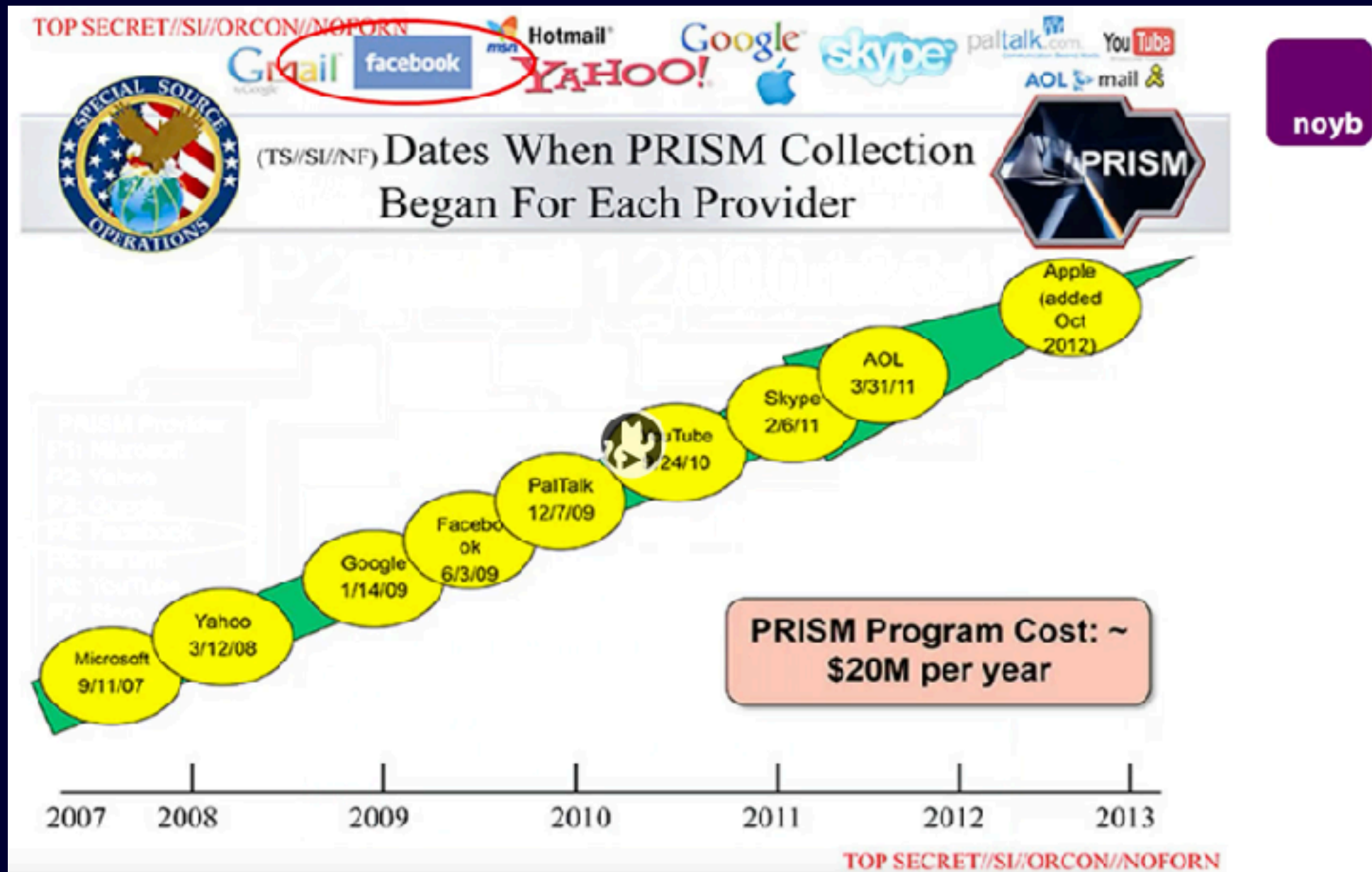
- Notice
- Choice
- Onward transfer
- Security
- Data Integrity
- Access
- Enforcement



Snowden 2013



Snowden 2013



FISA § 1881a

noyb

- **Electronic Communication Service Provider**
- **„Foreign Intelligence Information“**

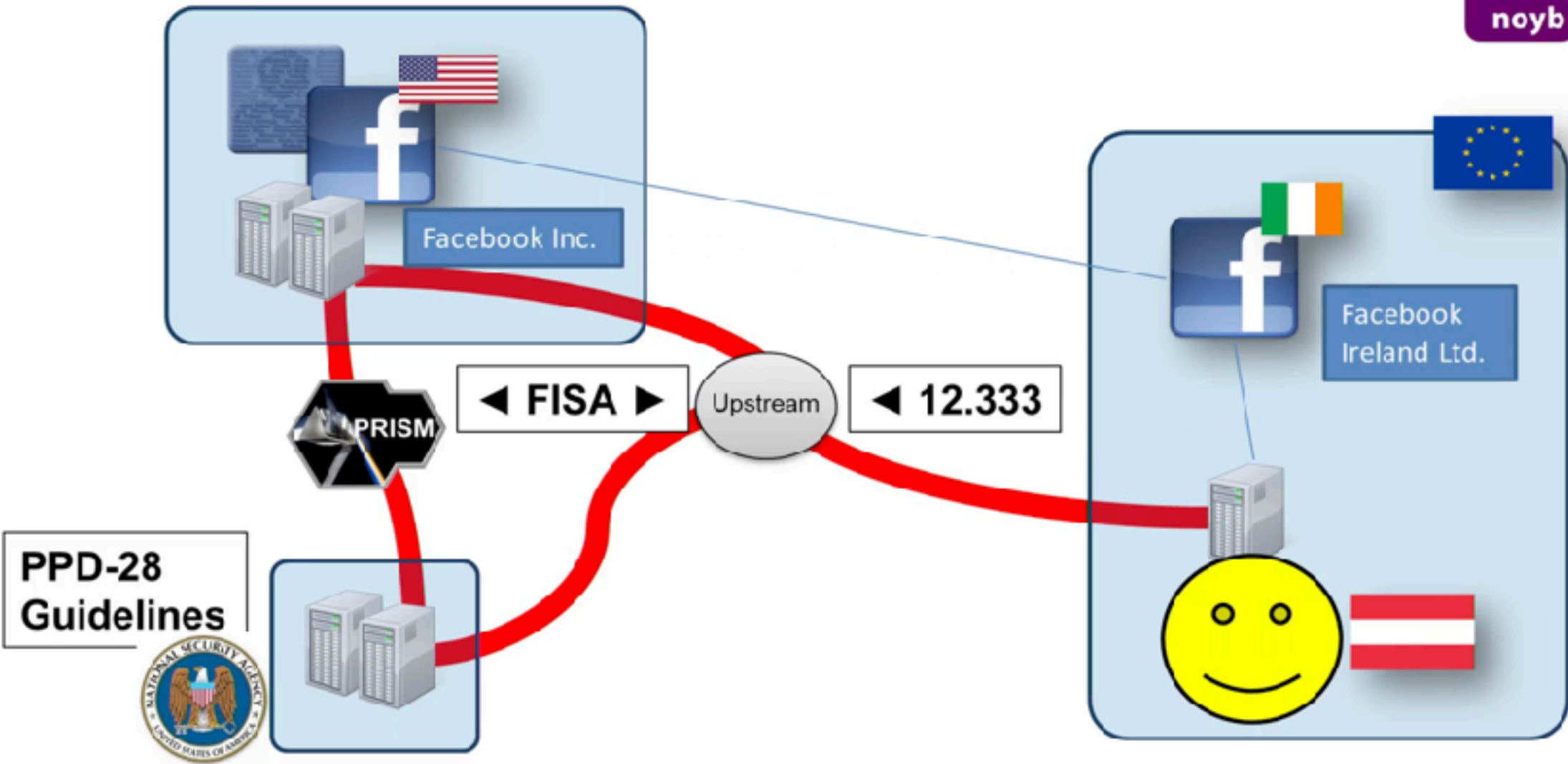
- **Certification for one year** („FISA Court“)
 - Minimizing / Targeting procedures (US persons)
- **„Directive“ at Service Provider**
 - Technical Interface (?)

CLASSIFIED





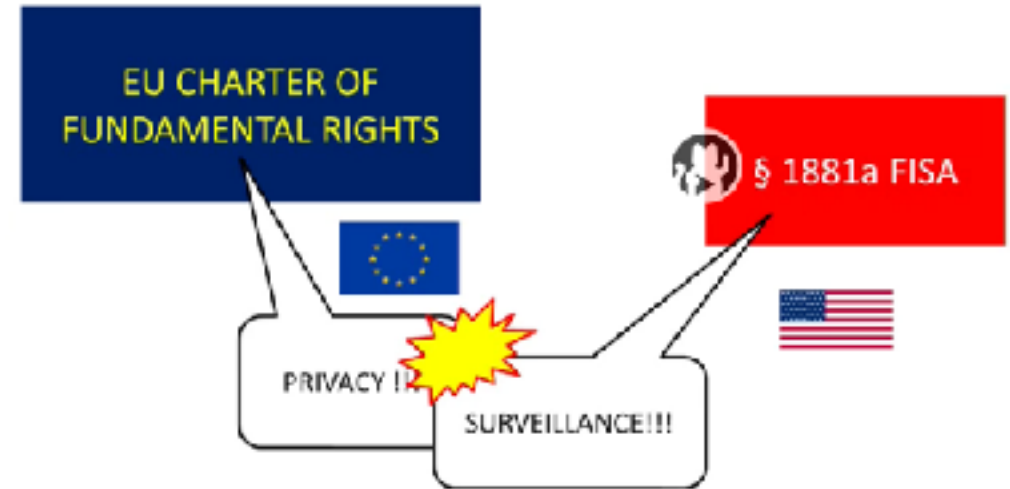
Snowden 2013



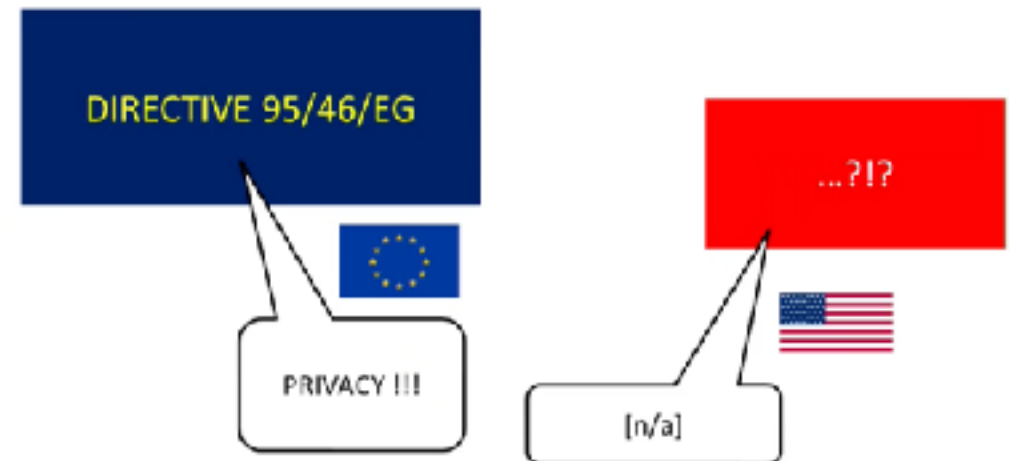
Schrems I

- 1) 2016 invalidating Safe Harbour
- 2) Privacy rights activist Max Schrems
- 3) Snowden
- 4) Violations:
 - Mass Surveillance violates Art 7 CFR
 - Legal Redress in US violates Art 47 CFR

GOVERNMENT: CONFLICT OF LAW



PRIVATE SECTOR: LACK OF LAW





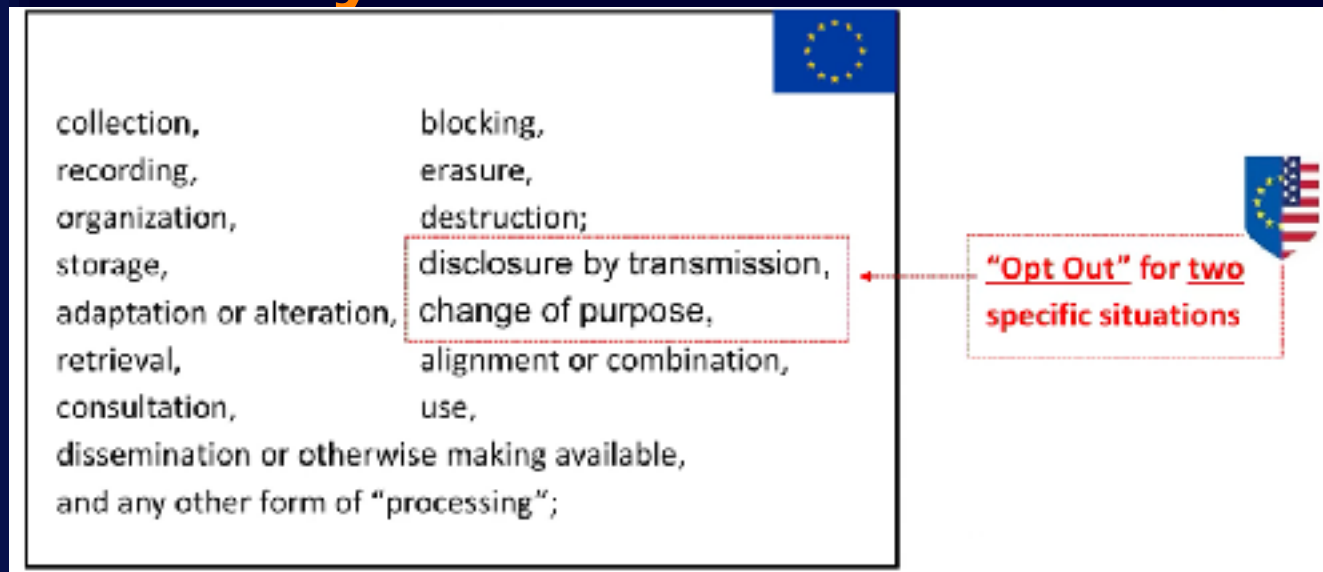
Privacy shield

- 1) Safe Harbour 1.0.1
- 2) Same agreement with a limited amount of new text
- 3) Still uses Notice & Choice and not consent





Privacy shield



USE A BROAD PURPOSE

+

THIRD PARTY CLAUSE

=

UNLIMITED DATA PROCESSING



Schrems II (2020)

1) Court case invalidating the EU-US Privacy shield

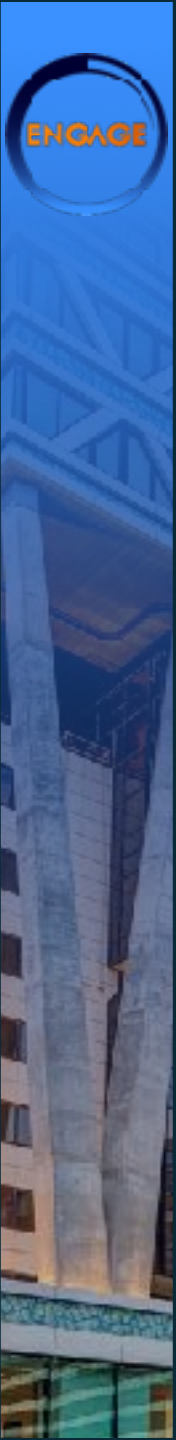
2) Most important findings of the court

- US law has limited protection for personal data, so the shield cannot be guaranteed
- US foreign Intelligence and Surveillance Act and their surveillance programs were found not to be compliant with the agreed shield.



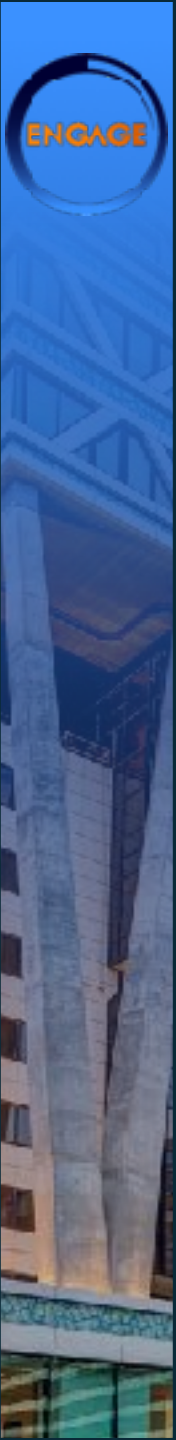
Data privacy framework

- 1) 2023
- 2) Protect EU citizens data when transferred to US
- 3) Limit US intelligence authorities access to data
- 4) Enhancing Safeguards for United States Signals Intelligence Activities Executive order signed by Joe Biden in 2022
- 5) Limits access to data by US intelligence in proportion to national security
- 6) But, legal challenges remain



Schrems III ?

- 1) Might not be needed
- 2) Initial complaints not resolved
- 3) EU might pause the agreement



Latombe case

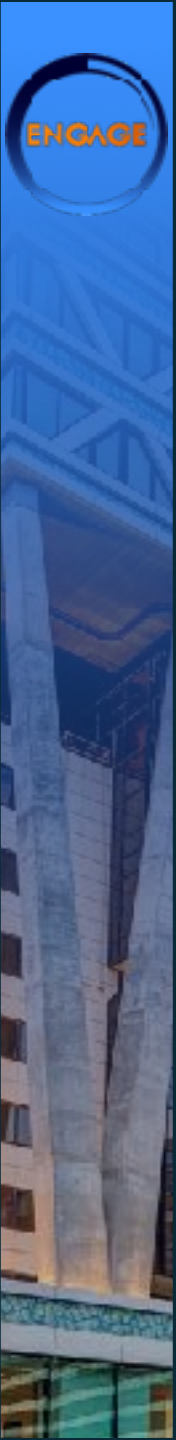
1) Started April 1

2) Philippe Latombe, French MP



Trump

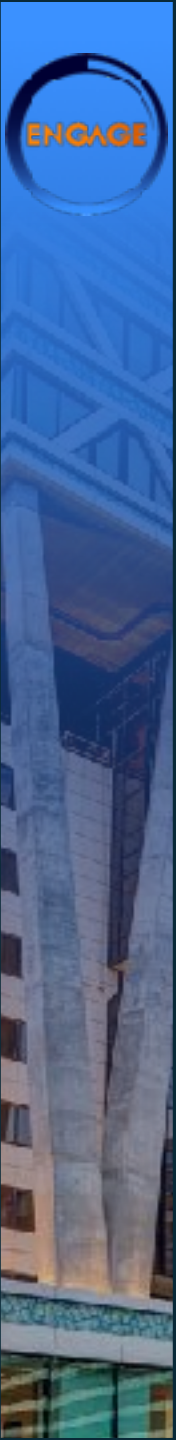
- 1) Requested resignation of democrats in PCLOB
- 2) In one of the first Executive Orders that he signed on Inauguration Day, President Trump decided that his predecessor's national security decisions – including the decisions creating and supporting the DPF – should be reviewed and potentially annulled within 45 days



Risks when invalidated

- 1) Need to rely on SSCs for data transfer
- 2) Meta was fined 1.2bn for relying on SSCs by the Irish DPC in 2023
- 3) Risk of fines
- 4) No more US cloud





Some Examples

- **French government** officially declared that the use of #O365 (and #Teams) is not allowed for French Public Admin organizations.

<https://www.channelnews.fr/letat-ferme-ses-portes-a-office-365-dans-le-cloud-de-microsoft-105899>

- **Swedish Tax Authority**

Denies the usage/participation in external meetings conducted via Teams

- **Germany: Hessen**

Using U.S. Cloud products forbidden in Schools

<https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/duldung-des-hbdi-f%C3%BCr-die-nutzung-insbesondere-us>



Skatteverket

Decision

Date
03/05/2021

Reference no.
The Swedish Tax Agency
8 958696

1(20)



Kronofogden

The Swedish Enforcement Authority
KFM 10419-2021

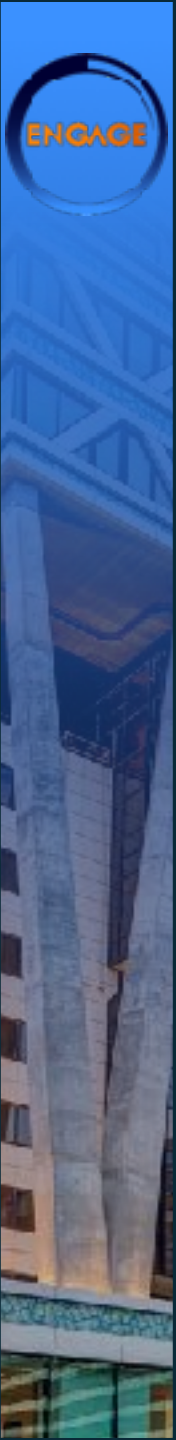
Decision

The Swedish Tax Agency and the Swedish Enforcement Authority ("Kronofogden") have decided:

- not to replace the application Skype with the cloud service Teams for video conferencing and collaboration
- to allow participation in external meetings conducted via Teams
- that the Swedish Tax Agency, the Swedish Enforcement Authority, and other authorities that choose to participate, will set up a cross functional working group to investigate suitable alternative video conferencing and collaboration platforms.

Reasons

The Swedish Tax Agency and the Swedish Enforcement Authority have jointly investigated the possibility of replacing Skype with Teams as their main video and collaboration platform. The decision follows the recommendations set out in the attached memorandum.



“It’s Secure!”

- **Russian hackers breached key Microsoft systems**
<https://edition.cnn.com/2024/03/08/tech/microsoft-russia-hack/index.html>

≡ **CNN Business**

DOW
S&P 500
NASDAQ

Business / Tech

Russian hackers breached key Microsoft systems

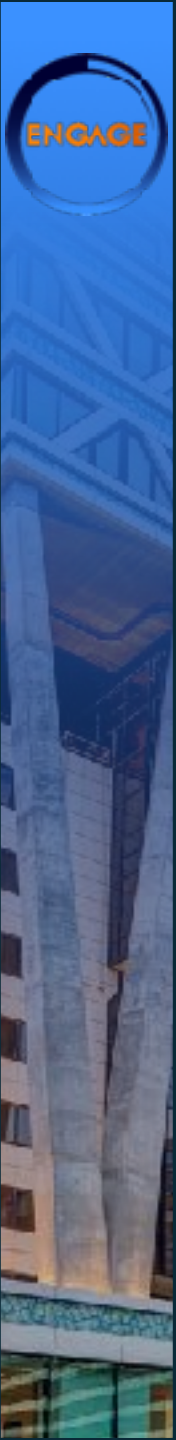
By Sean Lyngaas, CNN

🕒 2 minute read · Updated 11:34 AM EST, Fri March 8, 2024



A photograph of a Microsoft sign at the company's headquarters. The sign features the four-colored Microsoft logo (red, green, blue, yellow) and the word "Microsoft" in a large, metallic, sans-serif font. The sign is mounted on a low, dark stone wall. In the background, there is a modern glass-walled building, some trees with red leaves, and a well-manicured hedge.

A Microsoft sign is seen at the company's headquarters on March 19, 2023 in Seattle, Washington. | Ryu/Visual China Group/Getty Images



“Its Stable”

[Website down checker](#)[Product](#)[Docs](#)[Screenshots](#)[Pricing](#)[Login](#)[Start trial](#)

Is this website down?

Enter a URL to check if a website is down from around the world.

Check

OnlineOrNot can also monitor your company's websites automatically, [learn more](#).

Results

[Share results](#)

URL: <http://zoo.tokyo>

Date checked: 5/15/2025, 10:45:14 AM

Asia Pacific (Sydney)

120ms
5/3

Offline

Asia Pacific (Tokyo)

118ms
5/3

Offline

Europe (Frankfurt)

155ms
5/3

Offline

US East (N. Virginia)

152ms
5/3

Offline

US West (N. California)

209ms
5/3

Offline

Want to be notified when your company's website goes up or down?

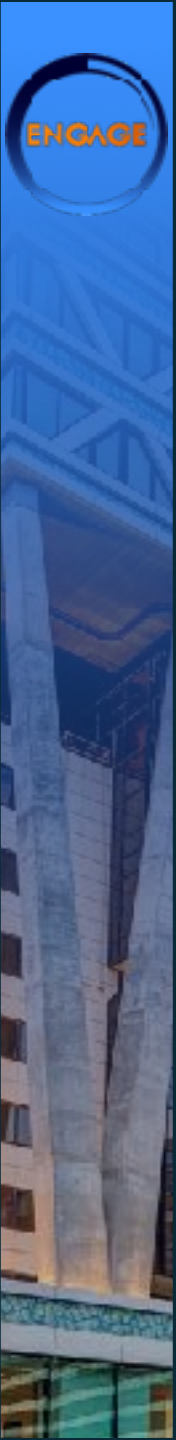
[Learn more](#)



Did you know

- Microsoft has stored your passwords online – even against your will.
- Microsoft is cracking password protected zip files to analyze the data within.
<https://www.heise.de/news/Microsoft-untersucht-auch-passwortgeschuetzte-zip-Dateien-auf-Malware-9057387.html>
- Google is doing the same...
<https://www.heise.de/news/Google-scannt-Cloud-Dateien-nach-rechtswidrigen-und-schaedlichen-Inhalten-6298682.html>





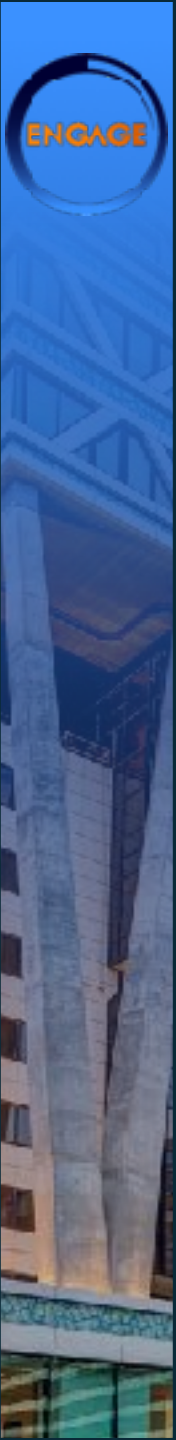
Politics on the hook of Microsoft

FTC has opened an Antitrust case against Microsoft

<https://www.bloomberg.com/news/articles/2024-11-27/us-antitrust-watchdog-launches-broad-microsoft-investigation>



<https://www.nytimes.com/2024/11/27/technology/microsoft-ftc-antitrust.html>



- **Complete dependence on American tech giants**
- No control over own data
- Lawful access via CLOUD Act
- The recent police hack, made possible by **weak security in Microsoft Outlook**, shows how vulnerable this dependence makes us.

In this hack, the data of 65,000 police officers was stolen
<https://innovationorigins.com/nl/de-zeer-verontrustende-politiehack-moet-wakeupcall-zijn-voor-elk-bedrijf/>

<https://ioplus.nl/en/posts/trump-has-free-rein-over-dutch-government-data>

Trump has free rein over Dutch government data

The Netherlands relies heavily on American IT service providers such as Microsoft, Google and Amazon for the storage of government data.

Published on February 13, 2025





- It is not possible to use M365 in any legal way
https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

- Microsoft consultants will continue to trick customers
<https://www.kuketz-blog.de/nach-dsk-bewertung-zu-ms365-rechtsberater-weiterhin-auf-kundenfang/>

AG DSK „Microsoft-Onlinedienste“

Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung.

1. Untersuchungsauftrag, Verfahren und Untersuchungsgegenstand

Die DSK hatte am 22. September 2020 eine **Bewertung des Arbeitskreises Verwaltung** zu den dem Einsatz des Cloud-Dienstes Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service Terms (OST) sowie den Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020 – hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die damalige Bewertung des AK Verwaltung kam zu dem Ergebnis, „dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“ sei.

Die DSK hat in ihrer Sitzung am 22. September 2020 eine Arbeitsgruppe unter Federführung Brandenburgs und des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) gebeten, Gespräche mit Microsoft aufzunehmen, „um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die strenge B-Festcheidung des FzGH aufgezeigten Mängel bei den Drittscotentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen“.

Daraufhin hat diese Arbeitsgruppe Ende 2020 Gespräche mit Microsoft begonnen. Teilnehmer der AG waren: Brandenburg und BayLDA (beide Leitung), BfDI, Baden-Württemberg, Berlin, Hessen, Mecklenburg-Vorpommern, Sachsen, Saarland und Schleswig-Holstein. Für Microsoft haben Beschäftigte der Microsoft Deutschland GmbH einschließlich eines Mitgliedes der Geschäftsleitung sowie je nach Schwerpunkt Ansprechpartner der Microsoft Corporation (USA) teilgenommen. Im Rahmen der Gespräche fanden 14 mehrstündige Videokonferenzen statt.

Beiden Gesprächen war zu berücksichtigen, dass federführende Datenschutzaufsichtsbehörde für Microsoft Ireland Operations, Ltd. als Partei des Auftragsverarbeitungsvertrags die irische Aufsichtsbehörde ist und die deutschen Aufsichtsbehörden für die Aufsicht der jeweiligen deutschen Kunden (z.B. Unternehmen, Behörden, also die Verantwortlichen im Sinne von Art. 4 Nr. 7

¹ Vgl. TOP9 L TOP 9 – Datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Microsoft Office 365¹, S. 5, abufbar unter: https://www.datenschutzkonferenz-online.de/media/p/20201030_protokoll_1_zusatzkonferenz.pdf



More links

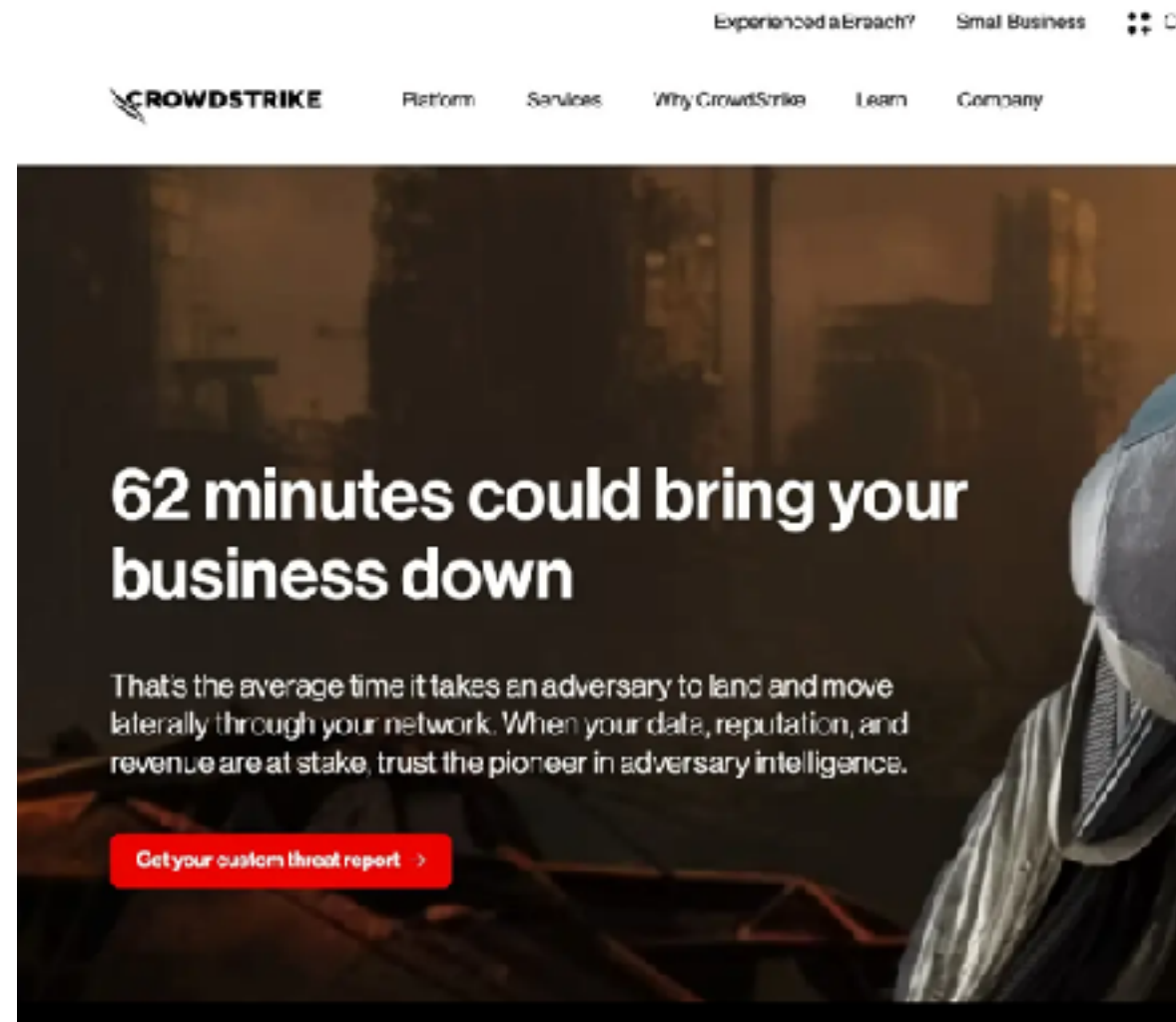
References:

- **EU and Microsoft : Laziness as excuse for not having an alternative**
<https://www.kuketz-blog.de/kommentar-eu-und-microsoft-365-alternativlosigkeit-als-bequeme-ausrede/>
- **Data Protection Impact Assessment (DPIA): Diagnostic Data processing in Microsoft Teams, OneDrive, SharePoint and Azure AD**
<https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad>
- <https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/>
- <https://www.kuketz-blog.de/bildungswesen-entlarvung-der-haeufigsten-microsoft-mythen/>
- Despite violating the law, even governments don't take any action against Microsoft
<https://artikel91.eu/2021/11/02/aufsichten-vs-microsoft-cloud-viel-dialog-fast-keine-sanktionen/>
- Customers are afraid of sanctioning of Microsoft – instead planning an exit strategy:
<https://www.kath-datenschutzzentrum-ffm.de/wp-content/uploads/MS-Cloud-2019-KDSZ-FFM.pdf>



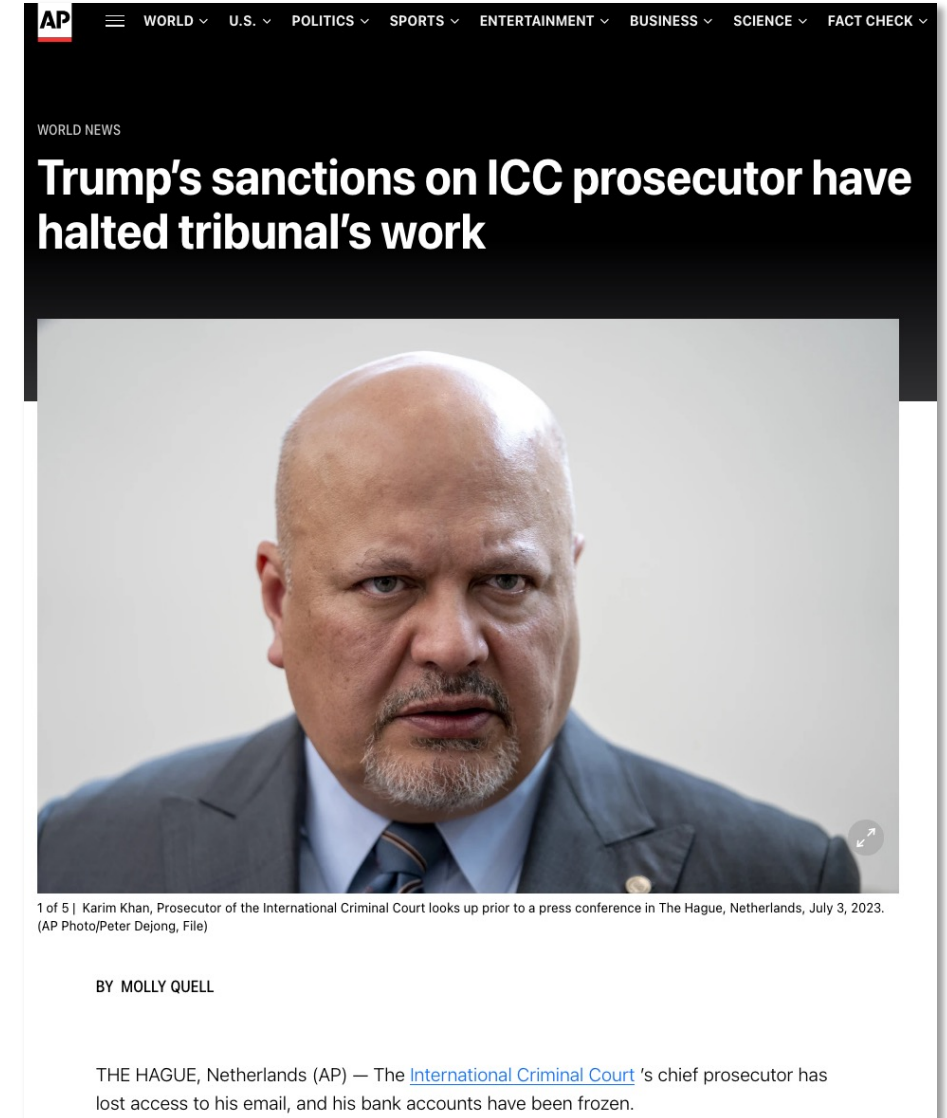
Monocultures are a risk

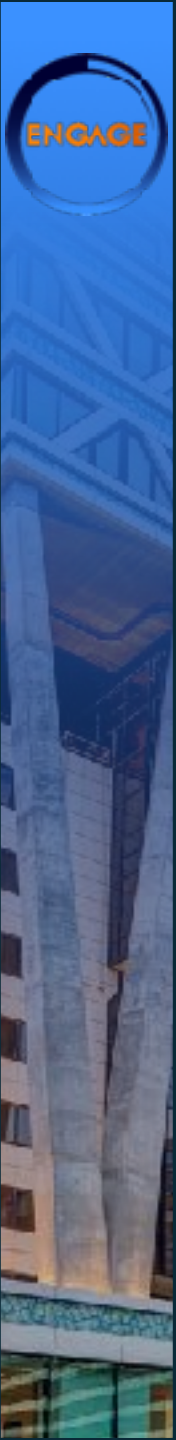
Remember CrowdStrike?



The Hague

- Trump's sanctions on ICC prosecutor have halted tribunal's work <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>
- Microsoft cancelled Khan's email account
- bank accounts in his home country of the U.K. have been blocked.







Tommaso Gagliardini • 3rd+
Cryptographer and Cybersecurity Expert
6d •



You have probably seen this [#viral #infographic](#) on [#eu #digitalsovereignty](#) by [#reddit](#) user u/lukakopajtic. It was viral but not very accurate 😬 recommending [#bluesky](#) and [#firefox](#) as "EU alternatives"? How? Anyway, he just updated the infographic, and it's much, much better! Most is ~~now~~ have been corrected. I think there is still a couple of issues I disagree with: 1) recommending [#matrix](#) instead of [#jabber #xmpp](#) 2) recommending [#freenode](#) instead of [#grapheneos](#) (but OK, I can understand this if the focus is on self-sovereignty only), 3) recommending [#roidify](#) instead of [#acrescent](#) (but, even here, I can understand if the goal is to replace [#playstore](#)), and 4) recommending [#thunderbird](#) as a comparison to [#gmail](#) (nothing wrong with Thunderbird, but that's an email client, not a Gmail-like suite provider, I would have rather recommended [#mailfence](#) or [#mailbox](#)). Kudos for the initiative though, the intentions are good!

<https://lnkd.in/drWdqApB>

👍💡🌐 88

36 comments · 3 reposts



Like



Comment



Repost



Send

DIGITAL INDEPENDENCE

Updates and more info on lukakopajtic.com/independence

  →  

 →  


 →  




    →  

  →  

  →  

 →  

 →  

   →  

 →  

  →  

 →  

 →  

 →  

 →  

 →  

 →  

  →  

  →  



Fichter: Der US-Staat veranstaltet gerade Hackathons mit den Steuerdaten der US-Bevölkerung, während Akteure wie Musk und das Doge-Gremium Zugriff auf Milliarden sensibler Datensätze haben. Die Tech-Konzerne zeigen Bereitschaft zur engen Zusammenarbeit mit der Trump-Regierung.

« US-Behörden können jederzeit auf Daten von US-Cloud-Anbietern zugreifen – unabhängig vom Standort. »

Das Beispiel des Hackathons zeigt: Die Regierung hat nicht nur theoretisch Zugriff auf riesige, zuvor getrennte Datenöpfel, sondern will mit leistungsfähigen KI-Modellen alles zusammenführen, um neue Informationen zu gewinnen. Schutzmauern fallen – alles wird zusammengeworfen und ausgewertet.

Was bedeutet das für Nutzerinnen und Nutzer?

US-Behörden können jederzeit auf Daten von US-Cloud-Anbietern zugreifen – unabhängig vom Standort der Rechenzentren. Die Konzerne dürfen solche Zugriffe nicht öffentlich machen. Zwar versprach die Biden-Administration eine stärkere Kontrolle der Geheimdienste, woraus ein neues transatlantisches Datenschutzabkommen zwischen den USA, der EU und der Schweiz entstand. Doch dieses Kontrollorgan wurde unter Trump wieder abgeschafft. Es ist zu

theregister.com/2025/03/19/dutch-parliament_us_tech/?id=r1-3a

The Register

Time to ditch US tech for homegrown options, says Dutch parliament

Trump administration 'has made the call for tech sovereignty an urgent geopolitical issue'

By [Brandon Vukobratovic](#)

Wed 19 Mar 2025 | 17:02 UTC

in

on

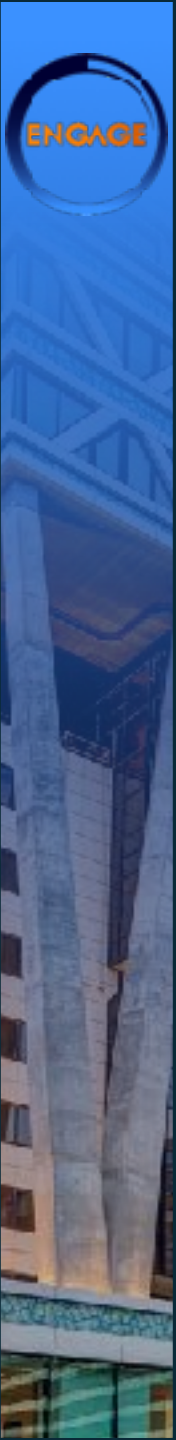
Not content to wait for open letters to influence the European Commission, Dutch parliamentarians have taken matters into their own hands by passing eight motions urging the government to ditch US-made tech for homegrown alternatives.

Concerns over European reliance on US tech companies are mounting, with tech experts in the EU sounding the call as the Trump administration's international posture becomes increasingly bellicose.

Boffins in the Netherlands, in particular, rang the alarm in February, with Dutch Electoral Council technical advisor Bert Hubert warning that using US cloud services was no longer safe for either the government or civil society.

It's perhaps for that reason that parliamentarians have been considering the motions passed yesterday for a while, as Kathmann explained.





Solutions are available but..

- you need to research
- you need to verify the solutions
- you need to invest time-money-resources
and make sure to cover all relevant
compliance requirements

Although Microsoft is not subject to BIR 2012 compliance, government customers who wish to use cloud services can use Microsoft's existing certifications to determine their compliance with this standard.

▼ EMEA

EU Cloud CoC

EU EN 301 549

EU ENISA IAF

EU GDPR

EU Model Clauses

Germany C5

Germany IT-Grundschutz Workbook

Netherlands BIR 2012

Qatar NIA

Russia personal data law

Spain ENS High

Spain LOPD

UAE DESC

UK Cyber Essentials Plus

UK G-Cloud

UK PASF



Local authorities are stepping up and will support your quest

The BSI is the Federal Cyber Security Authority and the chief architect of secure digitalisation in Germany.



French Cybersecurity Agency (ANSSI) Agence nationale de la sécurité des systèmes d'information





Local authorities are stepping up and will support your quest

ilink Kommunikationssysteme GmbH

Betrieb der HCL-Anwendungen
'HCL Sametime' und 'HCL Verse'
auf Basis 'HCL Domino'

IONOS

zoom



UBIKA WAAP Gateway





collab.cloud is moving to IONOS



What makes the IONOS Cloud data sovereign?

- Locations and jurisdiction: Headquartered in Germany, IONOS operates all services under German jurisdiction. Your data remains within German territory* – foreign intelligence services and third countries have no access. This gives you complete digital sovereignty and maximum legal certainty.
- Open source standards: IONOS consistently relies on open technologies and avoids vendor lock-in. You retain full transparency and control over your data and infrastructure.
- Verified security: IONOS is regularly audited and certified by the government, including C5 certification, ISO 27001 and BSI IT-Grundschutz certification.



Security and privacy driven vendors..

Trust and transparency powered by open source

An open source codebase enables the security of Bitwarden products to be easily audited by independent security researchers, notable security firms, and the Bitwarden community.

Open-Source-Standards: IONOS setzt konsequent auf offene Technologien und vermeidet Vendor Lock-in. Sie behalten volle Transparenz und Kontrolle über Ihre Daten und Infrastruktur.

We believe in the power of open source

Transparency is the only way to earn the trust of our community

All Proton apps are open source and have been independently audited and verified by third-party experts. Anyone can see and verify that our apps do what we claim.



Security and privacy driven vendors..

and often: Choice of deployment

- Hyperscale Cloud
- local Cloud
- Sovereign Clouds
- **on premises**

 HCL Verse

 HCL Notes

 HCL Domino

 HCL Sametime

 HCL Connections

 HCL Nomad

 HCL Domino Leap



Cloud or self-host password manager, secure file send, authenticator and more

Deploy fast and efficiently in the US or EU cloud, or host your Bitwarden organization on-premises for maximum privacy and control over your environment



Simple, encrypted solutions to protect your business
Advanced protection for your company's emails, calendars, passwords, network, and more with our suite of secure business apps.

Swiss-based offering



End-to-end encrypted exchange of messages, calls, and files for businesses, military, authorities, and individuals – GDPR-compliant and developed in Switzerland.



Proton in the News with a current case

BY MOLLY QUELL

Updated 11:26 AM CEST, May 15, 2023

Share

THE HAGUE, Netherlands (AP) — The [International Criminal Court](#)'s chief prosecutor has lost access to his email, and his bank accounts have been frozen.

The Hague-based court's American staffers have been told that if they travel to the U.S. they risk arrest.

Some nongovernmental organizations have stopped working with the ICC and the leaders of one won't even reply to emails from court officials.

Those are just some of the hurdles facing court staff since U.S. President Donald Trump [in February slapped sanctions on its chief prosecutor](#), Karim Khan, according to interviews with current and former ICC officials, international lawyers and human rights advocates.

<https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>

American staffers at the organization, like Iverson, have been warned by its attorneys that they risk arrest if they return home to visit family, according to ICC officials. Six senior officials have left the court over concerns about sanctions.

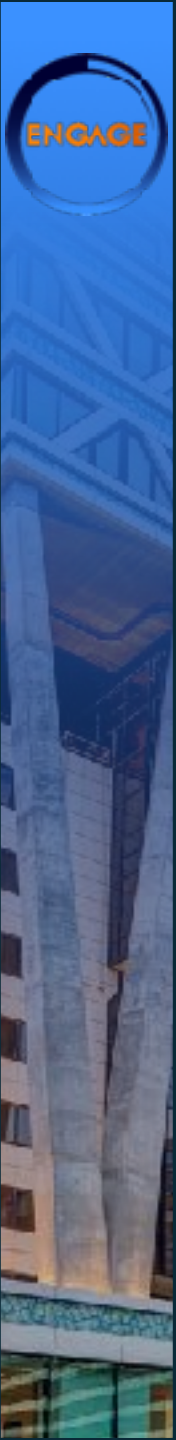
One reason the the court has been hamstrung is that it relies heavily on contractors and non-governmental organizations. Those businesses and groups have curtailed work on behalf of the court because they were concerned about being targeted by U.S. authorities, according to current and former ICC staffers.

Microsoft, for example, cancelled Khan's email address, forcing the prosecutor to move to Proton Mail, a Swiss email provider, ICC staffers said. His bank accounts in his home country of the U.K. have been blocked.

Microsoft did not respond to a request for comment.

Staffers at an NGO that plays an integral role in the court's efforts to gather evidence and find witnesses said the group has transferred money out of U.S. bank accounts because they fear it might be seized by the Trump administration.

Senior leadership at two other U.S.-based human rights organizations told the AP that their groups have stopped working with the ICC. A senior staffer at one told the AP that employees have stopped replying to emails from court officials out of fear of triggering a response from the Trump administration.

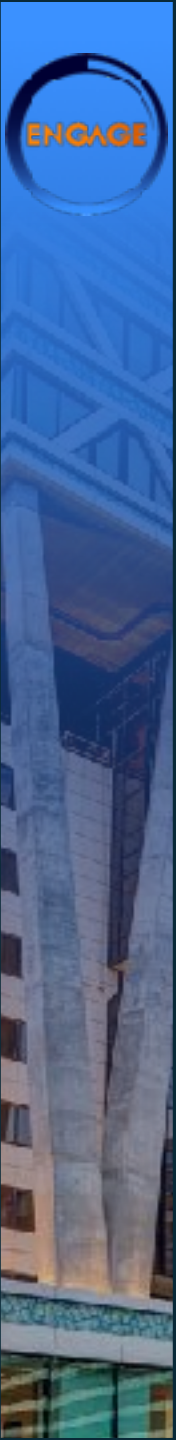


Important to remember

Google, Microsoft, AWS et al do report how many data requests they had to “fulfil”

- <https://transparencyreport.google.com/user-data/overview>
- <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data#tab-requests-for-enterprise-customer-data>
- https://www.amazon.com/gp/help/customer/display.html?ref_hp_left_v4_sib&nodeId=GYS DRGWQ2C2CRYEF
- https://d1.awsstatic.com/Security/pdfs/Amazon_AWS_Information_Request_Report_H2_2024.pdf

I expect a very high rise of such requests for 2025...

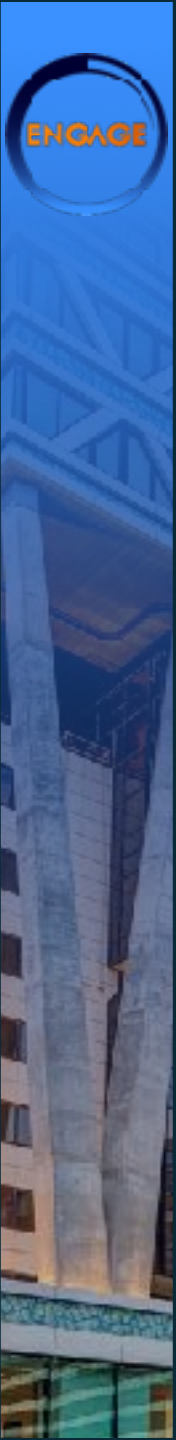


Checklist for companies

Monitoring of political developments

Closely follow political developments in the US and their impact on the EU-US Data Privacy Framework.

We will keep you informed of all important developments, but the websites of data protection authorities and professional associations also often have helpful information available.

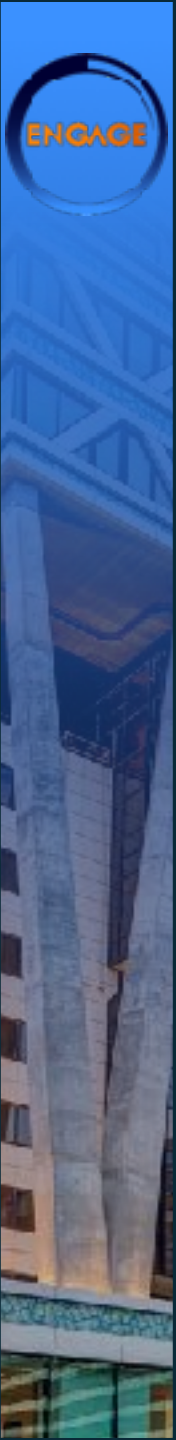


Checklist for companies

Use of EU servers

Check the possibility of using EU servers from your US cloud providers to reduce the risk of data transfer to the US. Make sure that the cloud provider gives clear contractual assurances that no data transfers to the US will take place.

This might not prevent the “handing over” of data because of a government request, but will make it more complicated.



Checklist for companies

Conclude EU Standard Contractual Clauses (SCC)

Conclude EU Standard Contractual Clauses with the cloud providers and conduct a Transfer Impact Assessment.

Document all steps and results of the TIA to be able to demonstrate that you have taken appropriate action in the event of a review by data protection authorities.



Checklist for companies

Prepare an exit strategy

Have an exit strategy in place for your U.S. cloud providers to respond quickly in the event of a suspension of the Privacy Framework.

Identify alternative cloud providers and assess their data protection measures. If the risk is particularly high, it's worth creating a detailed plan for switching to another provider, including timelines, responsibilities, and communication strategies.

"If Europe wants to tax our companies, they don't get to use them. Simple," President Trump declared — threatening a full suspension of U.S. digital services in Europe in response to the proposed EU Digital Tax.

Services at risk include:

- Cloud: AWS, Azure, Google Cloud
- Comms: Microsoft 365, Zoom, Slack
- AI Tools: OpenAI, Anthropic, GitHub Copilot
- Payments: Stripe, PayPal, Visa APIs
- Infra: CDNs, DNS, App Stores

The EU has declared a "Digital Emergency", urging immediate migration to European providers and strategic tech alliances with Japan and South Korea.

🏢 Cross-border M&A impact? Massive.

🔍 New targets? Local cloud, AI, infrastructure firms.

📊 Valuations could shift overnight.

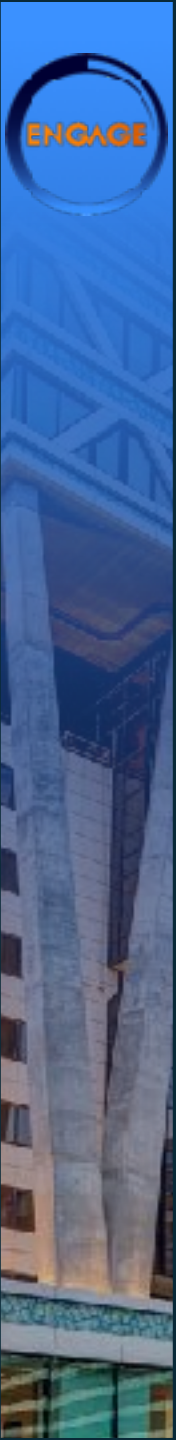
Digital sovereignty just became a boardroom priority.

👉 Let's hope it never comes to this...

[#MergersAndAcquisitions](#) [#AprilFools](#) [#DigitalSovereignty](#) [#smartmerger](#)

**BREAKING: U.S. TO HALT ALL
DIGITAL SERVICES TO
EUROPE — 'THE CLOUD
GOES DARK'**





Checklist for companies

Regular review and adaptation of data protection measures

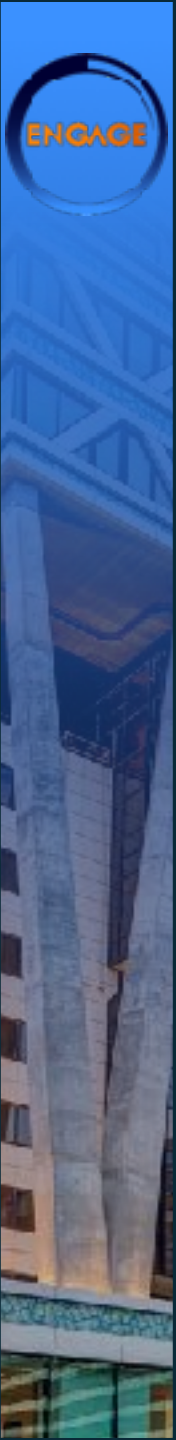
Regularly review and update your data protection measures to ensure they comply with current legal requirements and best practices.

If necessary, your own technical and organisational measures can also reduce the risks of third-country transfers. Adapt your measures as the political or legal environment changes, and ensure that your data protection strategy is flexible enough to respond to unforeseen developments.



References

- 1) EU Data Protection Directive
<https://short.wannesrams.com/bqfO1v>
<https://short.wannesrams.com/Y5cVf4>
- 2) World Economic Forum
<https://short.wannesrams.com/28Cvb3>
- 3) Safe Harbour agreement
<https://short.wannesrams.com/5Ymx7f>
- 4) FISA 1881a
<https://short.wannesrams.com/H2eUDR>
- 5) 12.333
<https://short.wannesrams.com/yZujji>
- 6) PPD-28
<https://short.wannesrams.com/VvpIKI>
- 7) EU Charter of Fundamental Rights
<https://short.wannesrams.com/ANp8SI>
- 8) Data Privacy Framework
<https://short.wannesrams.com/dp0Rfm>



Politics on the hook of Microsoft

Politics on the hook of Microsoft

The Microsoft Dilemma

- Trailer: <https://www.youtube.com/watch?v=9Nw2J1rXpSU>
- Full Movie: https://www.youtube.com/watch?v=_ZaDuinGf2o
- Interview Andrus Ansip, Kommissar für den digitalen Binnenmarkt
https://www.youtube.com/watch?v=f0ujMbkSK_8
- Controlling the government of India
<https://www.youtube.com/watch?v=qCXlr99jN4I>
- → Always use multiple vendors to never be dependent on a single one.