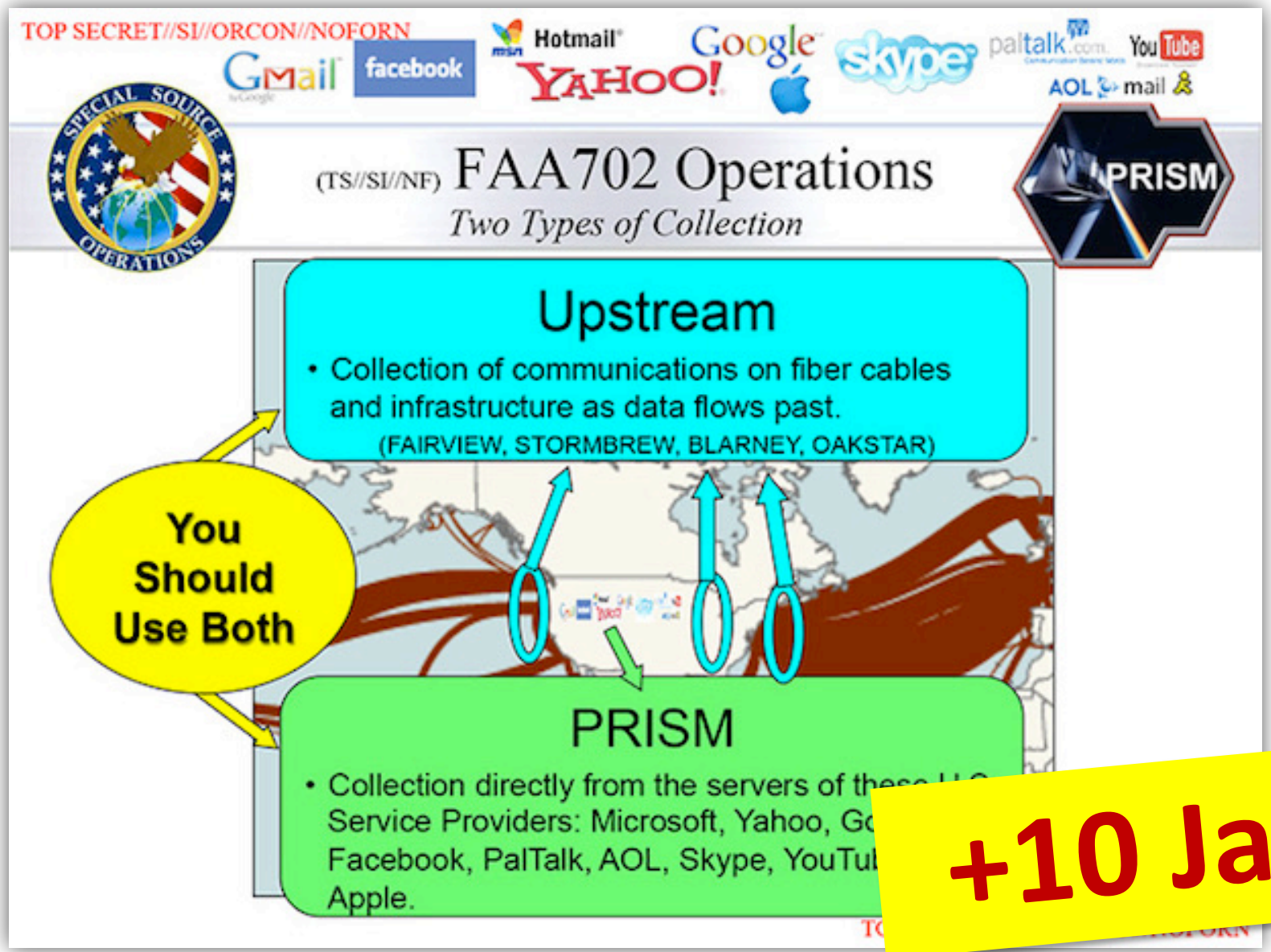
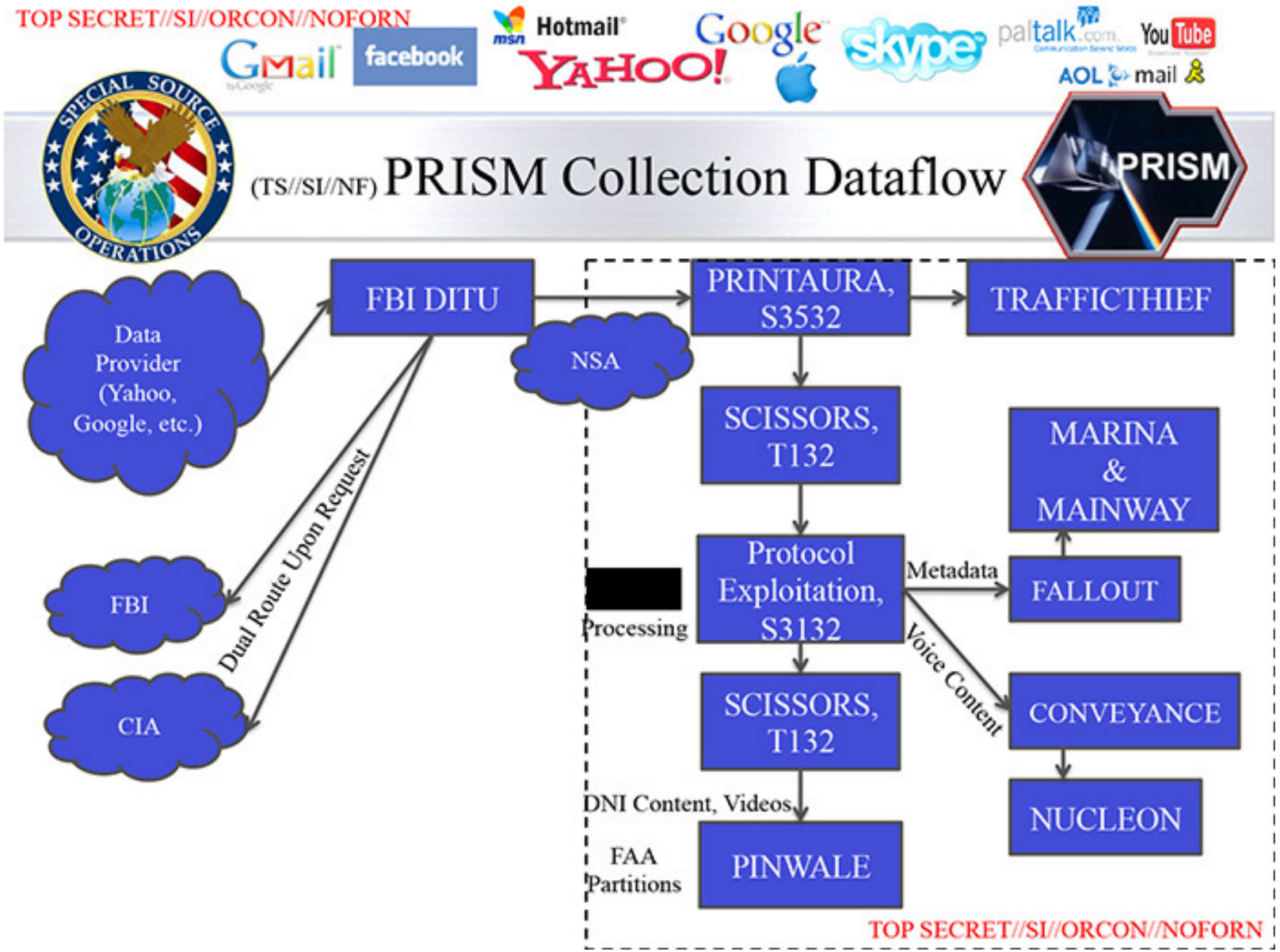
EU-US DATENTRANSFERS: WAY FORWARD?

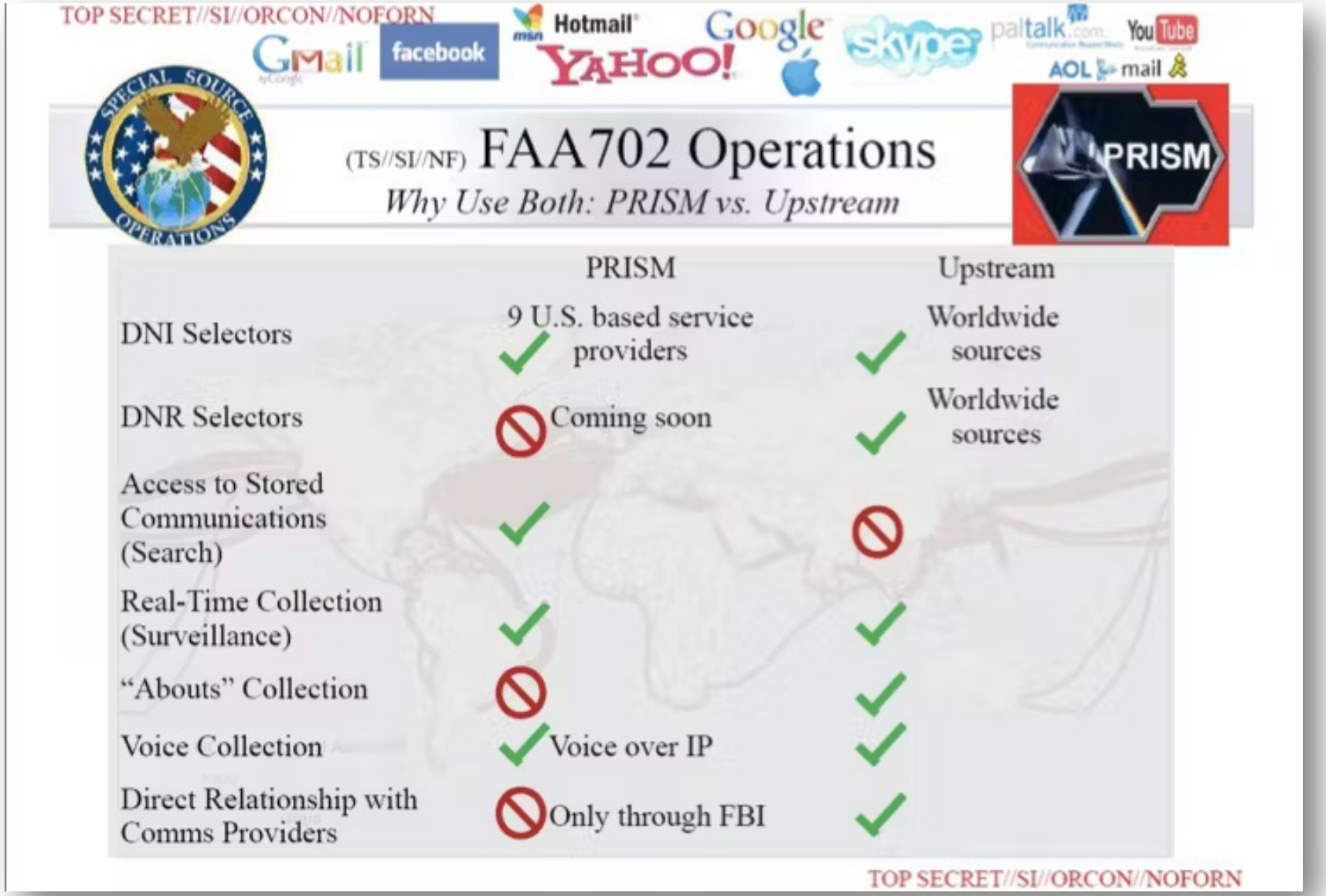
HINTERGRUND 1: US-RECHT



+10 Jahre

noyb

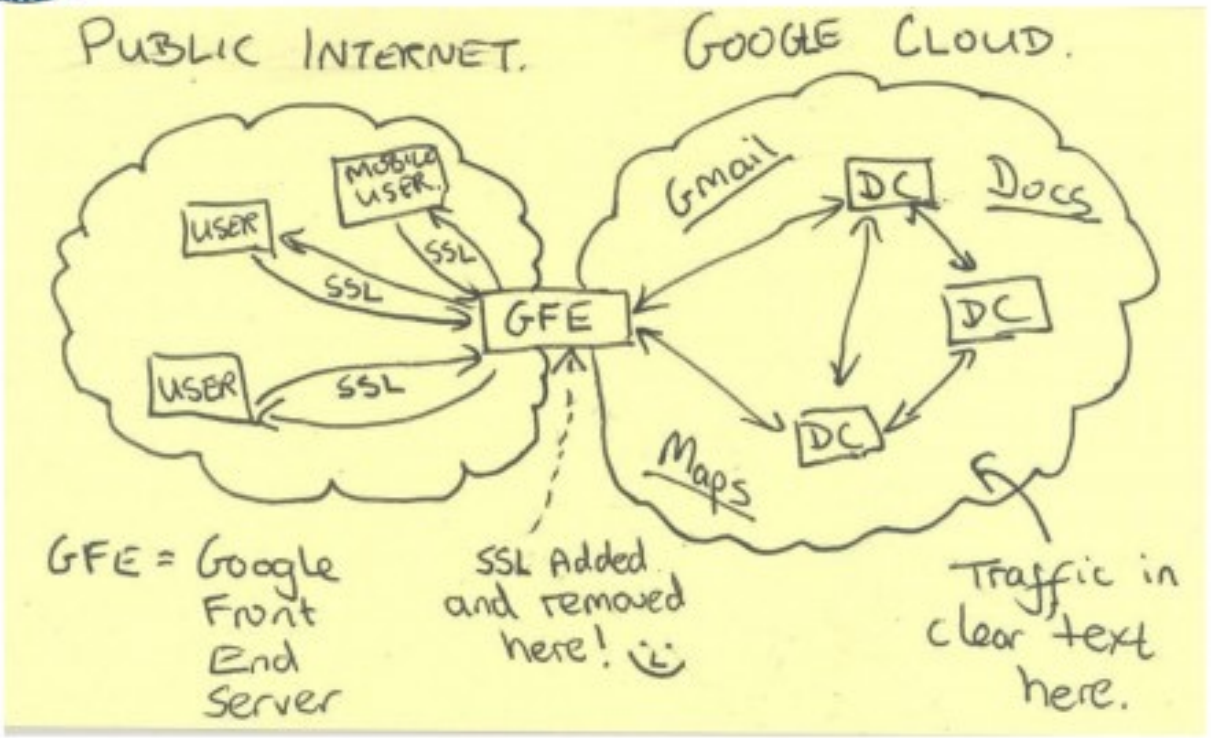

TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Dataflow
PRISM
Data Provider (Yahoo, Google, etc.)
FBI DITU
NSA
PRINTAURA, S3532
TRAFFICTHIEF
SCISSORS, T132
MARINA & MAINWAY
Protocol Exploitation, S3132
Metadata
FALLOUT
Processing
Voice Content
CONVEYANCE
SCISSORS, T132
NUCLEON
DNI Content, Videos
FAA Partitions
PINWALE
FBI
CIA
Dual Route Upon Request
TOP SECRET//SI//ORCON//NOFORN


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) FAA702 Operations
Why Use Both: PRISM vs. Upstream
PRISM
PRISM
Upstream
DNI Selectors
9 U.S. based service providers
Worldwide sources
DNR Selectors
Coming soon
Worldwide sources
Access to Stored Communications (Search)
Real-Time Collection (Surveillance)
"Abouts" Collection
Voice Collection
Voice over IP
Direct Relationship with Comms Providers
Only through FBI
TOP SECRET//SI//ORCON//NOFORN

noyb

noyb

Current Efforts - Google



FISA 702 (= 50 USC § 1881a)

- **Electronic Communication Service Provider (ECSP)**
- **“Foreign Intelligence Information“**

- **“Certification” für ein Jahr** *(„FISA Court“)*
  - Minimizing / Targeting procedures (US persons)
- **“Directive“ an den ECSP**
  - API (?)





HINTERGRUND 2: US-RECHT

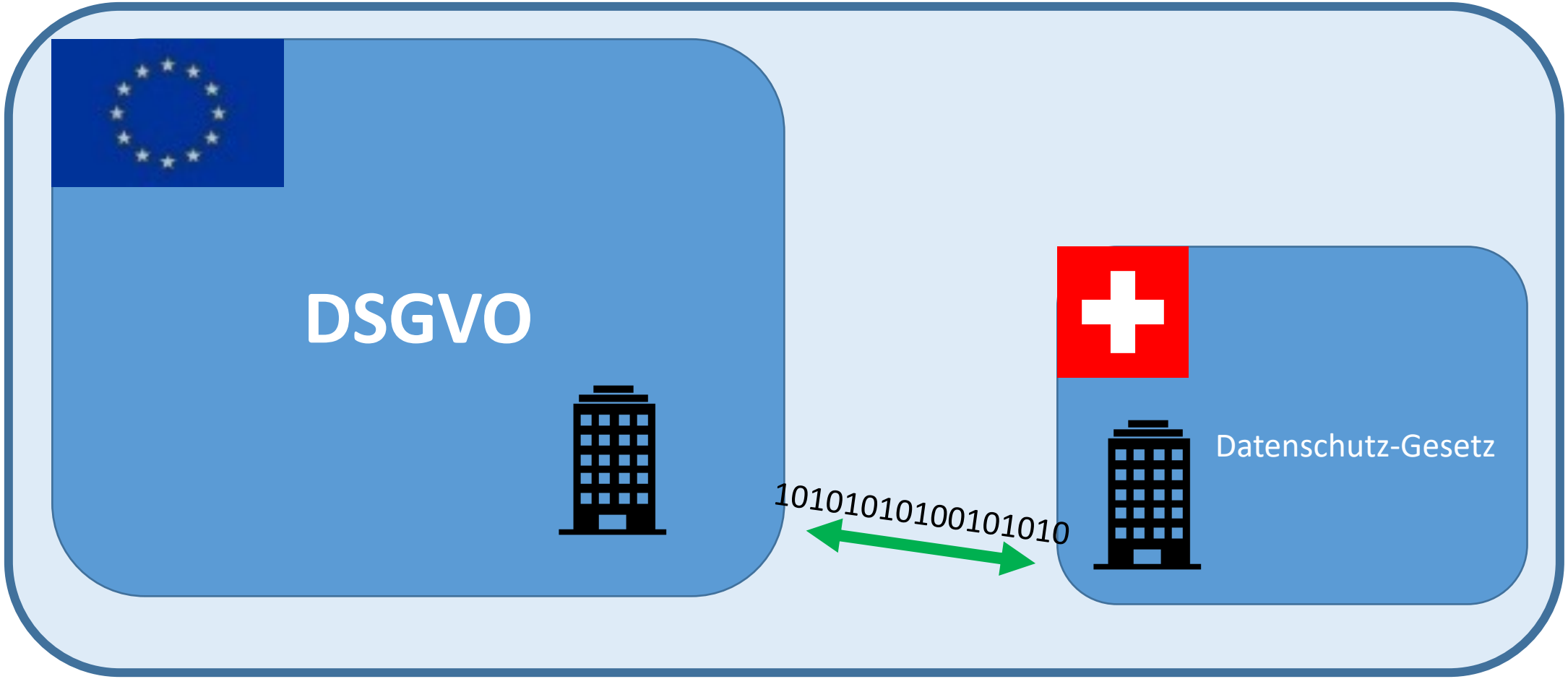
DATENÜBERMITTLUNG

- **Allgemeine Regel:** Exportverbot für personenbezogene Daten
- **Ausnahme:** "Notwendige Übermittlungen", nicht-strukturell (Art 49)

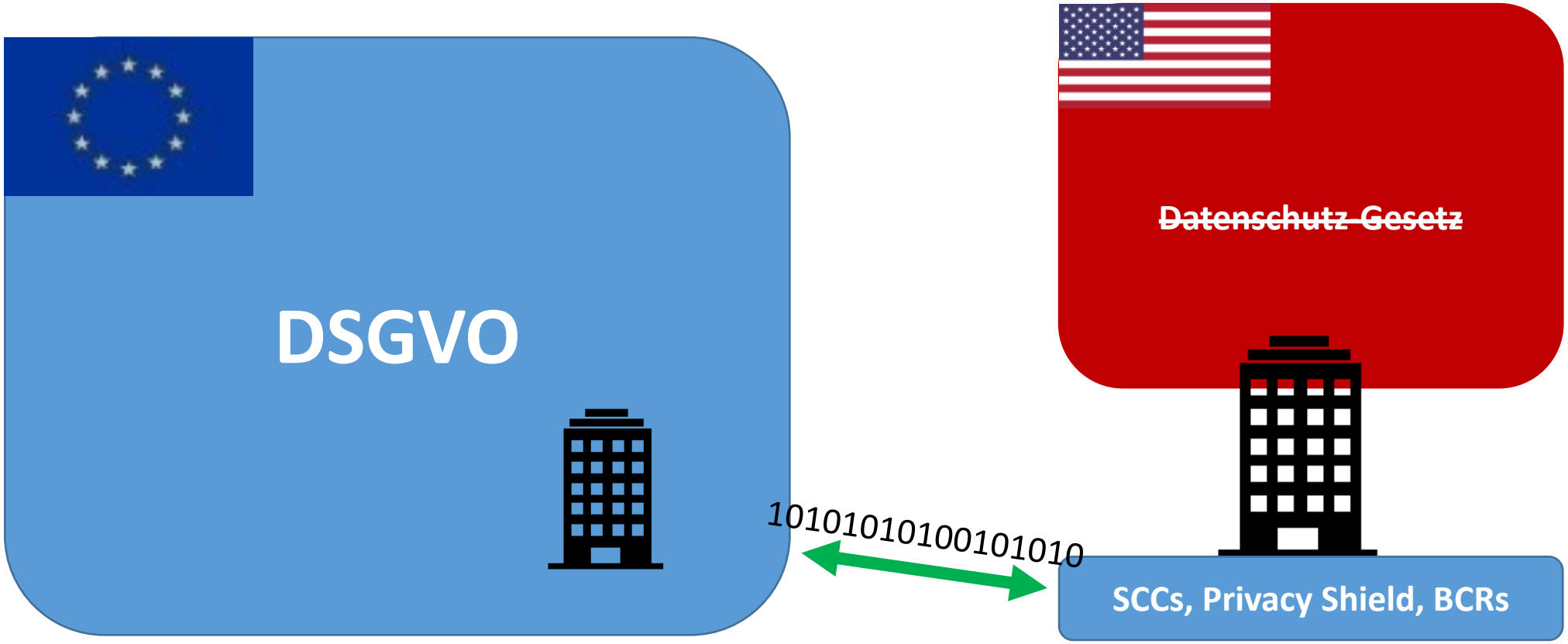
- **Outsourcing**:
  - Angemessenheit (Art 45)
  - Standardvertragsklausel/Musterklauseln (Art 46)
  - Verbindliche Unternehmensregeln (Art 47)

Ausweitung der DSGVO-Regeln in Drittländern

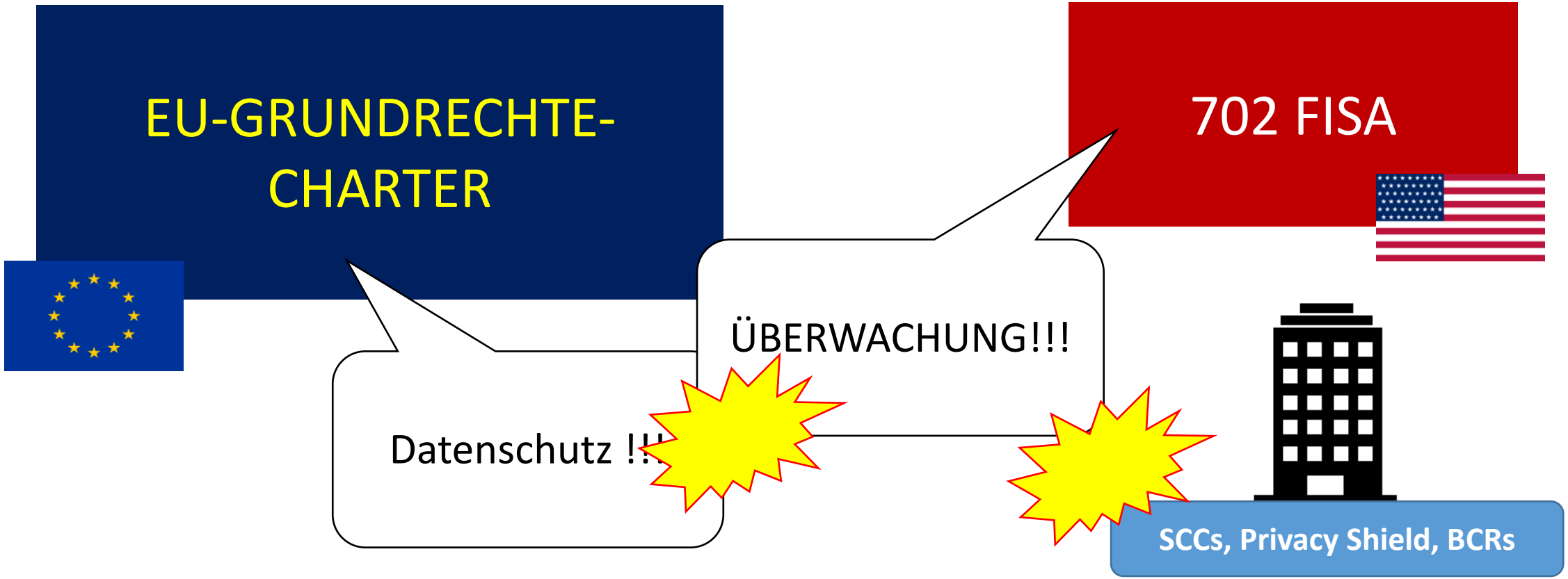
DATENSCHUTZ "BUBBLE": SCHWEIZ



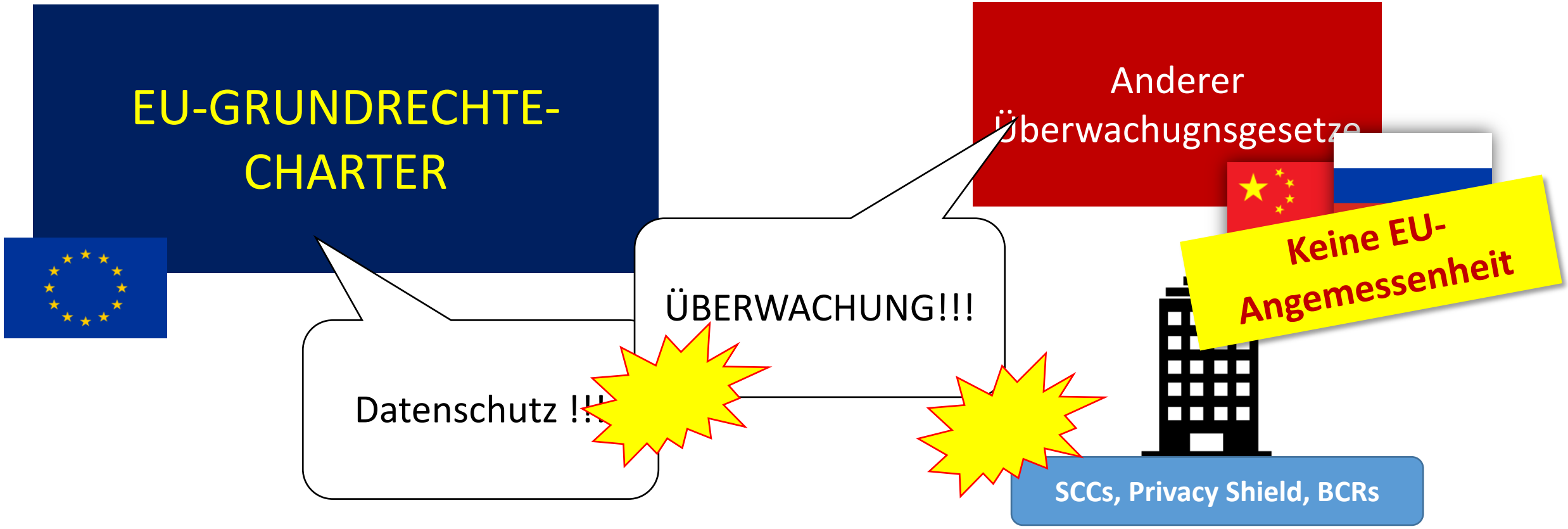
DATENSCHUTZ "BUBBLE": VERTRAG

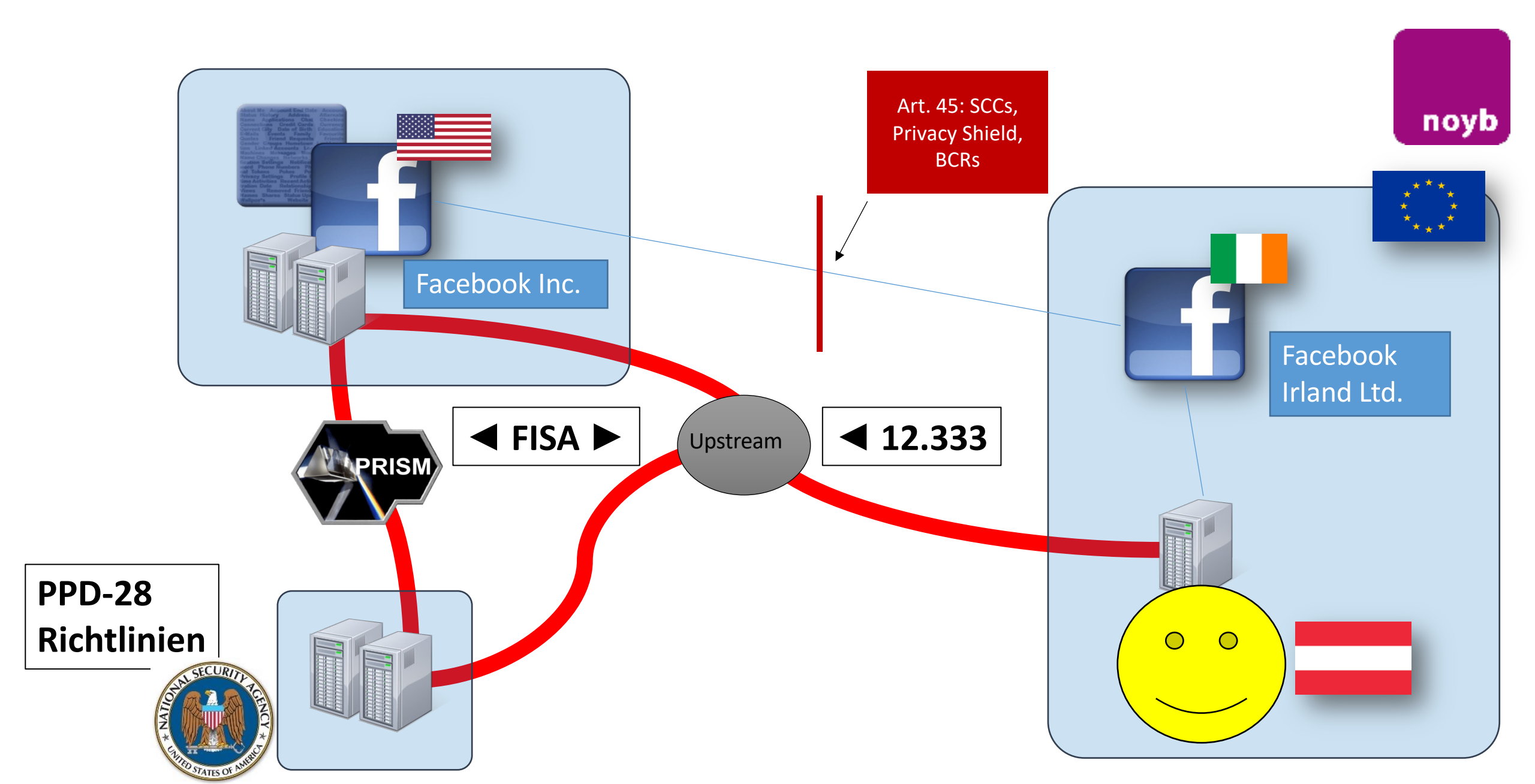


KONFLIKT DER RECHTSORDNUNGEN



KONFLIKT DER RECHTSORDNUNGEN




noyb
Art. 45: SCCs, Privacy Shield, BCRs
Facebook Inc.
Facebook Irland Ltd.
PRISM
◀ FISA ▶
Upstream
◀ 12.333
PPD-28 Richtlinien
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

EUGH: RECHTSPRECHUNG



noyb

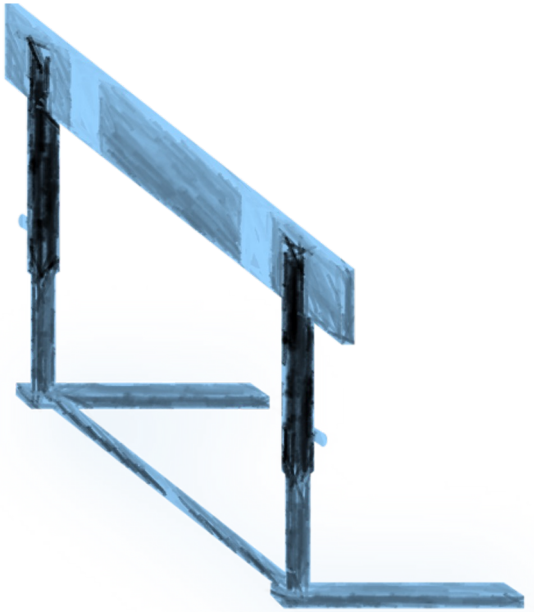
≈ DSGVO



Art 44-50 DSGVO

„der Sache nach gleich”

= GRC



GRC

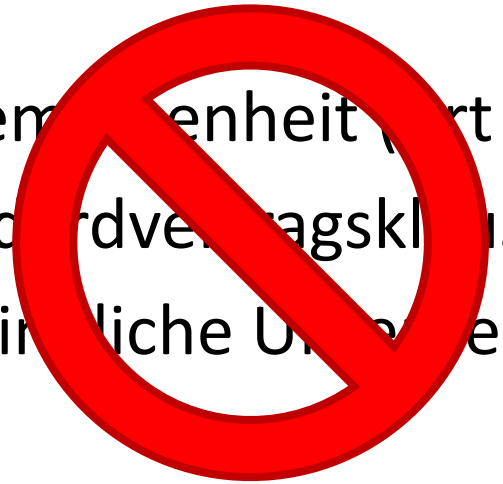
Art 7, 8 & 47

ERGEBNIS: PRAXIS

DATENÜBERMITTLUNGEN

- **Allgemeine Regel:** Exportverbot für personenbezogene Daten
- **Ausnahme:** "Notwendige Übermittlungen", nicht-strukturell (Art 49)

- **Outsourcing**:
  - Angem[illegible]enheit ([illegible]rt 45)
  - Stand[illegible]rdve[illegible]agskl[illegible]usel/Musterklauseln (Art 46)
  - Verbi[illegible]liche U[illegible]ehmensregeln (Art 47)

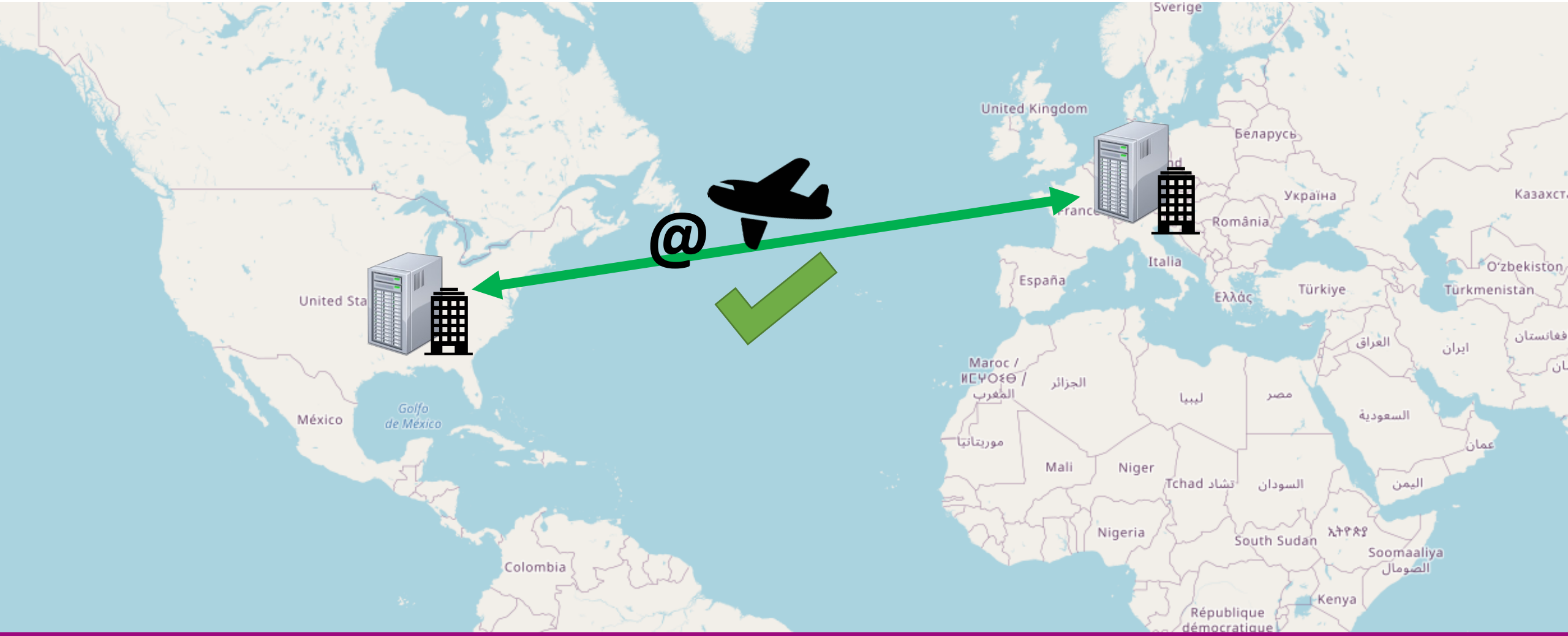


Ausweitung der DSGVO-Regeln in Drittländern

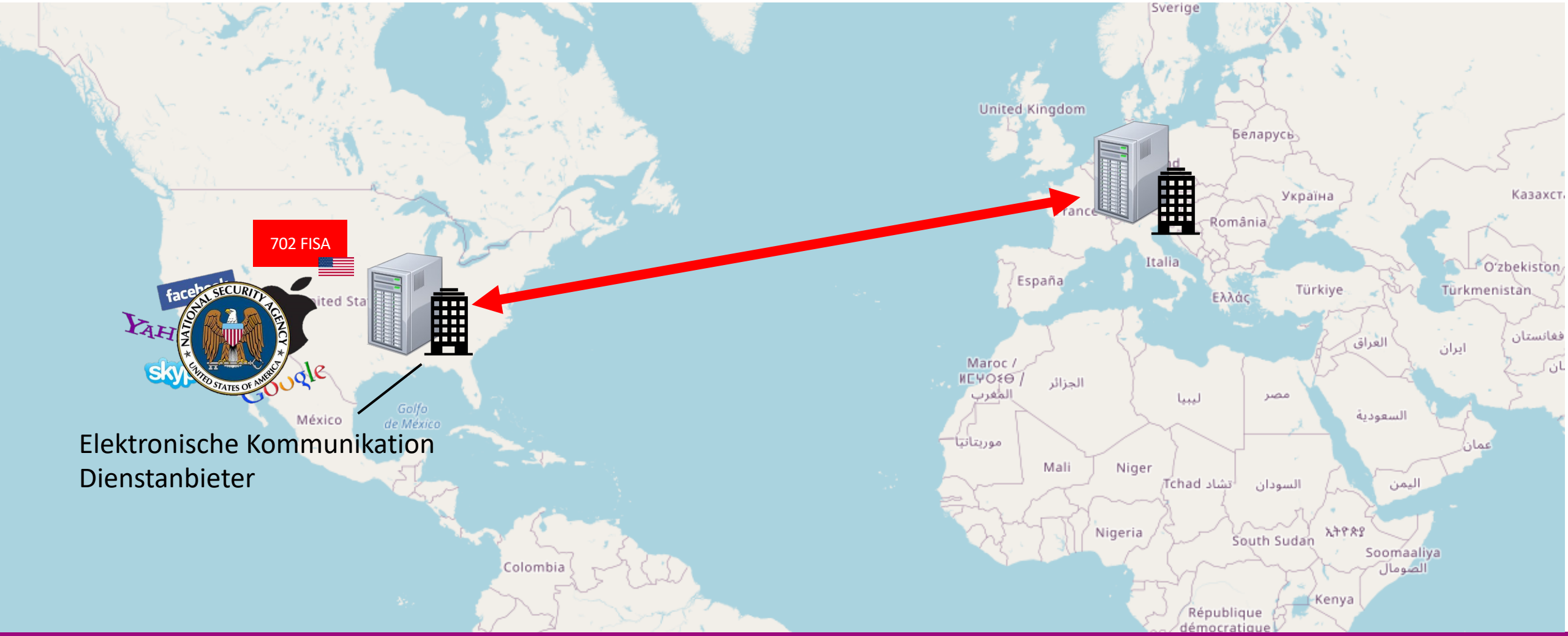
ÜBERMITTLUNGEN: NICHT PERSONENBEZOGEN



ÜBERMITTLUNGEN: NOTWENDIG

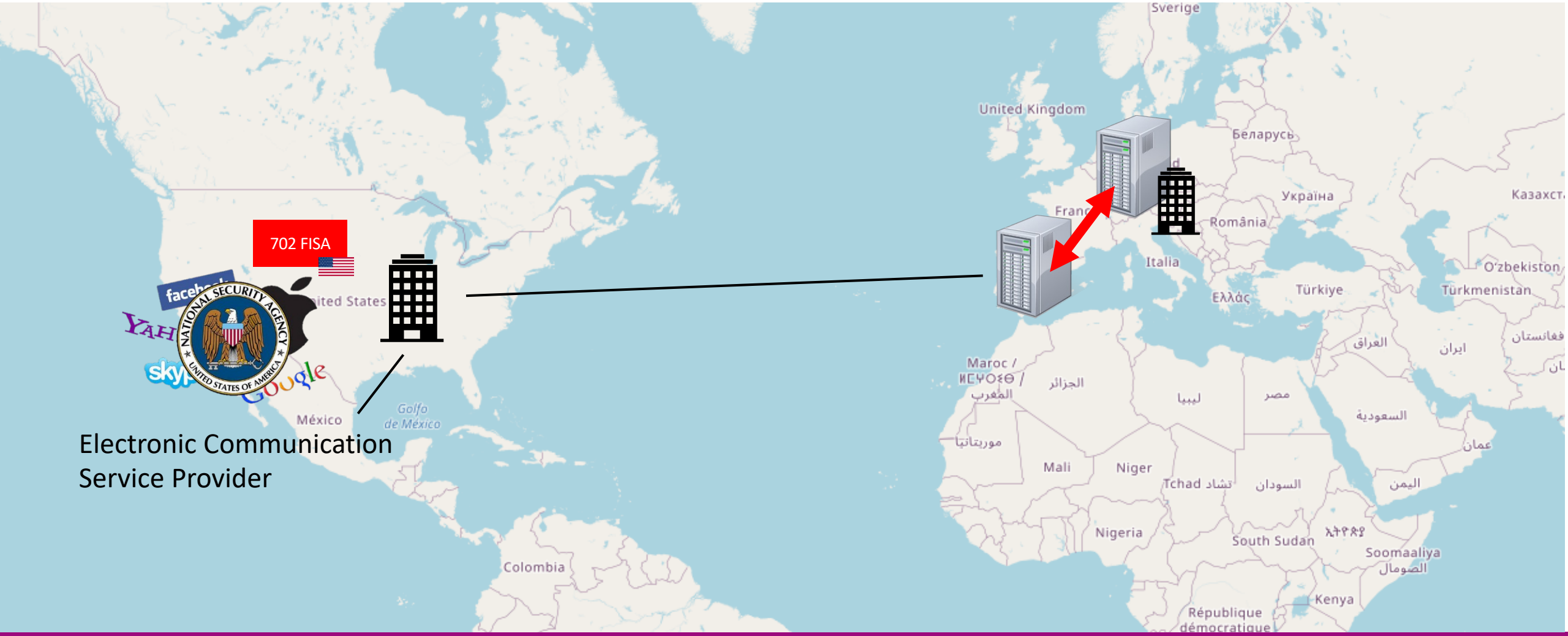


ÜBERMITTLUNG: “OUTSOURCING” (FISA)

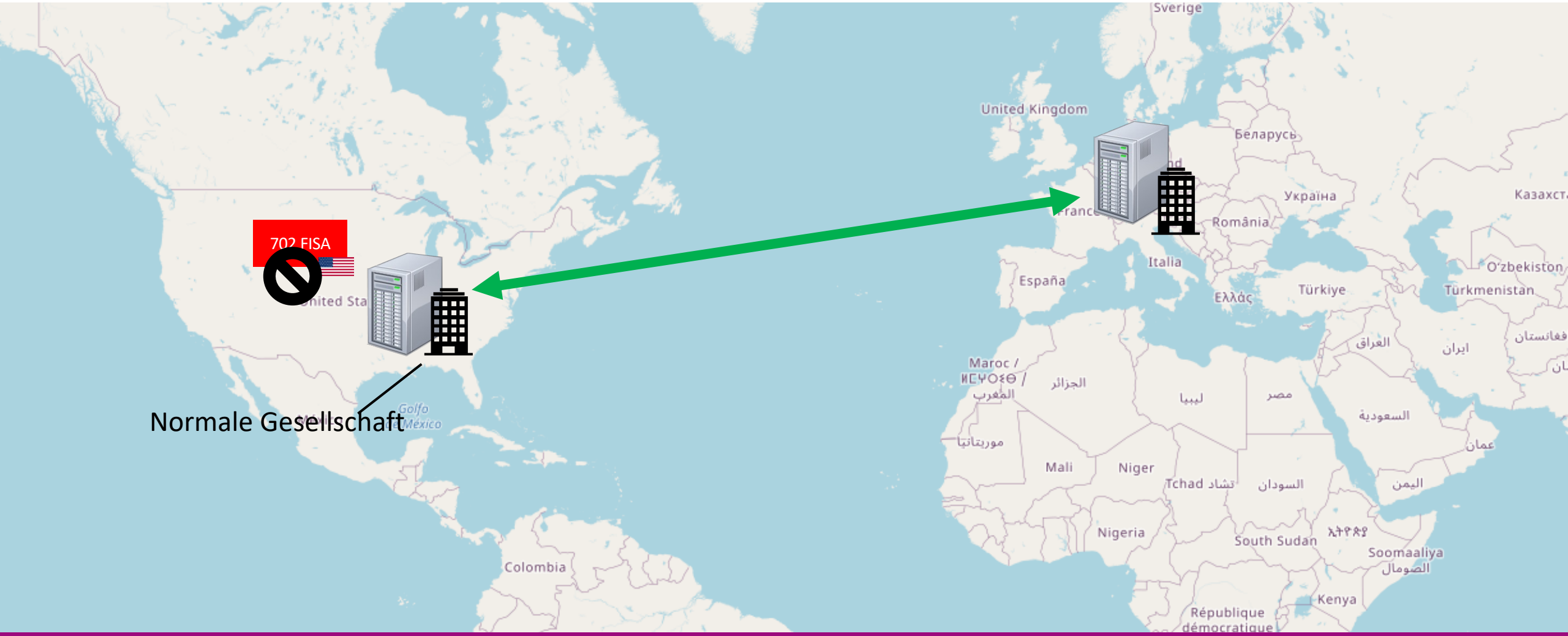


Elektronische Kommunikation Dienstanbieter

TRANSFERS: “OUTSOURCING” (FISA) - EU



ÜBERMITTLUNG: NICHT-FISA

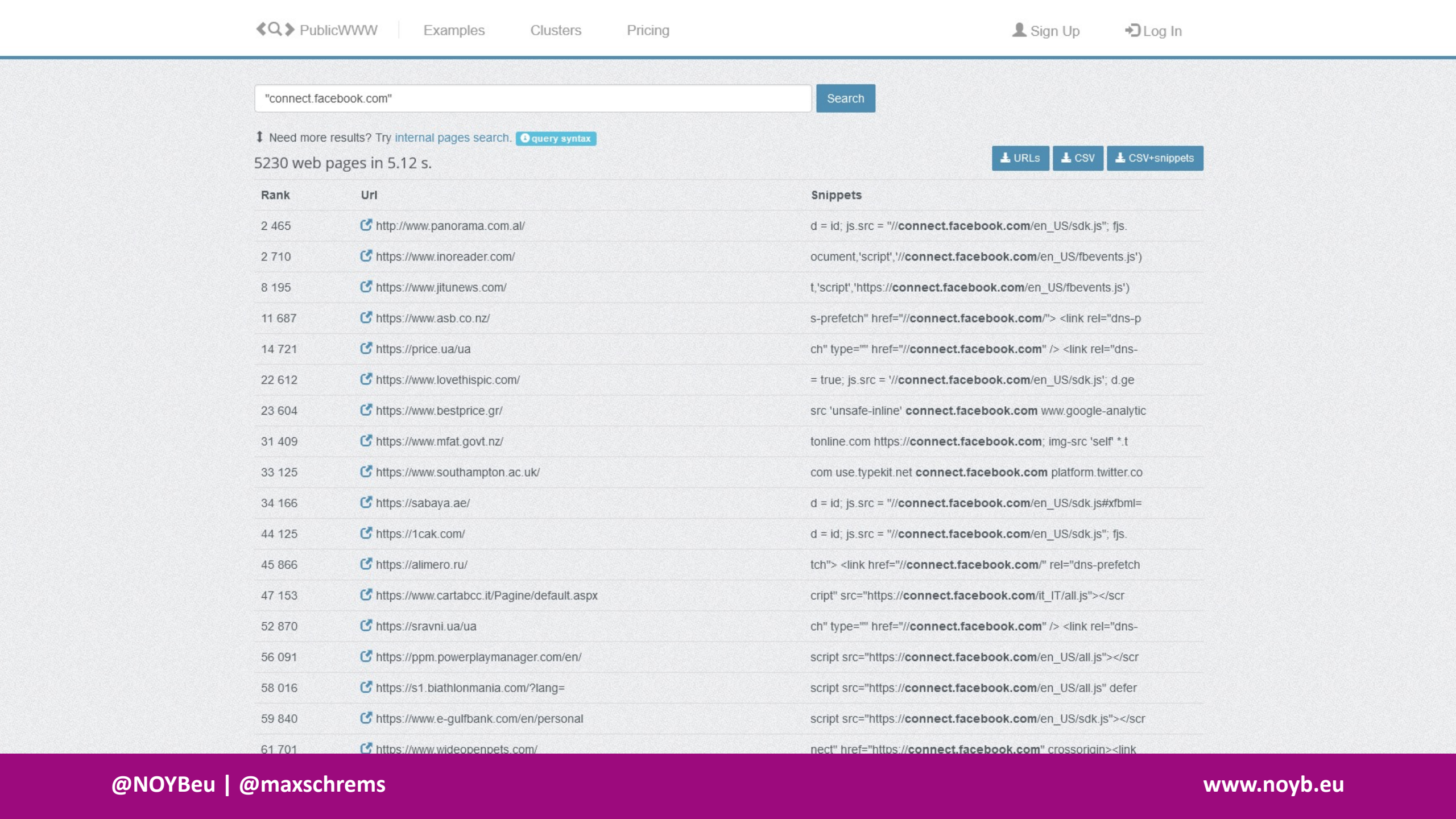


DURCHSETZUNG: 101 BESCHWERDEN

noyb






PublicWWW
Examples
Clusters
Pricing
Sign Up
Log In
"connect.facebook.com"
Search
Need more results? Try internal pages search.
query syntax
5230 web pages in 5.12 s.
URLs
CSV
CSV+snippets
Rank
Url
Snippets
2 465
http://www.panorama.com.al/
d = id; js.src = "//connect.facebook.com/en_US/sdk.js"; fjs.
2 710
https://www.inoreader.com/
ocument,'script','//connect.facebook.com/en_US/fbevents.js')
8 195
https://www.jitunews.com/
t,'script','https://connect.facebook.com/en_US/fbevents.js')
11 687
https://www.asb.co.nz/
s-prefetch" href="//connect.facebook.com/"> <link rel="dns-p
14 721
https://price.ua/ua
ch" type="" href="//connect.facebook.com" /> <link rel="dns-
22 612
https://www.lovethispic.com/
= true; js.src = '//connect.facebook.com/en_US/sdk.js'; d.ge
23 604
https://www.bestprice.gr/
src 'unsafe-inline' connect.facebook.com www.google-analytic
31 409
https://www.mfat.govt.nz/
tonline.com https://connect.facebook.com; img-src 'self' *.t
33 125
https://www.southampton.ac.uk/
com use.typekit.net connect.facebook.com platform.twitter.co
34 166
https://sabaya.ae/
d = id; js.src = "//connect.facebook.com/en_US/sdk.js#xfbml=
44 125
https://1cak.com/
d = id; js.src = "//connect.facebook.com/en_US/sdk.js"; fjs.
45 866
https://alimero.ru/
tch"> <link href="//connect.facebook.com/" rel="dns-prefetch
47 153
https://www.cartabcc.it/Pagine/default.aspx
cript" src="https://connect.facebook.com/it_IT/all.js"></scr
52 870
https://sravni.ua/ua
ch" type="" href="//connect.facebook.com" /> <link rel="dns-
56 091
https://ppm.powerplaymanager.com/en/
script src="https://connect.facebook.com/en_US/all.js"></scr
58 016
https://s1.biathlonmania.com/?lang=
script src="https://connect.facebook.com/en_US/all.js" defer
59 840
https://www.e-gulfbank.com/en/personal
script src="https://connect.facebook.com/en_US/sdk.js"></scr
61 701
https://www.wideopenpets.com/
nect" href="https://connect.facebook.com" crossorigin><link

noyb



GEGENARGUMENTE

1. Upsi, haben wir jetzt gelöscht!
2. Zusätzliche garantien
3. „Risikobasierter Ansatz“

LÖSUNG: „ZUSÄTZLICHE GARANTIEN“?

ERWGR 109

„…Die Verantwortlichen und die Auftragsverarbeiter sollten ermutigt werden, mit vertraglichen Verpflichtungen, die die Standard-Schutzklauseln ergänzen, zusätzliche Garantien zu bieten.“

ZUSÄTZLICHE GARANTIEN

- **Technisch**
  - Verschlüsselung („Transit“)
  - Verschlüsselung (Backups)
  - *Datenteilung…*
  - „Zero Knowledge“



- **Vertraglich**
  - Herausgabe
  - Informationen
  - „Widerstand“

Recht in Drittländern




Max Schrems
@maxschrems
The #Microsoft "supplementary measures" on #SchremsII / #FISA702 in a 5 minute legal bullsh*t analysis (powered by Microsoft PowerPoint)..
(free to copy/used - especially for any legal department)
• First, we are committing that we will challenge every government request for public sector or enterprise customer data – from any government – where there is a lawful basis for doing so. This strong commitment goes beyond the proposed recommendations of the EDPB.
• Second, we will provide monetary compensation to these customers' users if we disclose their data in response to a government request in violation of the EU's General Data Protection Regulation (GDPR). This commitment also exceeds the EDPB's recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.
We call these protections Defending Your Data, and we will begin adding them to our contracts with public sector and enterprise customers immediately.
Defending Your Data makes a substantial addition to our foundational privacy promises, and builds on the strong protections we already offer customers.
• We use strong encryption: We encrypt customer data with a high standard of encryption both when it is in transit and at rest. Encryption is a critical point in the draft EDPB recommendations. We do not provide any government with our encryption keys or any other way to break our encryption.
• We stand up for customer rights: We do not provide any government with direct, unfettered access to customer data. If a government demands customer data from us, it must follow applicable legal process. We will only comply with demands when we are clearly compelled to do so. Our first step is always to attempt to re-direct such orders to customers or to inform them, and we routinely deny or challenge orders when we believe they are not legal.
• We are transparent: We have, for many years, published information about government demands for customer data. We sued the U.S. government over the ability to disclose more data about the national security orders we receive seeking customer data and reached a settlement enabling us to do so. As a result, twice a year, we disclose more detailed information about these national security orders across all our businesses (consumer, enterprise, and public sector), in addition to our regular Law Enforcement Request Report.
• We have a track record of legal success. We have more experience than any other company going to court to establish the limits of government surveillance orders, and we have even taken one case to the U.S. Supreme Court. Our efforts have provided customers with greater transparency and stronger protections. No commitment to challenge access orders can assure victory, but we feel good about our record of success to date.
Duty under Article 6(1)(c) – if there is no duty to comply (illegal request) then you can't provide the data... Challinging it is the logical consquence - nothing new...
Duty under Article 82 GDPR, but without all the limits (no class action, burden of proof on the user, etc) that Microsoft put into it's contract and that would actually limit (!) data subejcts' (third party) rights!
Required under Article 32 GDPR - big News.
Yeah, so Microsoft complies with FISA 702 which is the „legal process".
Yeah, so you even disclose that you provided the data of 28.500 to 29.998 accounts in 2019.
Congrats, good job on SCA – but frankly overturend by the Cloud Act and irrelevant when this is about FISA 702.


facebook®


Google
DEAR NSA:
PLEASE
KEEP OUT!

noyb

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉ

dsb
Republik Österreich
Datenschutz
behörde

EDPS
EUROPEAN DATA PROTECTION SUPERVISOR
The EU's independent data protection authority



AUTORITEIT
PERSOONSGEGEVENS

LÖSUNG: RISIKOBASIERTER ANSATZ

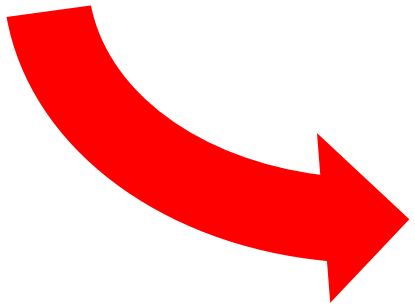
RISIKO IN DER DSGVO

- Verarbeitungsverzeichnis (Art 30)
- Datensicherheit (Art 32)
- Data Breaches (Art 33, 34)
- …



RISIKO IN DER DSGVO

- Verarbeitungsverzeichnis (Art 30)
- Datensicherheit (Art 32)
- Data Breaches (Art 33, 34)
- …



Generelles Prinzip der DSGVO?!

noyb



noyb

NEUE „LÖSUNG“: PRIVACY SHIELD

+ EU-US Framework“





WIRTSCHAFTLICH: “TADPF“ PRINCIPLES

II. PRINCIPLES

1. NOTICE

a. An organization must inform individuals about:

i. its participation in the EU-U.S. DPF and provide a link to, or the web address for, the Data Privacy Framework List,

ii. the types of personal data collected and, where applicable, the U.S. entities or U.S. subsidiaries of the organization also adhering to the Principles,

iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the EU-U.S. DPF,

iv. the purposes for which it collects and uses personal information about them,

v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,

vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

vii. the right of individuals to access their personal data,

viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by DPAs, (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,

x. being subject to the investigatory and enforcement powers of the FTC, the DOT or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,[5]

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

[5] See, e.g., section (c) of the Recourse, Enforcement and Liability Principle

b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

2. CHOICE

a. An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

b. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

c. For sensitive information (*i.e.*, personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

a. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

b. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii)

ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. SECURITY

a. Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

a. Consistent with the Principles, personal information must be limited to the information that is relevant for the purposes of processing.[6] An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

b. Information may be retained in a form identifying or making identifiable[7] the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

[6] Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.

[7] In this context, if, given the means of identification reasonably likely to be used (considering, among other things, the costs of and the amount of time required for identification and the available technology at the time of the processing) and the form in which the data is retained, an individual could reasonably be identified by the organization, or a third party if it would have access to the data, then the individual is "identifiable."

6. ACCESS

a. Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7. RECOURSE, ENFORCEMENT AND LIABILITY

a. Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum such mechanisms must include:

i. readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

ii. follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

iii. obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

b. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the EU-U.S. DPF. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to

such authorities with regard to the investigation and resolution of complaints.

c. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

d. In the context of an onward transfer, a participating organization has responsibility for the processing of personal information it receives under the EU-U.S. DPF and subsequently transfers to a third party acting as an agent on its behalf. The participating organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

e. Where an organization becomes subject to a FTC or court order based on [illegible] compliance or an order from a U.S. statutory body (e.g., FTC or DOT) listed in the Principles or in a future annex to the Principles that is based on noncompliance, the organization shall make public any relevant EU-U.S. DPF-related sections of any compliance or assessment report submitted to the FTC court or U.S. statutory body, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by participating organizations. The FTC and the DOT will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

noyb

WIRTSCHAFTLICHE DATENNUTZUNG





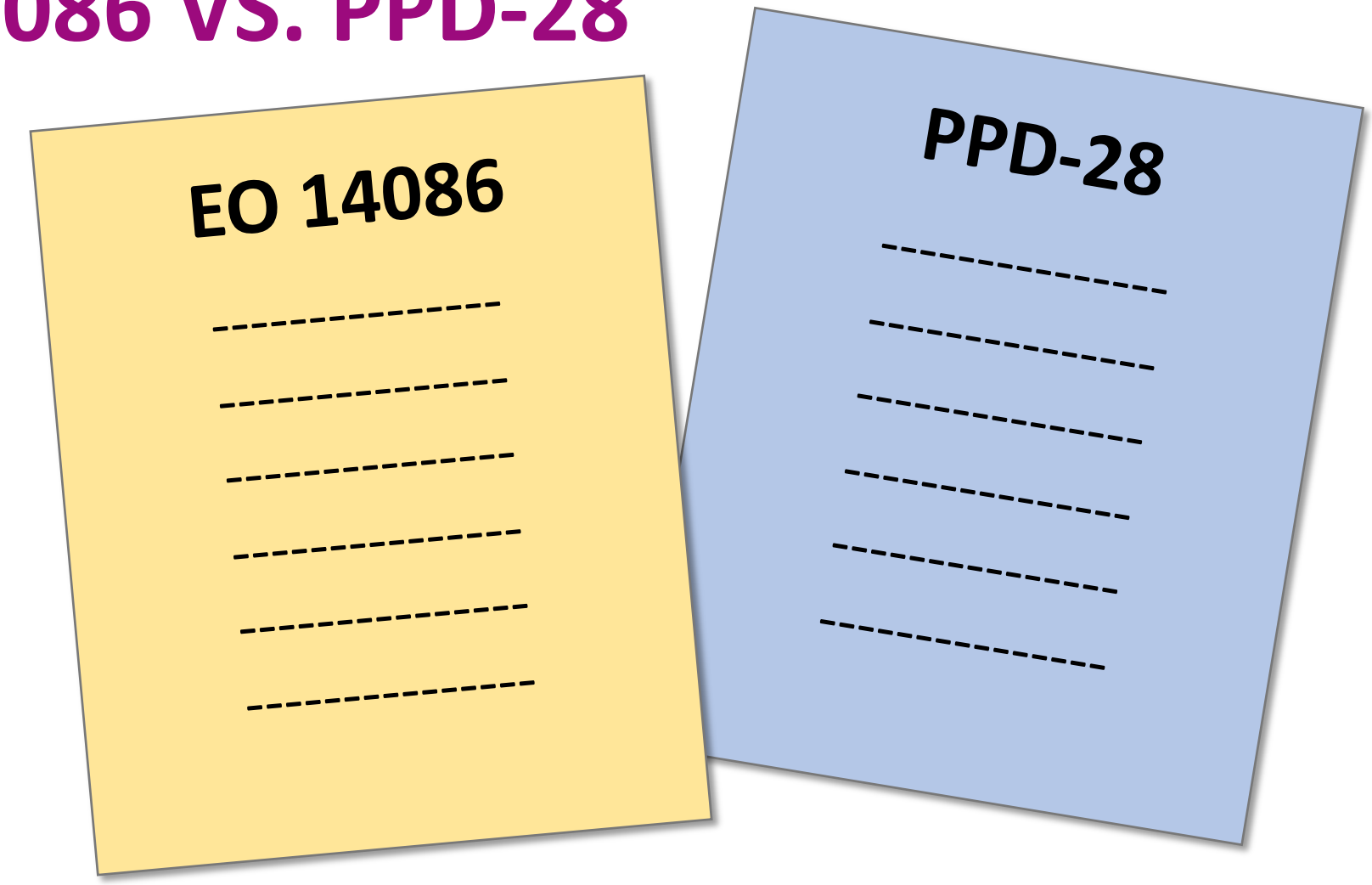
Consent (or other legal basis)	Opt-Out (only sharing, change of purpose)
Necessary	Relevant
Full Access	Limited Access

...

STAAT: “NEUE” EXECUTIVE ORDER



EO 14086 VS. PPD-28



EO 14086 VS. PPD-28

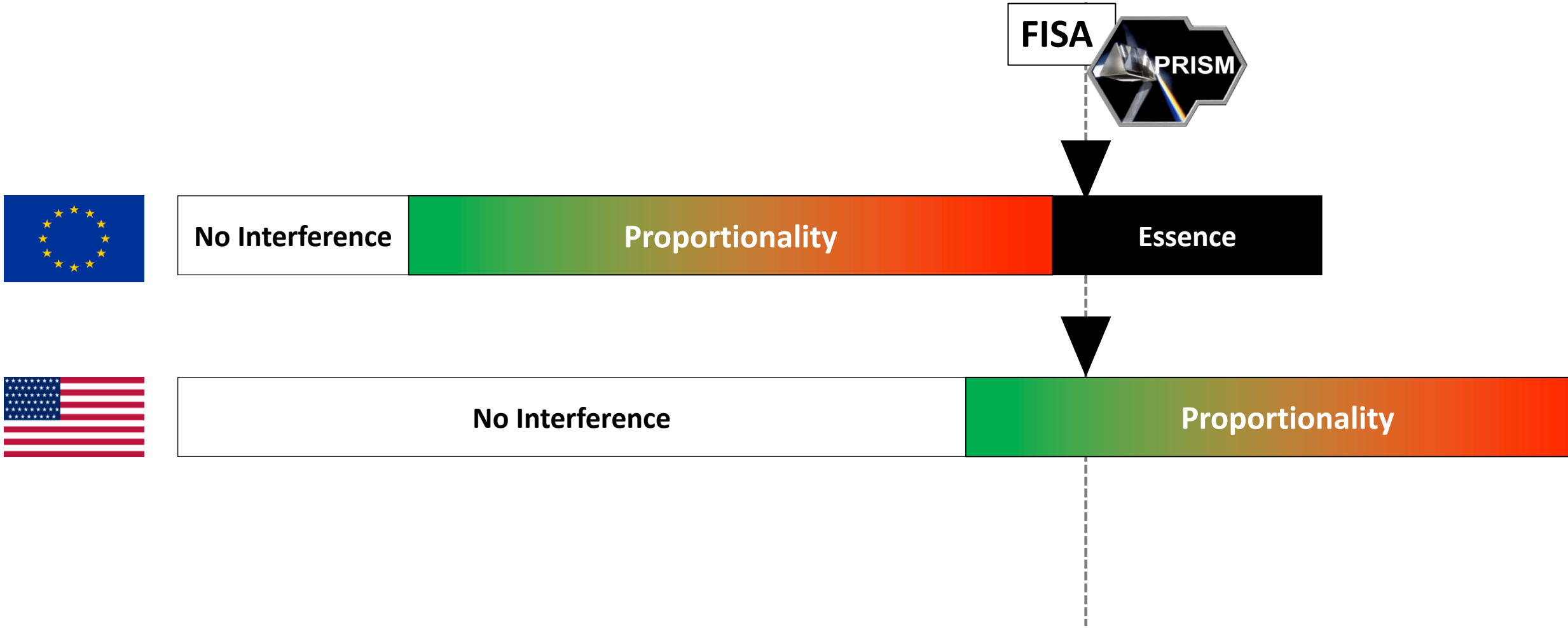
- **Biden EO 14086 hat im Prinzip die gleichen Beschränkungen wie die „alte“ Obama PPD-28**

- **Teilweise klarere Formulierungen**

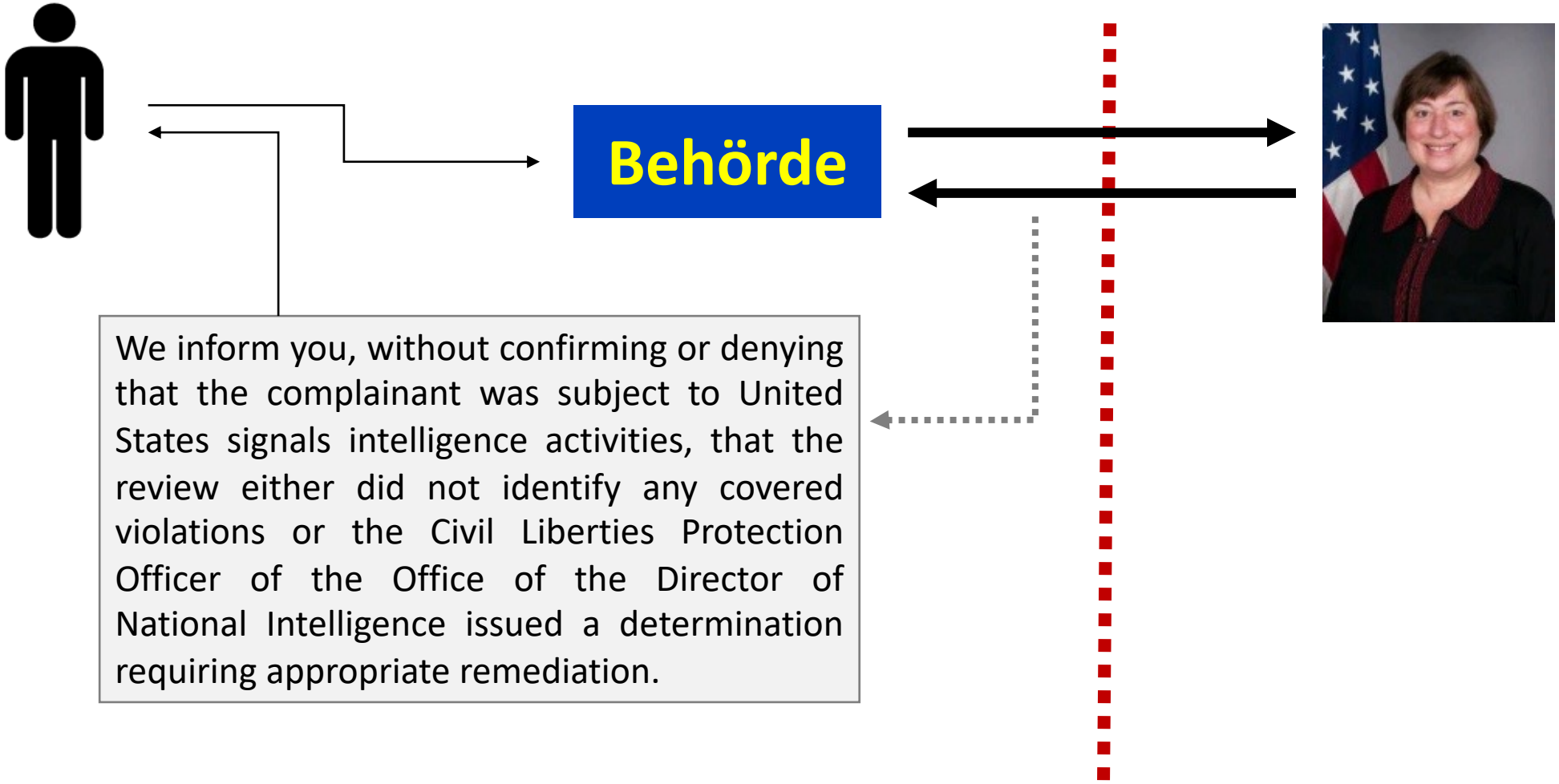
- **Zwei weitere Gründe für Massenüberwachung**
  (z.B. „health crisis“ und „climate change“)

- **„*Notwendig*“ ist jetzt „*Notwendig und Verhältnismäßig*“**
  (soll die Einhaltung von Artikel 7, 8 und 52 GRC sicherstellen)

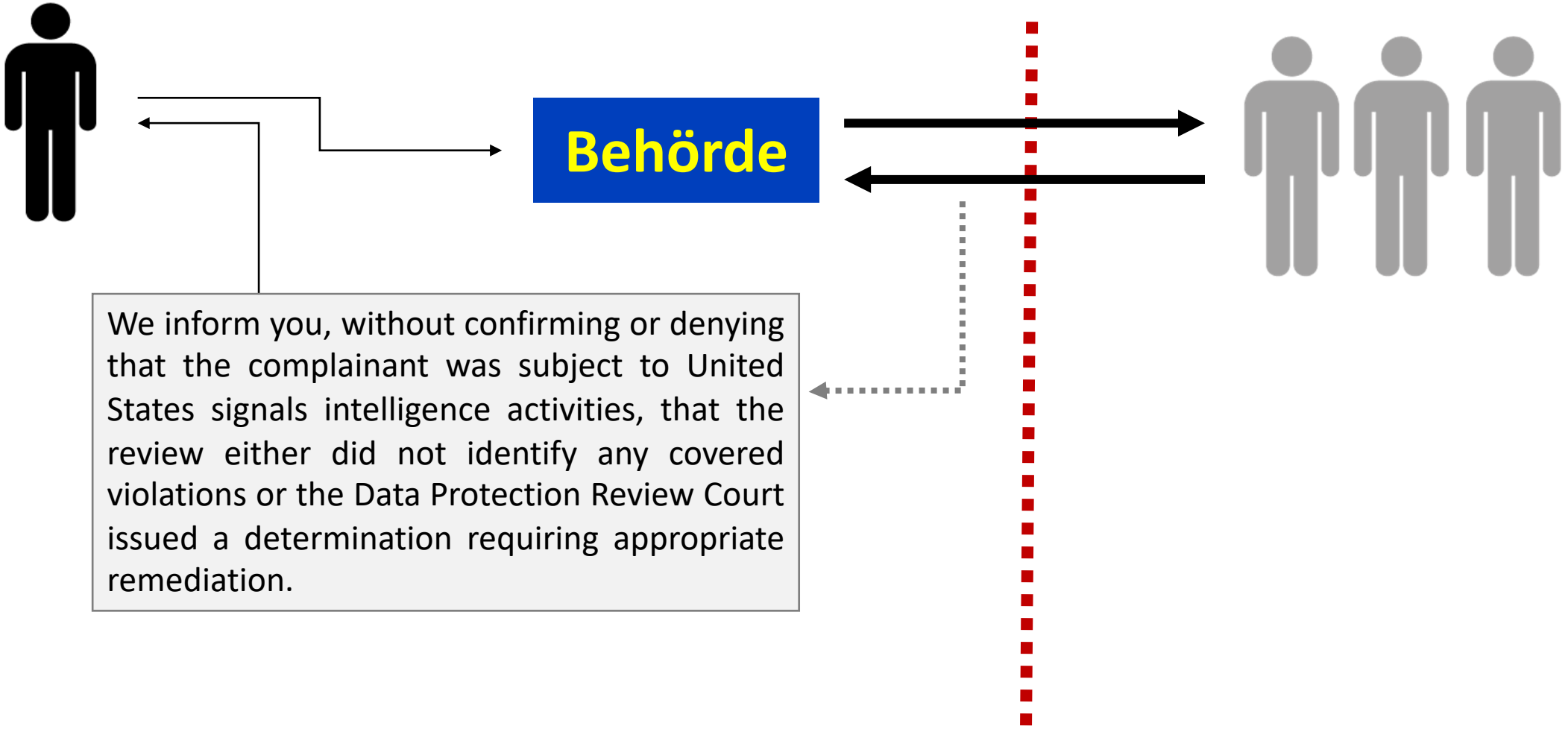
VERHÄLTNISMÄSSIGKEIT IN DEN USA?



„OMBUDSPERSON“ WIRD ZUM „CLPO“



DATA PROTECTION „COURT“



We inform you, without confirming or denying that you were subject to United States signals intelligence activities, that the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation.



KURZZEITUNG: EU-US „LÖSUNG“



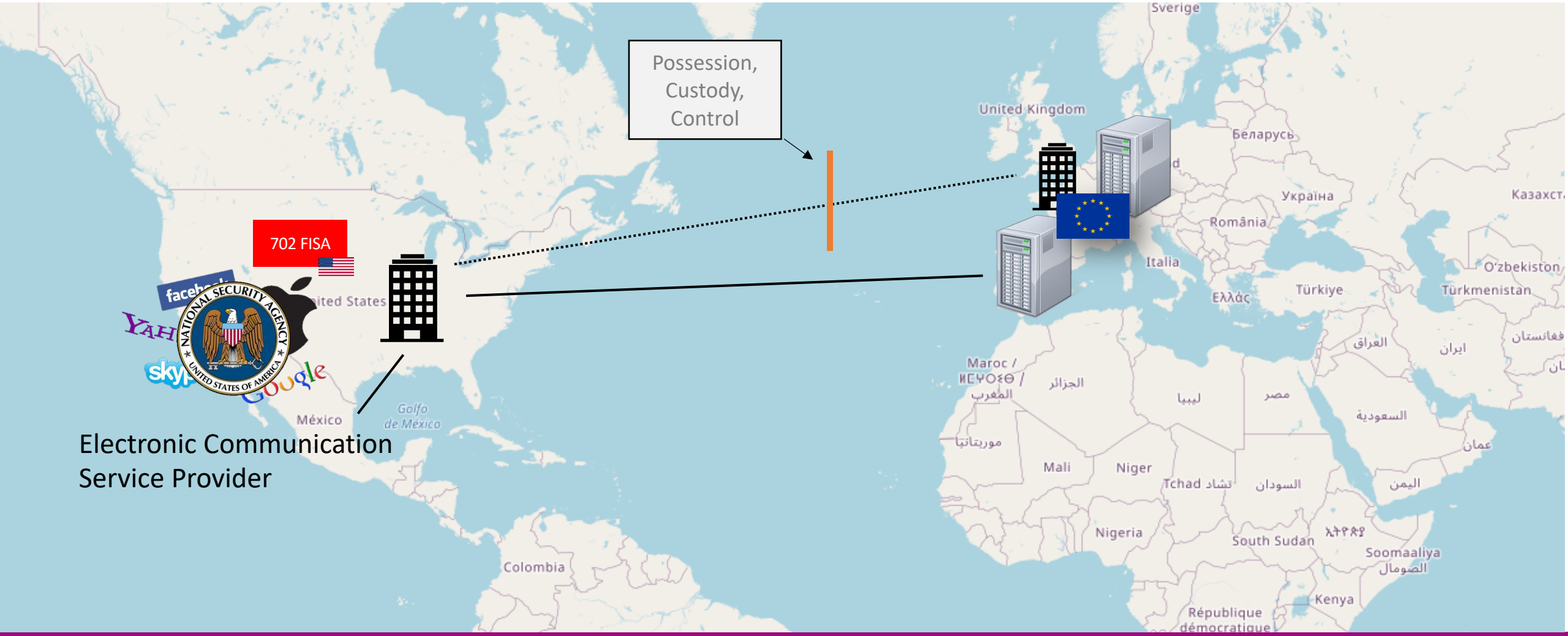


MITTELFRISTIG: ANDERE LÖSUNGEN

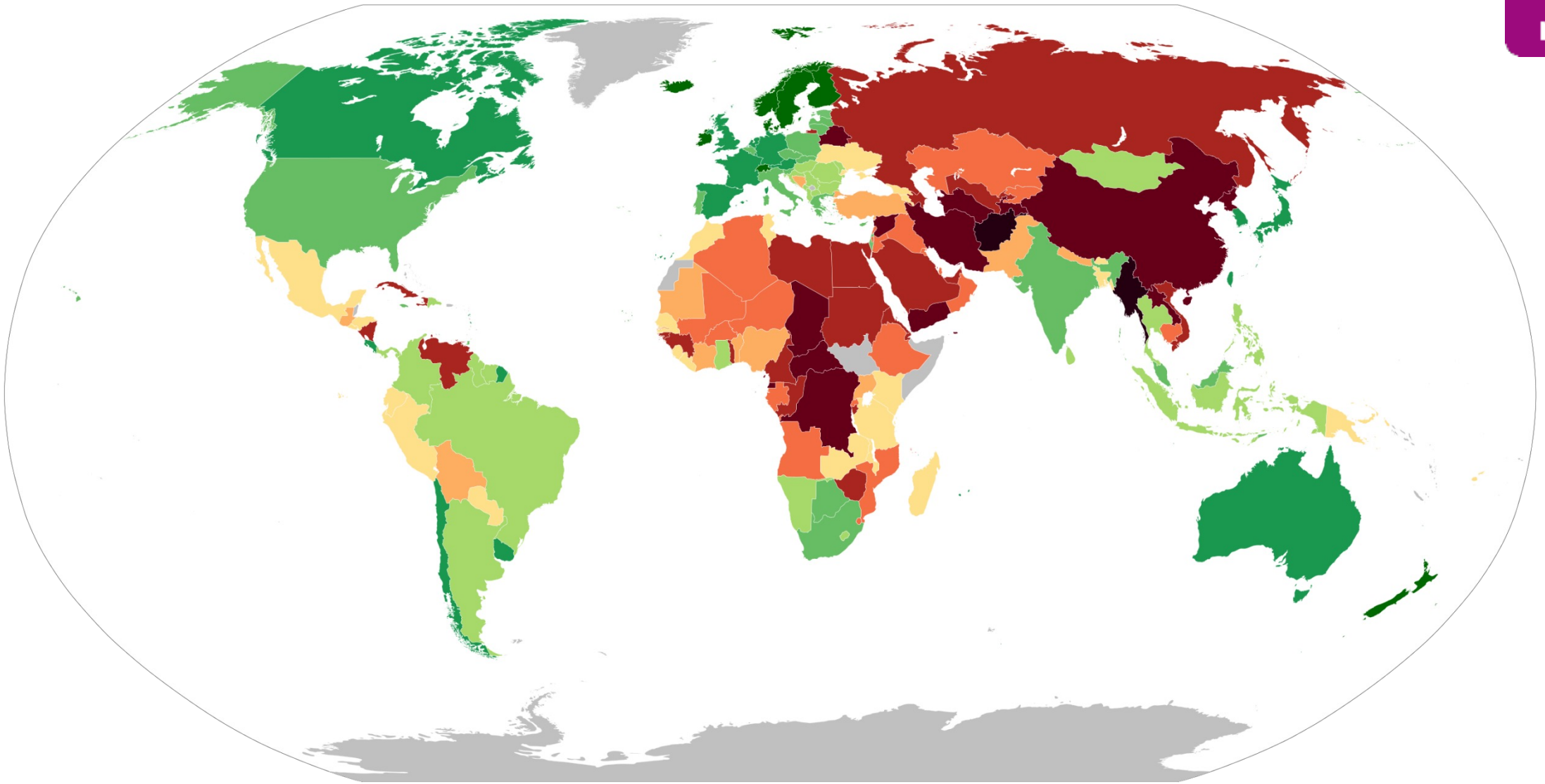




TRENNUNG: EU-SUBUNTERNEHMEN



LANGFRISTIG: UNDEMOKRATISCHE STAATEN



DANKE!