EUGH: C-311/18 ("*SCHREMS II*")

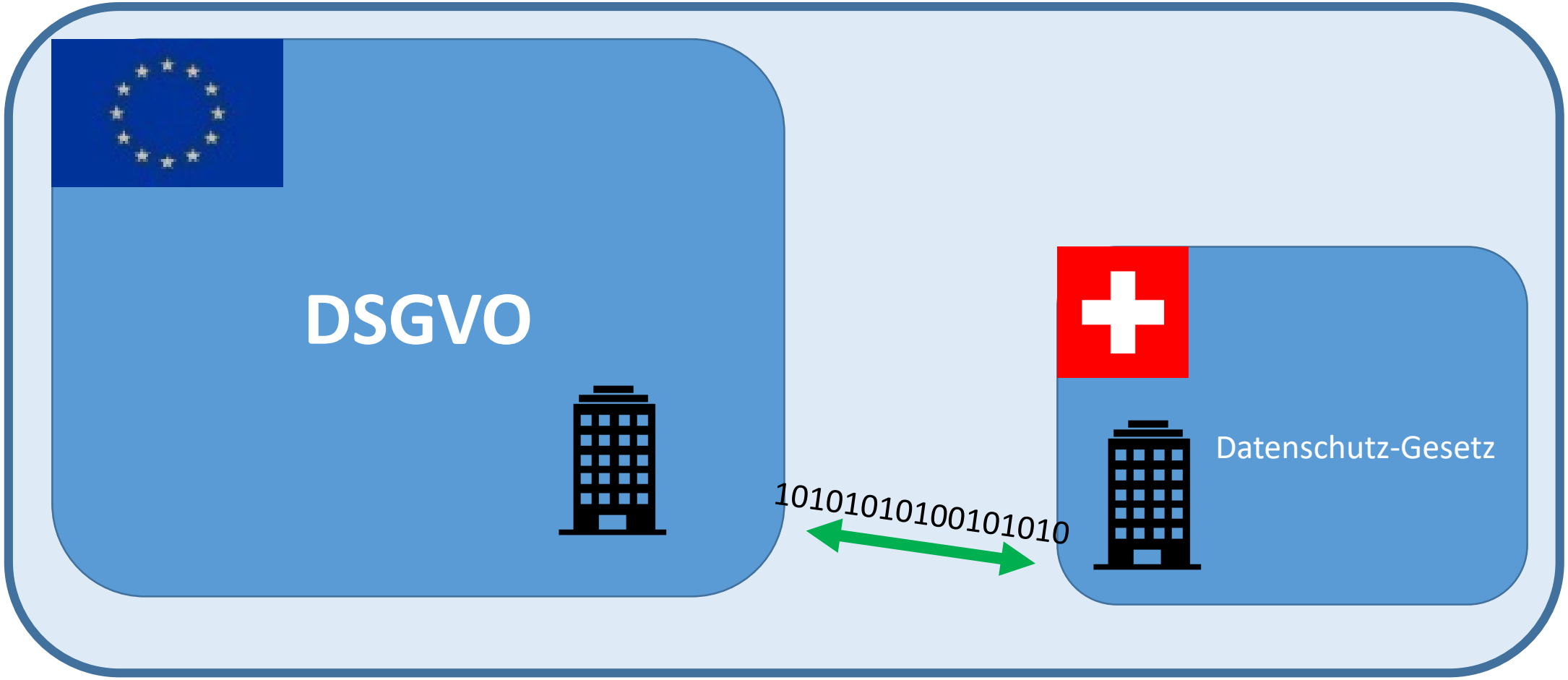
DATENÜBERTRAGUNGEN

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

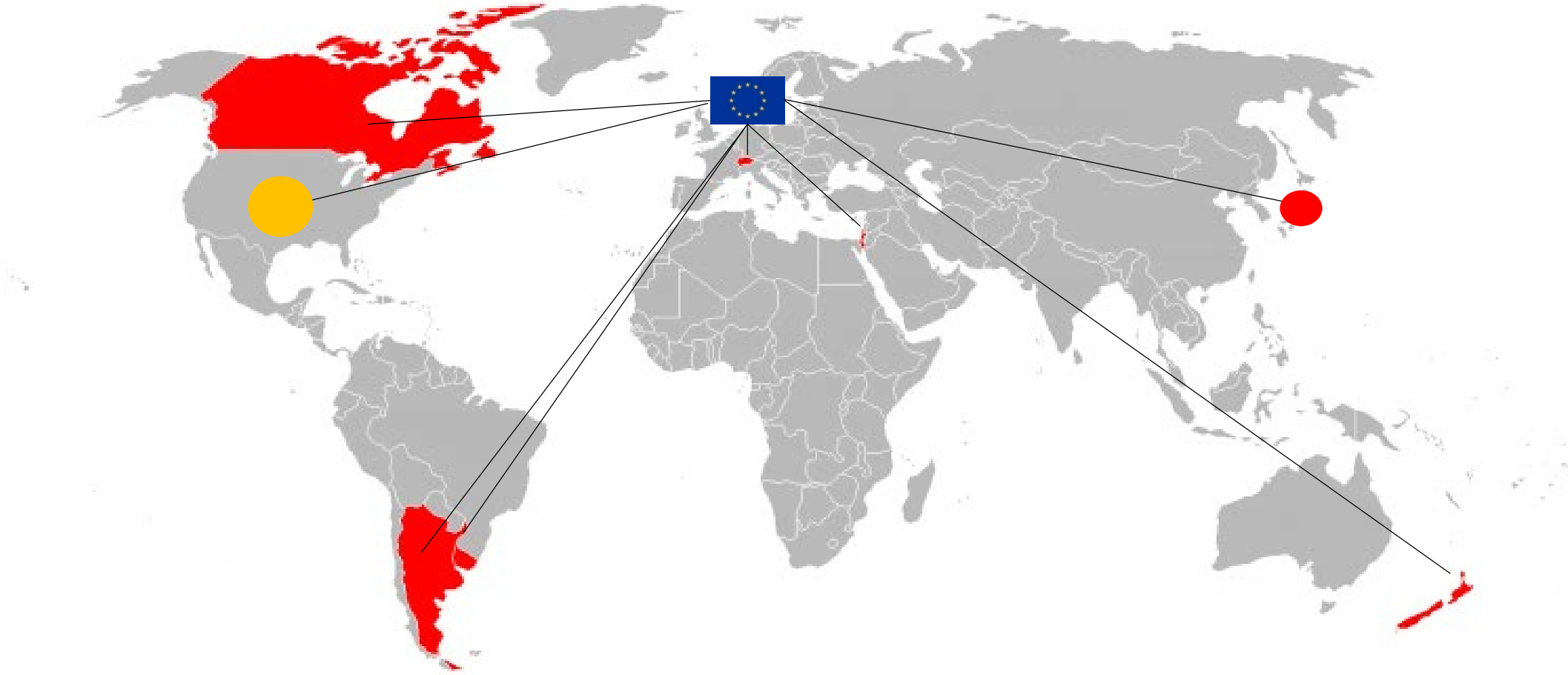
- **Outsourcing**:
  - Angemessenheit (Art 45)
  - Standardvertragsklausel/Musterklauseln (Art 46)
  - Verbindliche Unternehmensregeln (Art 47)

Ausweitung der DSGVO-Regeln in Drittländern

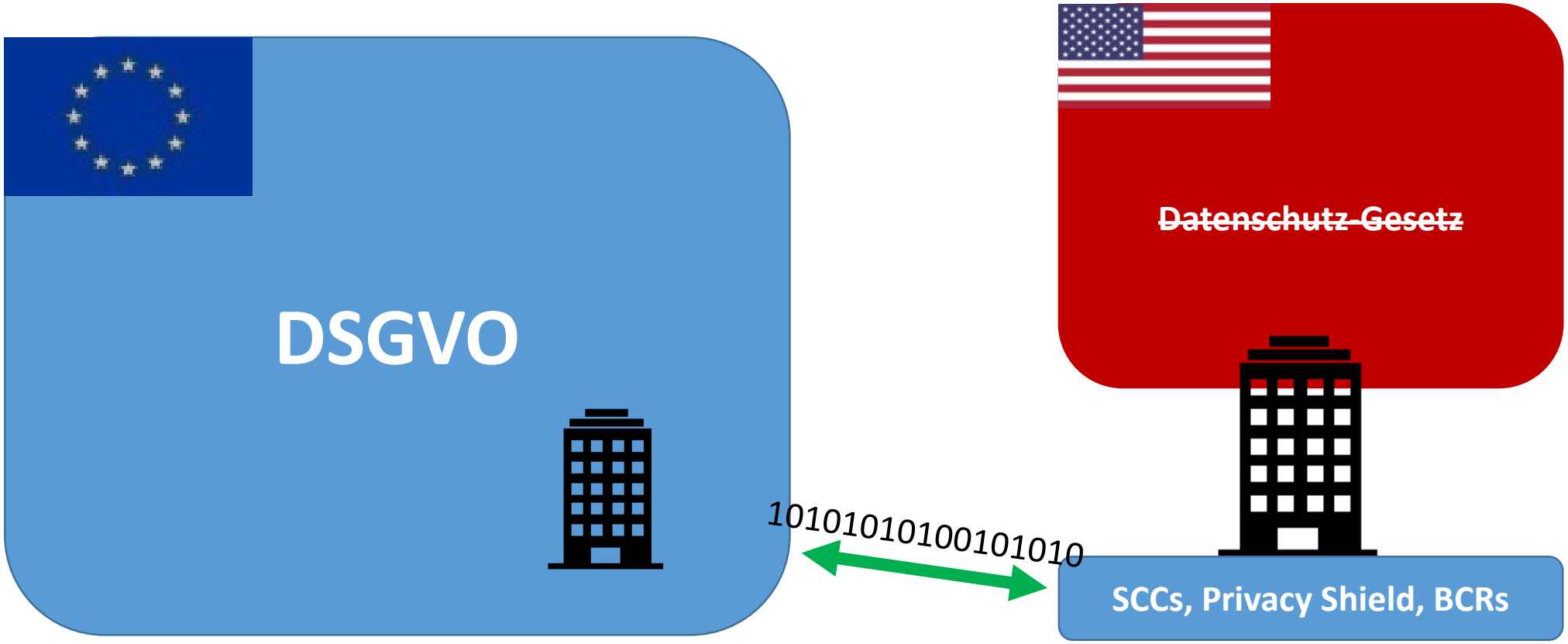
DATENSCHUTZ "BUBBLE": SCHWEIZ



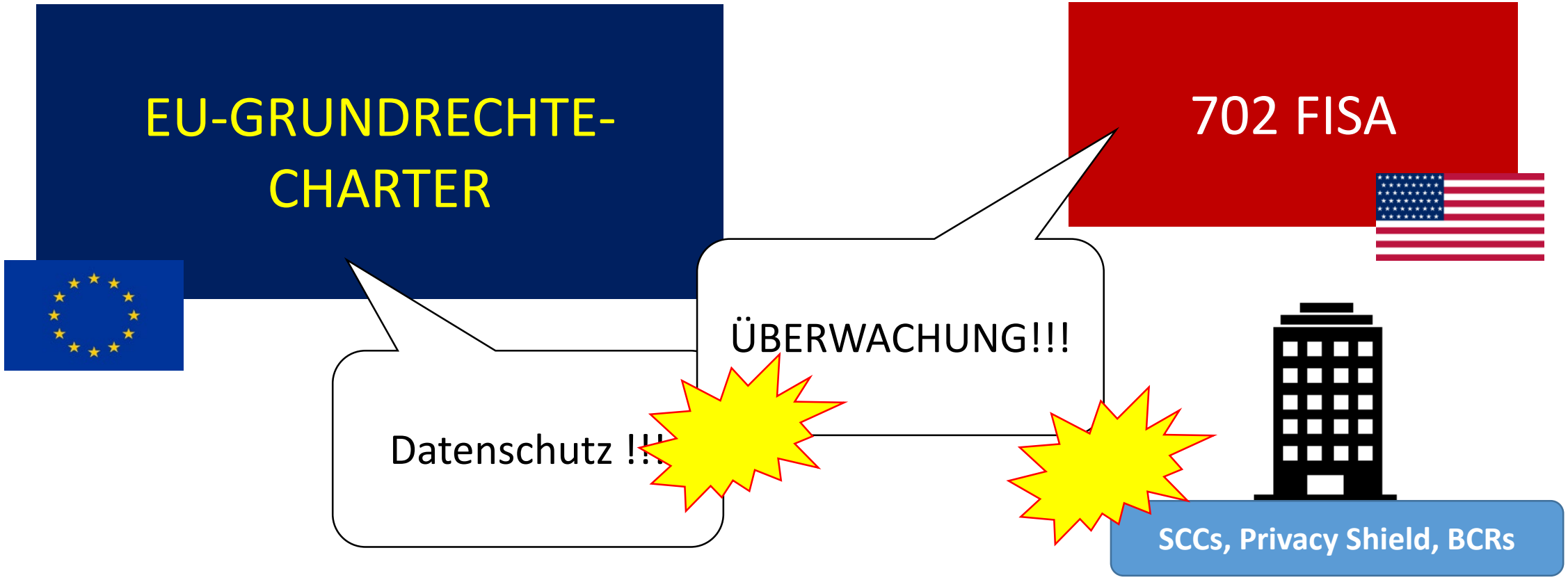
noyb

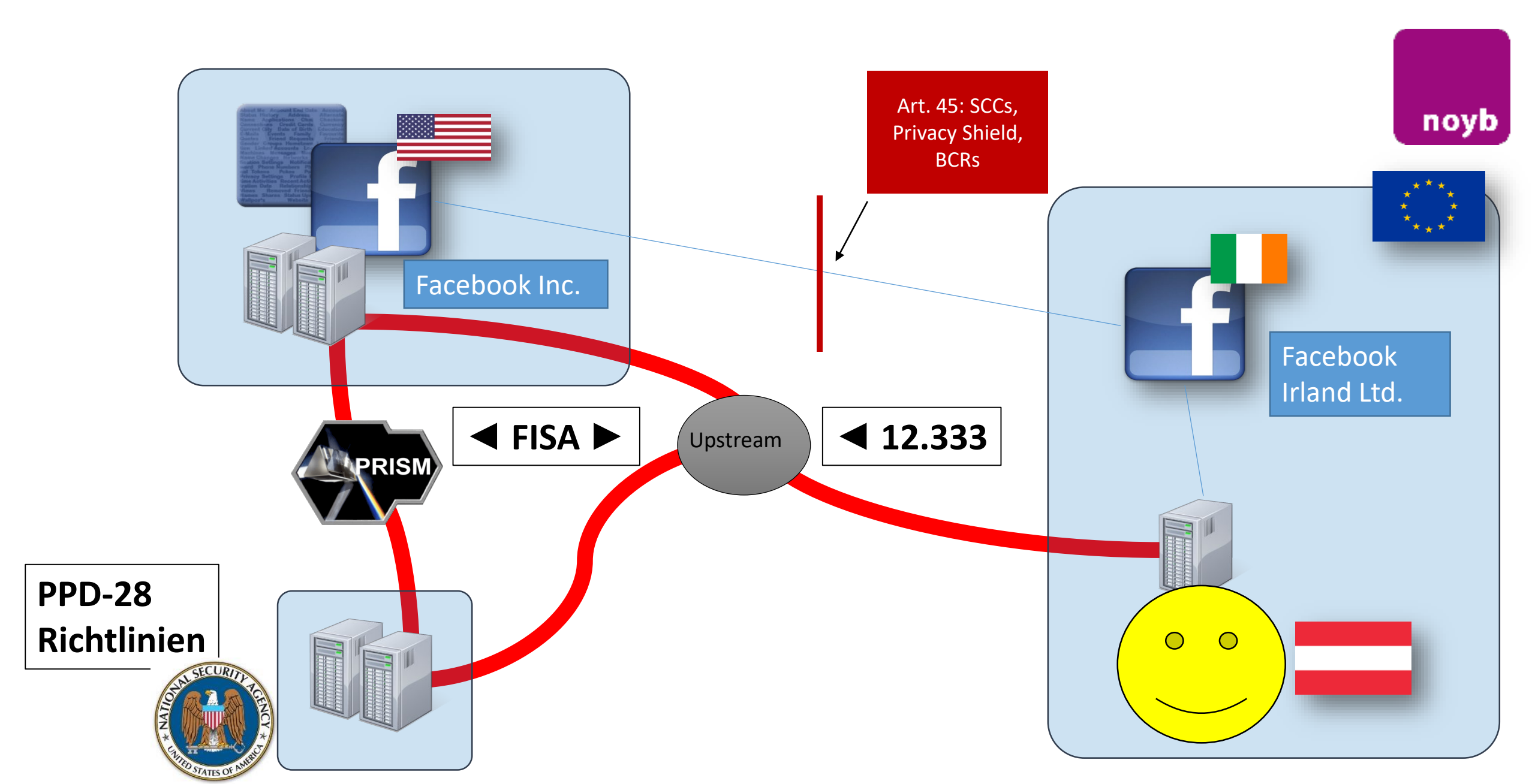


DATENSCHUTZ "BUBBLE": VERTRAG



EU-USA: 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

“KERNBEREICH”

1. Legitimer Zweck der Maßnahme
2. Eignung der Maßnahme
3. Erforderlichkeit (Alternative?)
4. Angemessenheit

noyb

PRIVACY SHIELD

- **Kommerzielle Datennutzung**
  - Materielle rechtliche Verbesserungen *(minimal)*
  - Administrative Verbesserungen

- **Staatliche Überwachung**
  - Überprüfung und Beschreibung des US-Rechts *(fehlte bisher, ab 2000)*
  - NEU: Ombudsperson *(Art 47 GRC)*

LIPSTICK ON A PIG?

noyb

ÜBERSICHT: PRIVACY SHIELD *(2. RUNDE)*

ZWEITE RUNDE (1)

- **Entscheidung des EuGH zu “Safe Harbor"** (Oktober 2015)
  - Der irische DPC informierte uns über Irrelevanz der Safe-Harbor-Entscheidung, da Facebook in Wirklichkeit SCCs verwendet (zuvor keine Information)

- **Aktualisierte Beschwerde über SCCs** (Hauptpunkt: Art 4 SCCs) (Dez 2015)

ZWEITE RUNDE (2)

- **DPC stellt Ermittlungen ein und erhebt Klage** gegen FB & MS als "natürliche Beklagte" wegen Nichtigkeit von SCCs (Frühjahr 2016)

  - EuGH hat ausschließliche Befugnis, EU-Recht für "ungültig" zu erklären
  - Amicus: US-Regierung, EPIC, zwei Industrie-Lobbygruppen (BSA + DigitalEurope)
  - FB bringt "Privacy Shield" in der letzten Anhörung vor dem High Court vor

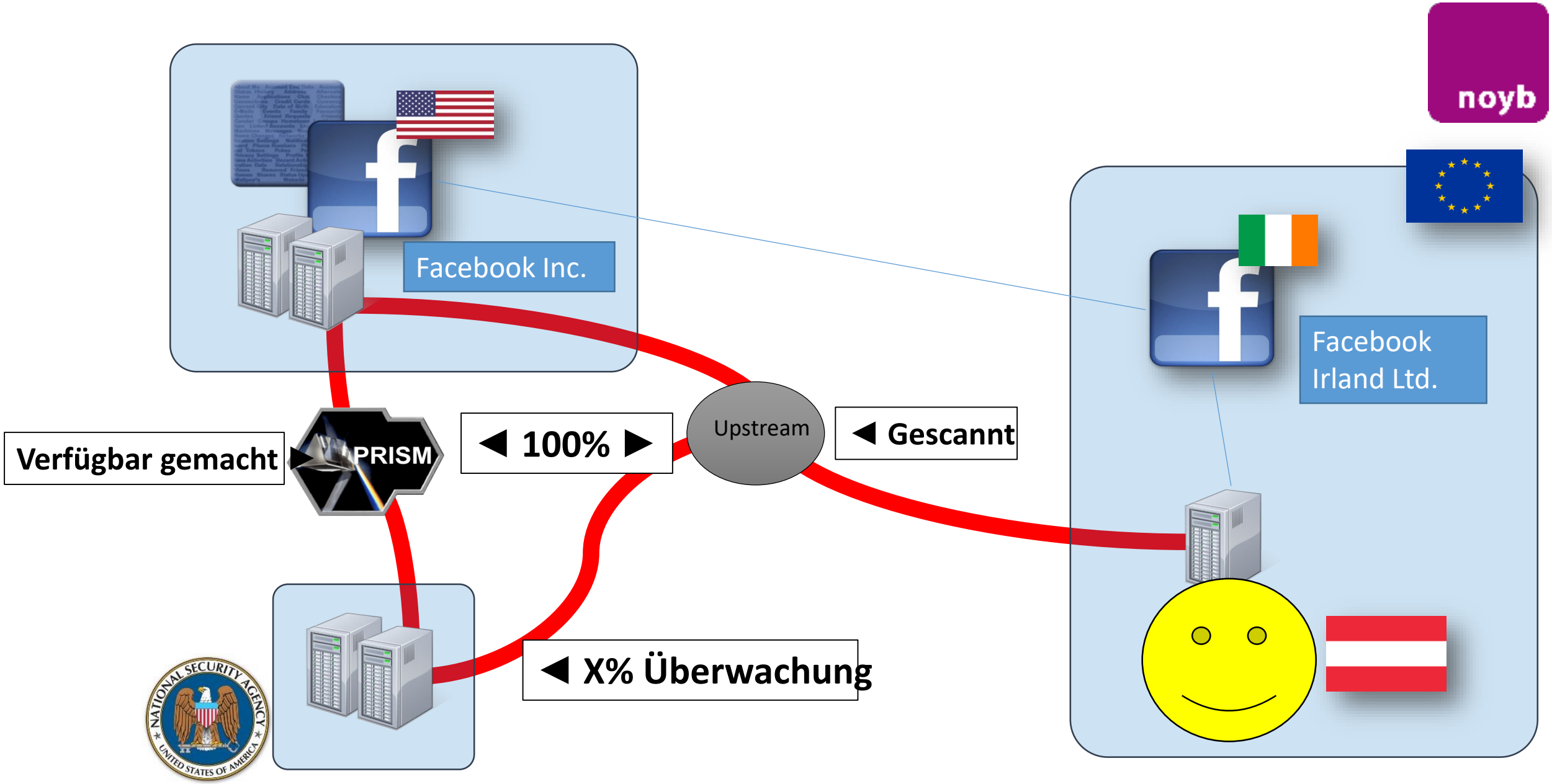
ZWEITE RUNDE (3)

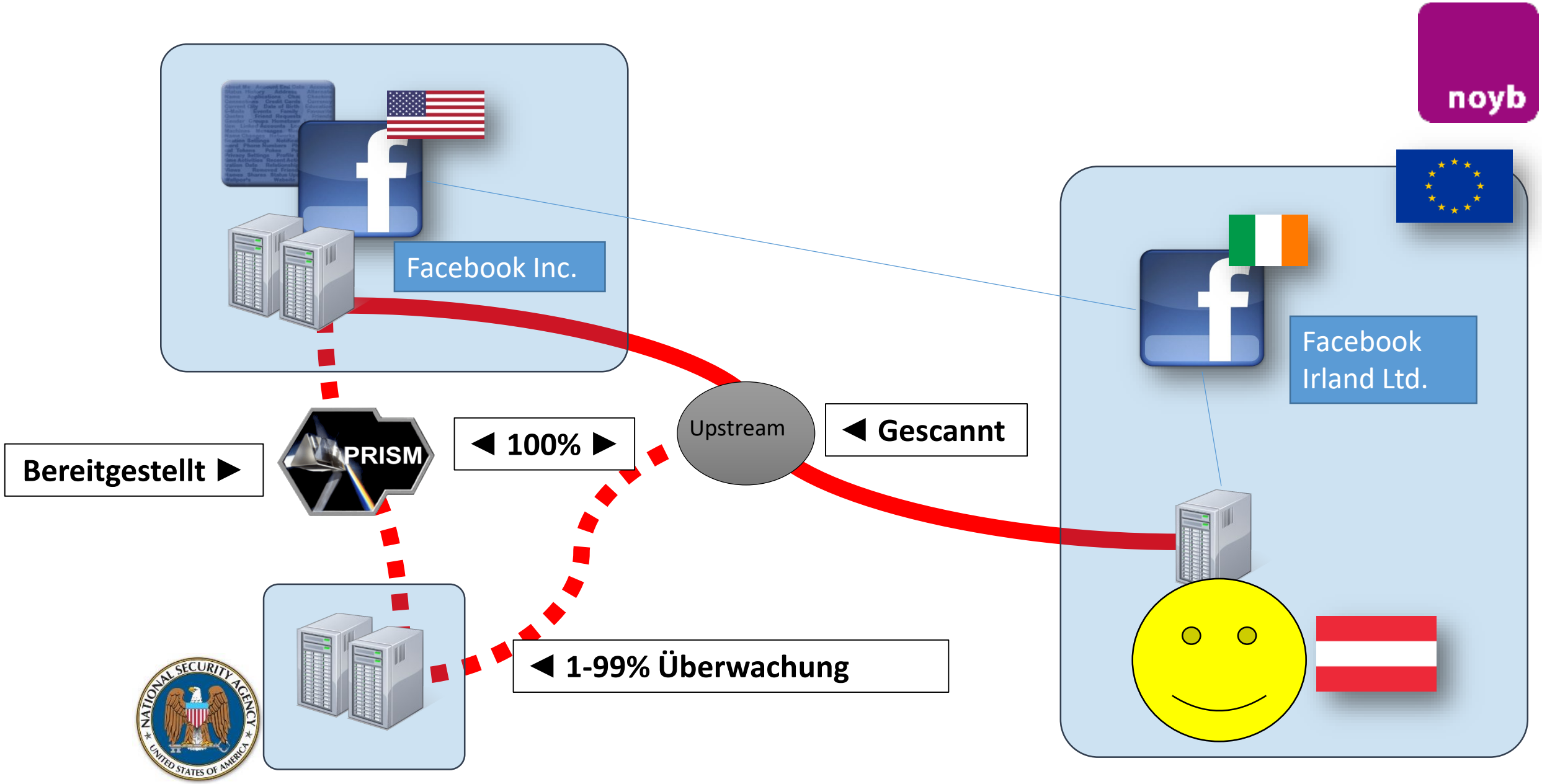
- **Irischer High Court legt Fall dem EuGH vor**
  - Faktenfeststellung: "Massenverarbeitung" durch PRIMS/Upstream
  - 11 Fragen
- **Stellungnahmen aller Parteien, *Amicus* und Amtsparteien**
  - Sieben irische Parteien, EU-Kommission, EU-Parlament, EDPB, Mitgliedstaaten...
- **Schreiben des EuGH mit weiteren Fragen**
  - Springen der meisten Fragen (faktisch gewonnen)
- **EuGH-Anhörung in Luxemburg**

EUGH-VORLAGE: FAKTEN

ETWAS ANDERE FAKTEN…

193. The Directive defines processing of personal data as including any operation or set of operations which is performed upon personal data such as collection… or otherwise making available the data. On the basis of this definition and the evidence in relation to the operation of the PRISM and Upstream programmes authorised under s. 702 of FISA, it is clear that there is mass indiscriminate **processing** of data by the Unites States government agencies, whether this is described as mass or targeted surveillance.


noyb
Facebook Inc.
Facebook
Irland Ltd.
Verfügbar gemacht
PRISM
◄ 100% ►
Upstream
◄ Gescannt
◄ X% Überwachung
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


noyb
Facebook Inc.
Facebook
Irland Ltd.
Bereitgestellt ▶
PRISM
◀ 100% ▶
Upstream
◀ Gescannt
◀ 1-99% Überwachung

KERNARGUMENTE

- Facebook sagte, dass es niemals Safe Harbor benutzt hat, aber SCCs

  Keine Überwachung, bzw wie in der EU *(“Kein Problem!”)*

- Schrems forderte DPC auf, Artikel 4 der SCCs für Facebook zu nutzen

  “Gezielte Lösung” nur für FISA-Unternehmen *("Art 4!")*

- Der irische DPC sah ein "systematisches" Problem und vertrat die Auffassung, dass die SCCs insgesamt ungültig sind

  Nichtigkeit von SCCs weltweit *(“Nuclear Option")*

EUROPÄISCHER ZWIESPALT

Article 4

1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.

2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

3. Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties.

The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.

The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.

Article 5

(ex Article 5 TEC)

1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.

2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the

ERGEBNIS

Ergebnis: Prozessrechtlich

Die "Lösung" ist Artikel 4 der SCCs *(alle außer der DPC)*

- Individuelle Durchsetzungsmassnahmen gegen "FISA"-Unternehmen
- Anullierung von SCCs nicht mehr relevant

Ergebnis: Materielles Recht

Fakten: Aus "Massenüberwachung" wurde "Massenverarbeitung".

US-Überwachungsgesetze sind nicht "verhältnismäßig“
(weniger als in Schrems I)

US-Rechtsschutz ist eine Verletzung des “Kernberichts“
(wie in Schrems I)

ERGEBNIS: PRAXIS

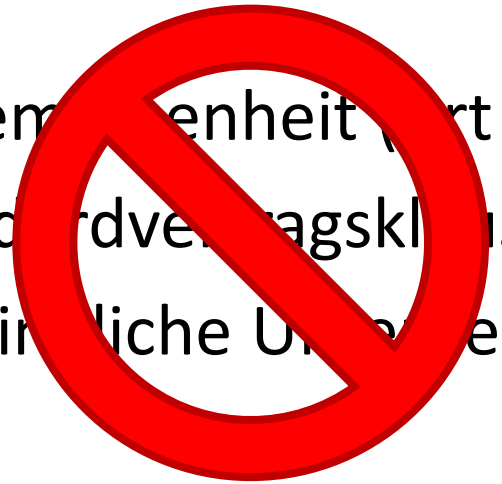
noyb

ERSTENS: DAS INTERNET IST *NICHT* TOT

DATENÜBERTRAGUNGEN

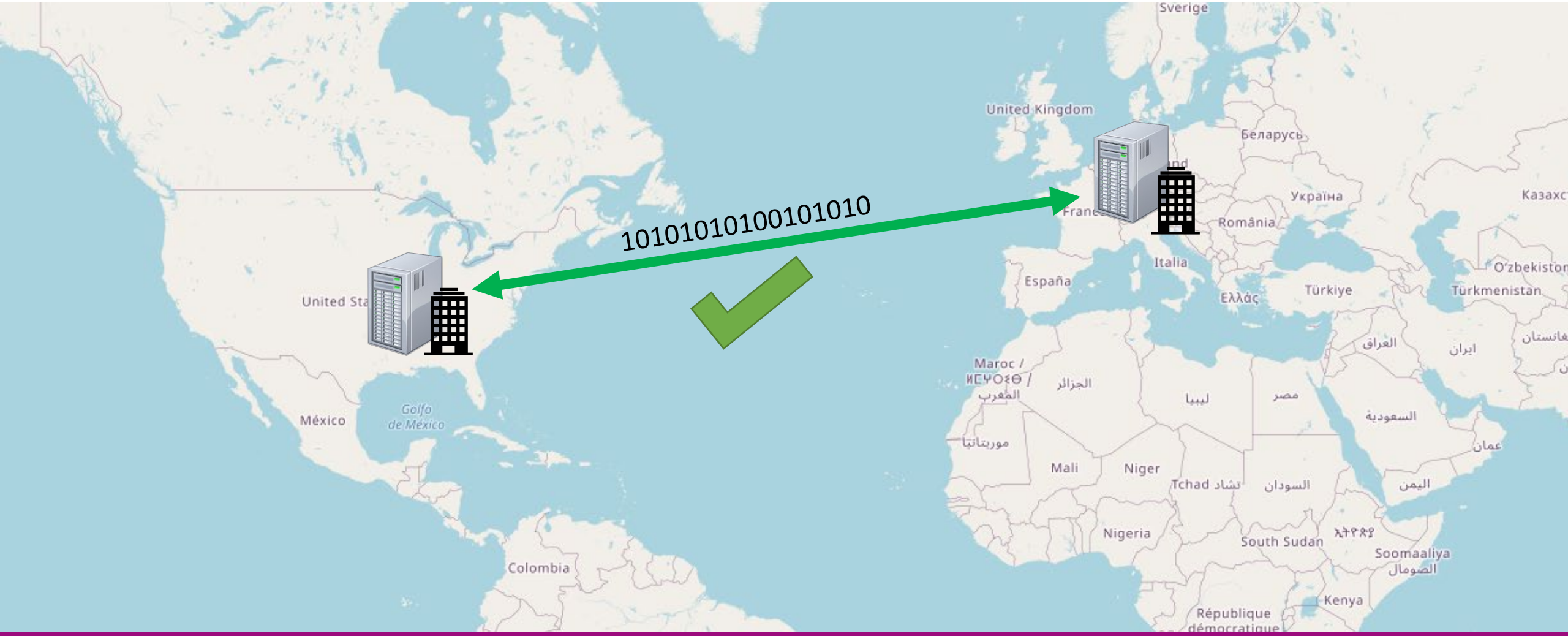
- **Allgemeine Regel:** Exportverbot für personenbezogene Daten
- **Ausnahme:** "Notwendige Übertragungen", nicht-strukturell (Art 49)

- **Outsourcing**:
  - Angem[illegible]enheit (Art 45)
  - Stand[illegible]rdvertragsklausel/Musterklauseln (Art 46)
  - Verbin[illegible]liche Unternehmensregeln (Art 47)

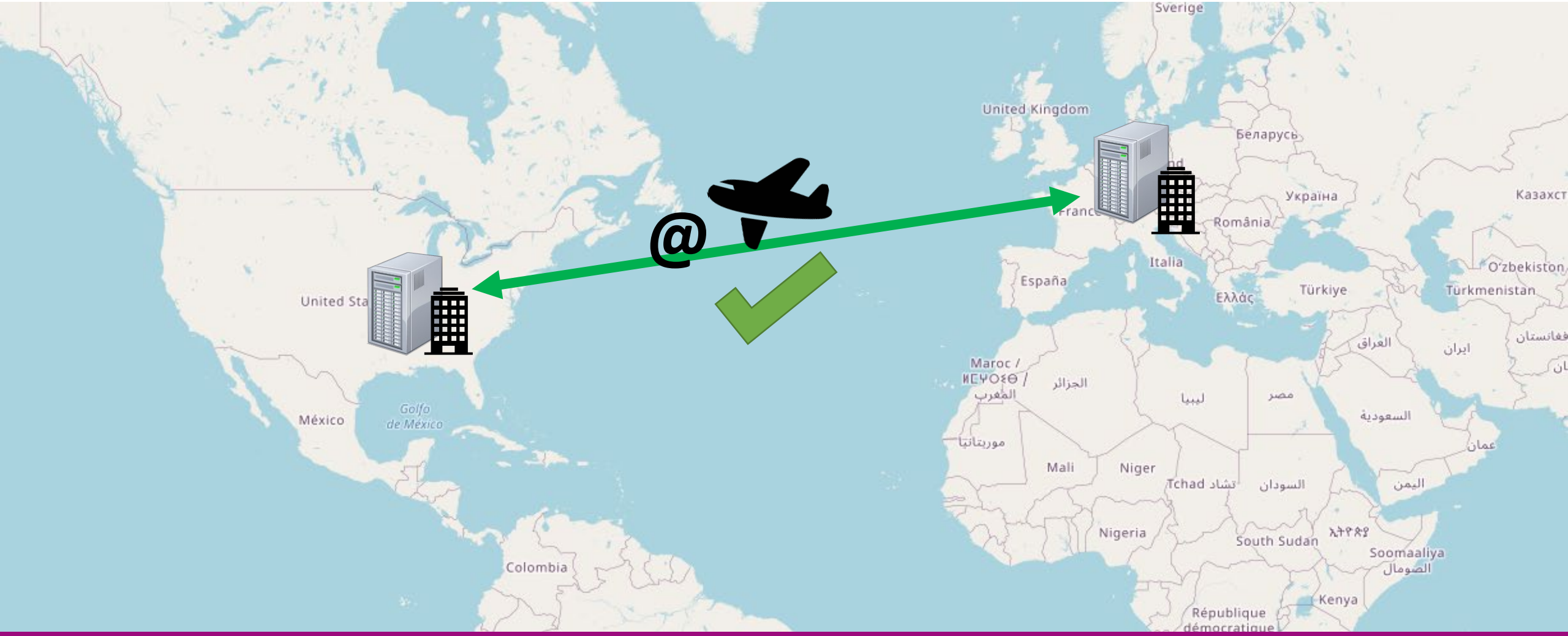


Ausweitung der DSGVO-Regeln in Drittländern

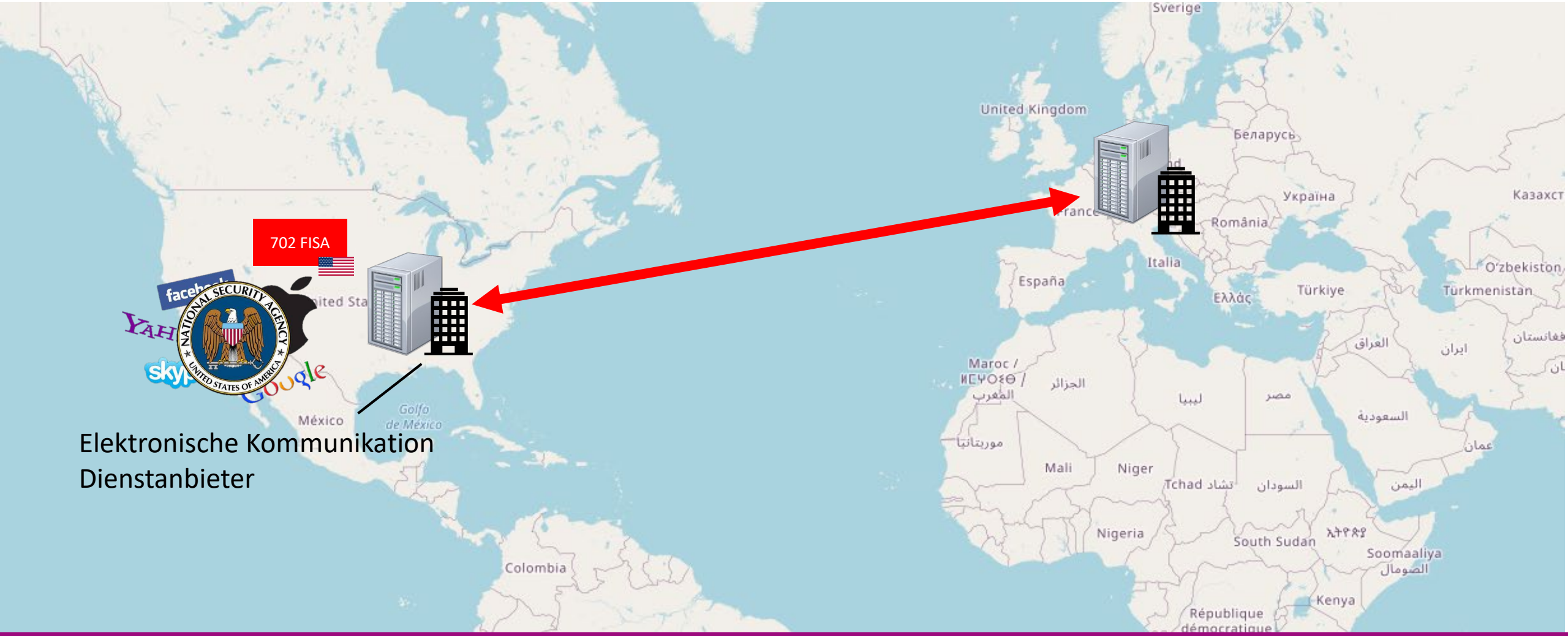
ÜBERMITTLUNGEN: NICHT PERSONENBEZOGEN



ÜBERMITTLUNGEN: NOTWENDIG

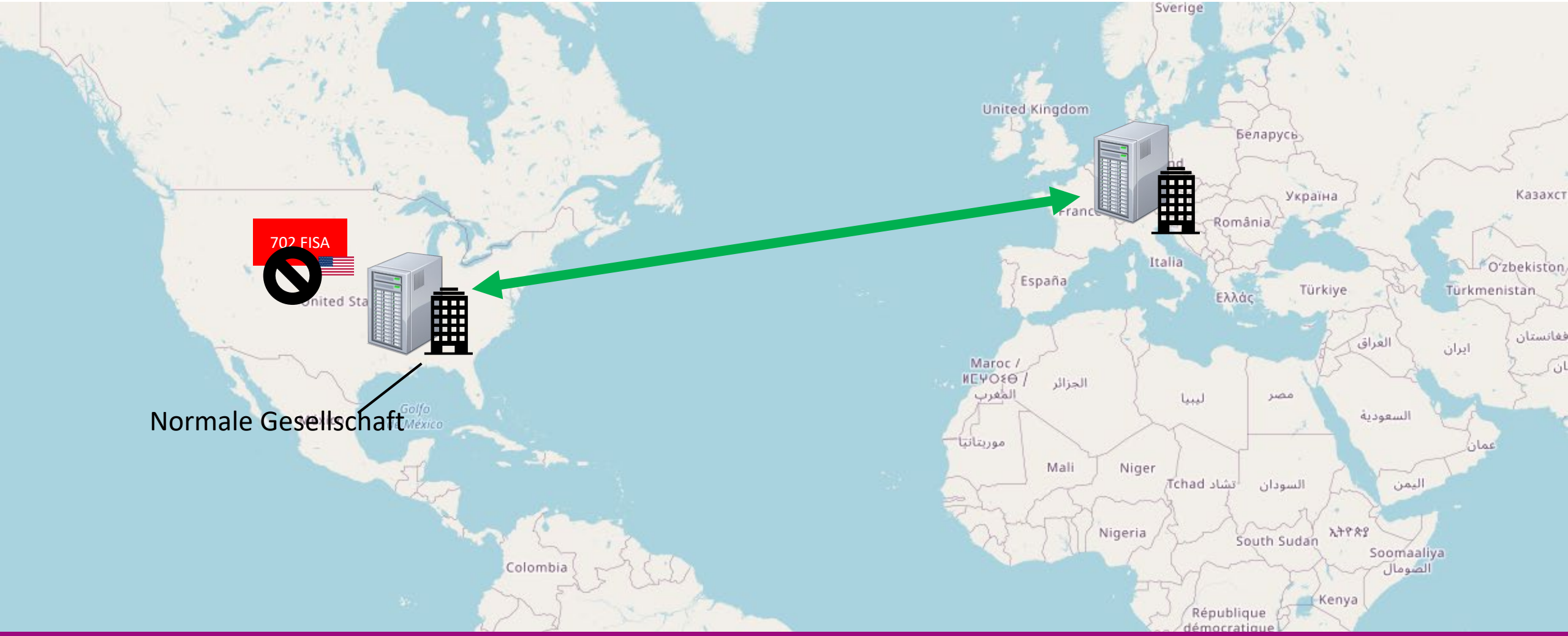


ÜBERMITTLUNG: “OUTSOURCING” (FISA)

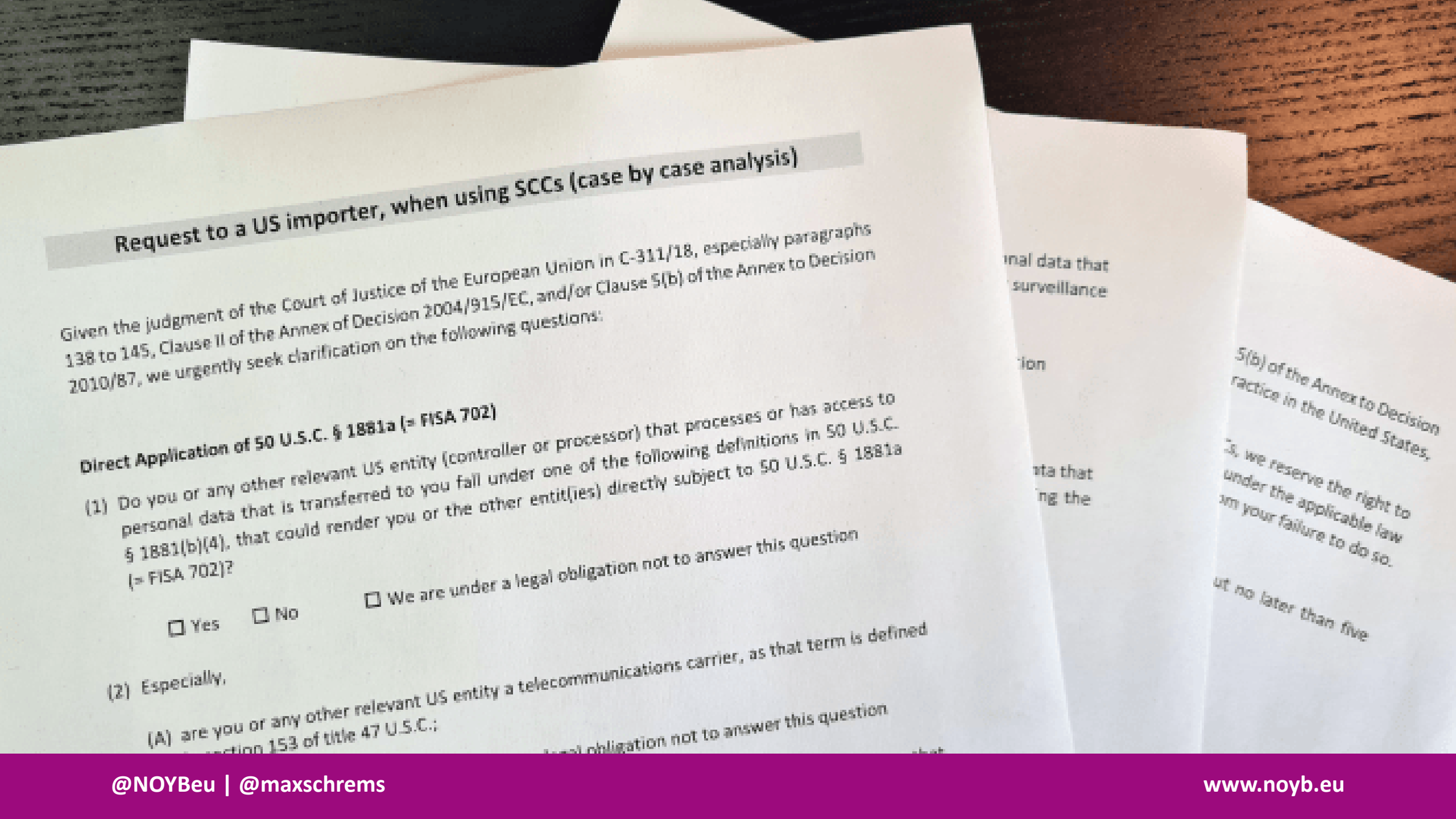


Elektronische Kommunikation Dienstanbieter

ÜBERMITTLUNG: NICHT-FISA



DURCHSETZUNG: AUFBAU VON DRUCK

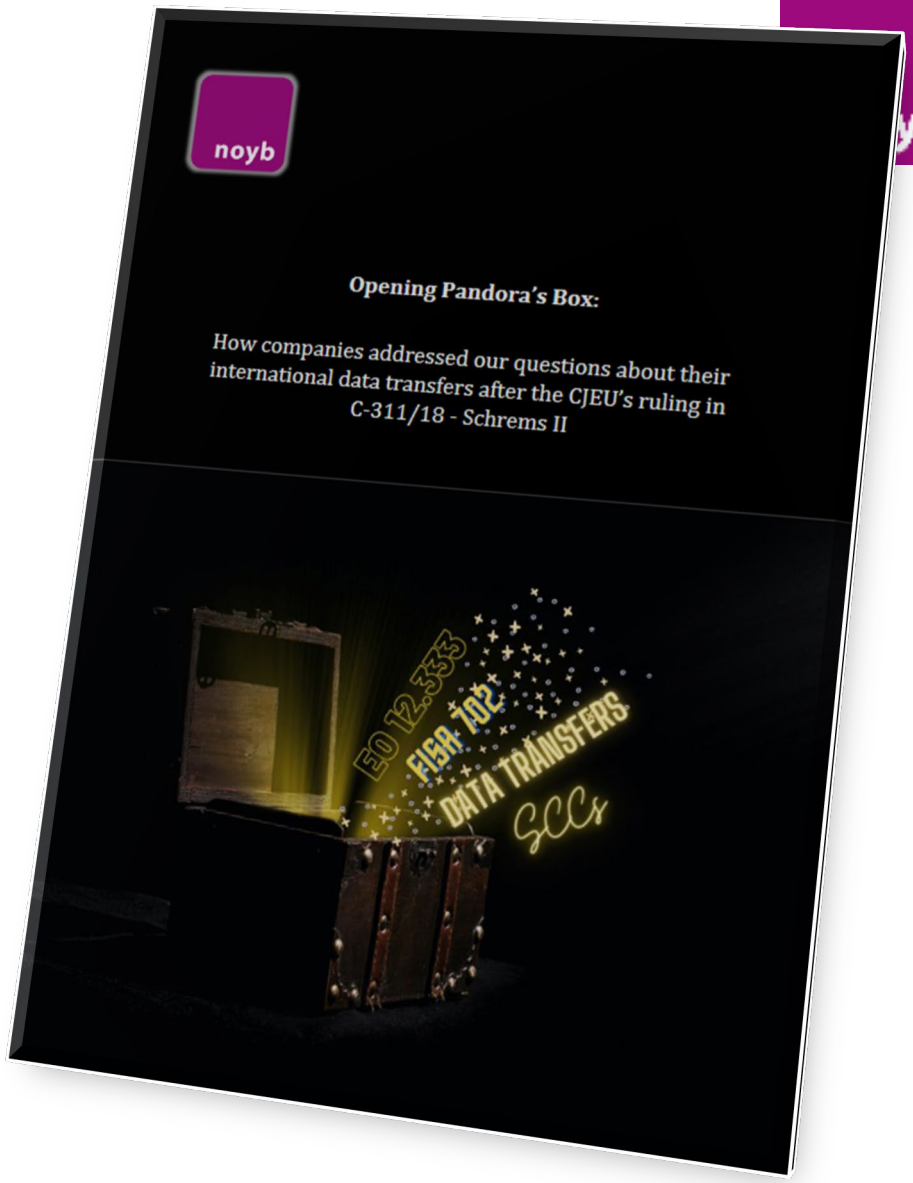

Request to a US importer, when using SCCs (case by case analysis)
Given the judgment of the Court of Justice of the European Union in C-311/18, especially paragraphs 138 to 145, Clause II of the Annex of Decision 2004/915/EC, and/or Clause 5(b) of the Annex to Decision 2010/87, we urgently seek clarification on the following questions:
Direct Application of 50 U.S.C. § 1881a (= FISA 702)
(1) Do you or any other relevant US entity (controller or processor) that processes or has access to personal data that is transferred to you fall under one of the following definitions in 50 U.S.C. § 1881(b)(4), that could render you or the other entit(ies) directly subject to 50 U.S.C. § 1881a (= FISA 702)?
☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question
(2) Especially,
(A) are you or any other relevant US entity a telecommunications carrier, as that term is defined


REMOTE PARTICIPANTS
noyb
SCHREMS MAX
REMOTE PARTICIPANTS
REYNDERS DIDIER
REMOTE PARTICIPANTS
edpb
European Data Protection Board
edpb.europa.eu
JELINEK ANDREA

noyb

Anfrage an 33 Unternehmen

- Outsourcing
- US-Übertragungen
- FISA 702
- EO 12.333



noyb's

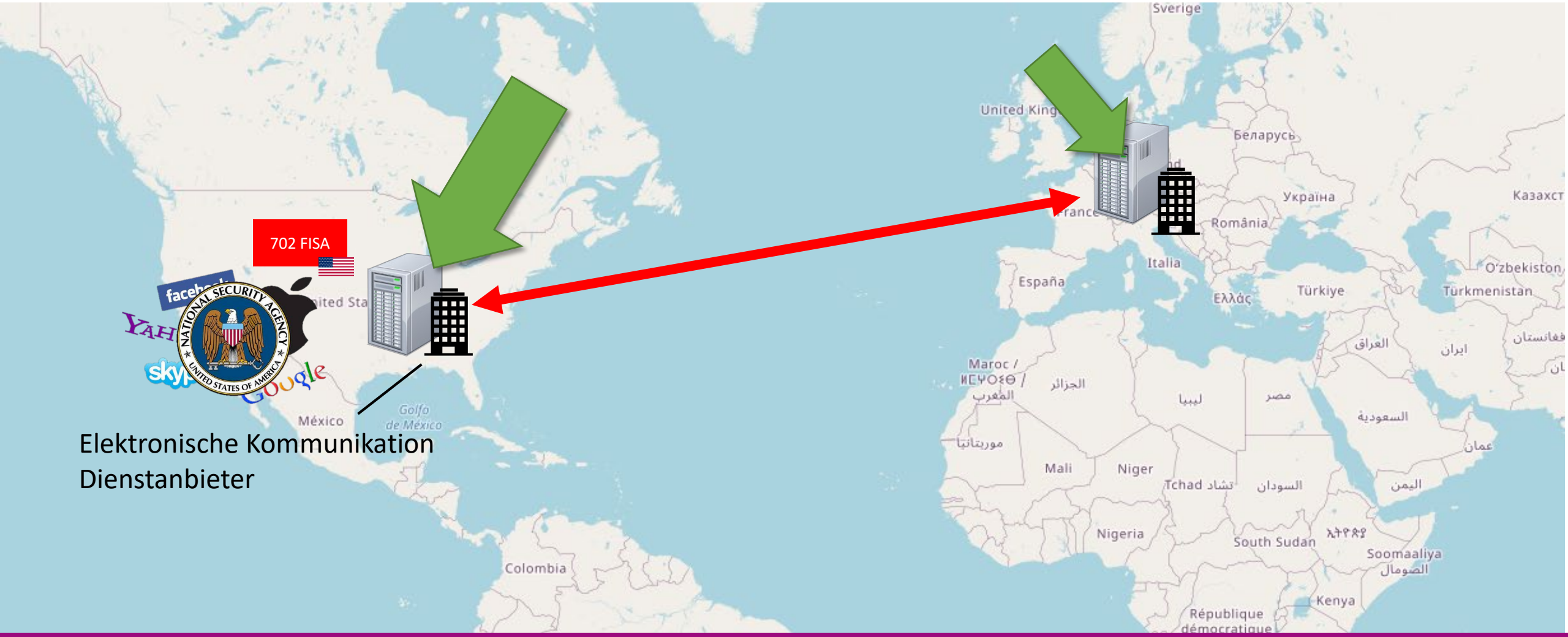
101 US TRANSFER COMPLAINTS

Facebook told it may have to suspend EU data transfers after Schrems II ruling

Natasha Lomas @riptari / 6:20 AM GMT+2 • September 10, 2020

DURCHSETZUNG: WEITER ZIELE

noyb



LÖSUNG: „ERGÄNZENDE MAßNAHMEN“?

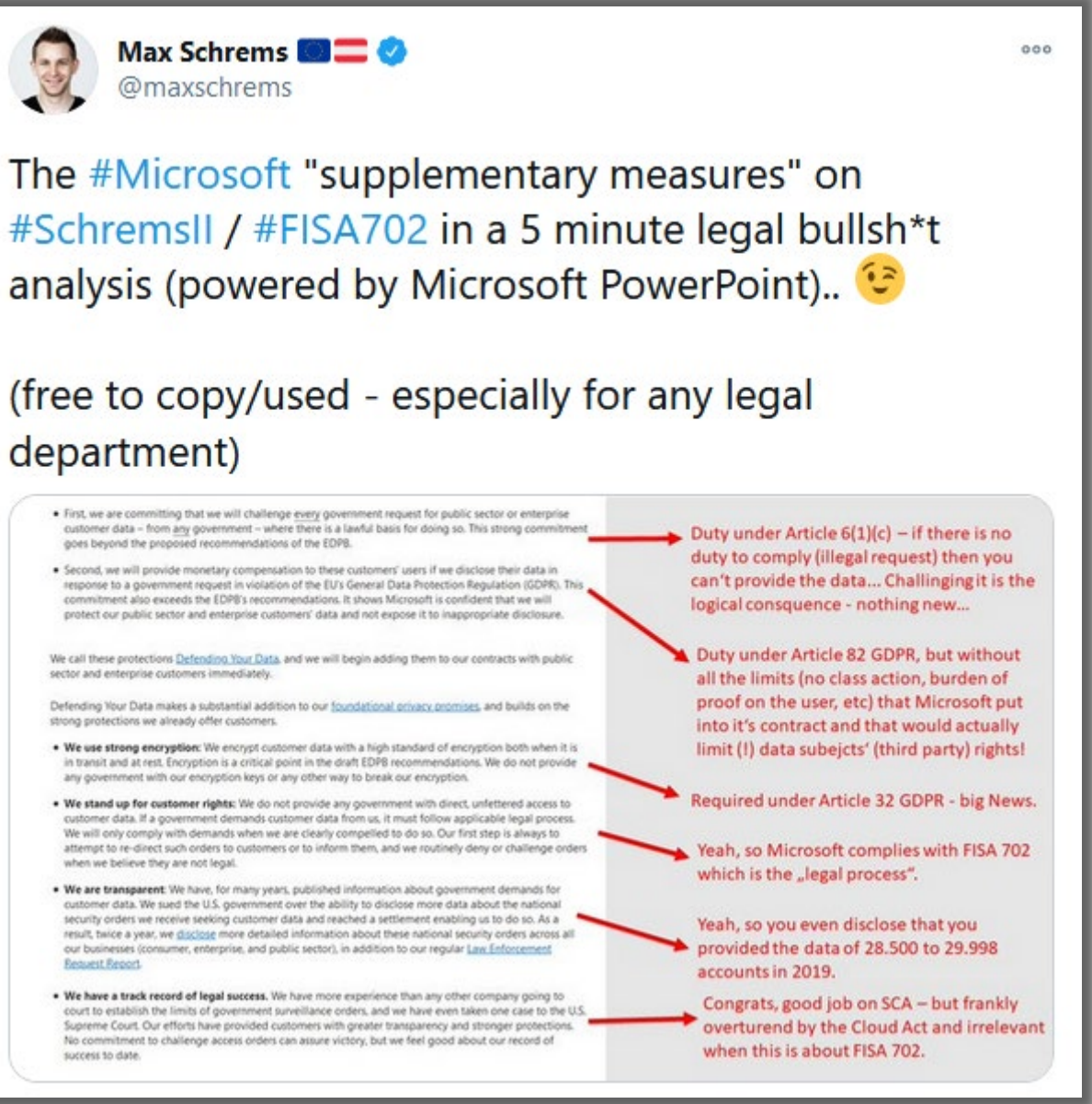
ERWGR 109

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

ERGÄNZENDE MAßNAHMEN

- **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.

noyb

LÖSUNG: DATENSCHUTZ = DATENFLUSS

FRAGEN, INPUT...?