IT Governance USA & DQM GRC webinar

EU-US data transfers: the Practical Implications of Schrems II

Date: 6 October 2020

Presented by:

- Preston Bukaty, GRC Consultant, IT Governance US
- Camilla Winlo, Director of Consulting Services, DQM GRC

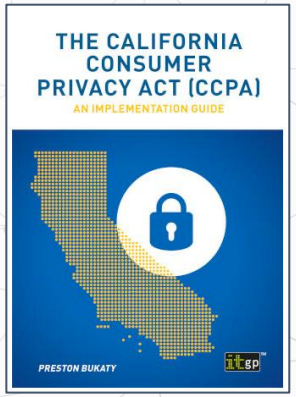
Introduction

Preston Bukaty – Denver, CO

GRC Consultant,

IT Governance USA

- Juris Doctorate, University of Kansas School of Law
- Author, "The CCPA: An Implementation Guide"
- Advise clients on cyber security and data privacy laws
- Program development, policy drafting, management, maintenance, internal audit, and staff training.
- Teach training and certification courses covering evolving laws (GDPR, CCPA), and respective risk management frameworks (ISO 27001, NIST 800-53).



Introduction

Camilla Winlo,
Director of Consulting Services, DQM GRC

- Not a lawyer
- Award-winning Privacy by Design trainer and consultant
- Leads DQM GRC's data privacy implementation consultancy
- Over a decade of experience in commercialising regulatory change - including as part of a leadership team which developed and launched three financial services businesses
- Chartered Banker, Post-Graduate Professional Diploma in Marketing, CISMP, ISO 27001 and Certified DPO

About GRC International

A trusted global Compliance Partner

15 years of experience,

200 employees

IT governance, risk and compliance solutions

Over 12,000 clients across six continents

Over 4,000 training solutions delivered

Protect • Comply • Thrive

About IT Governance & DQM GRC

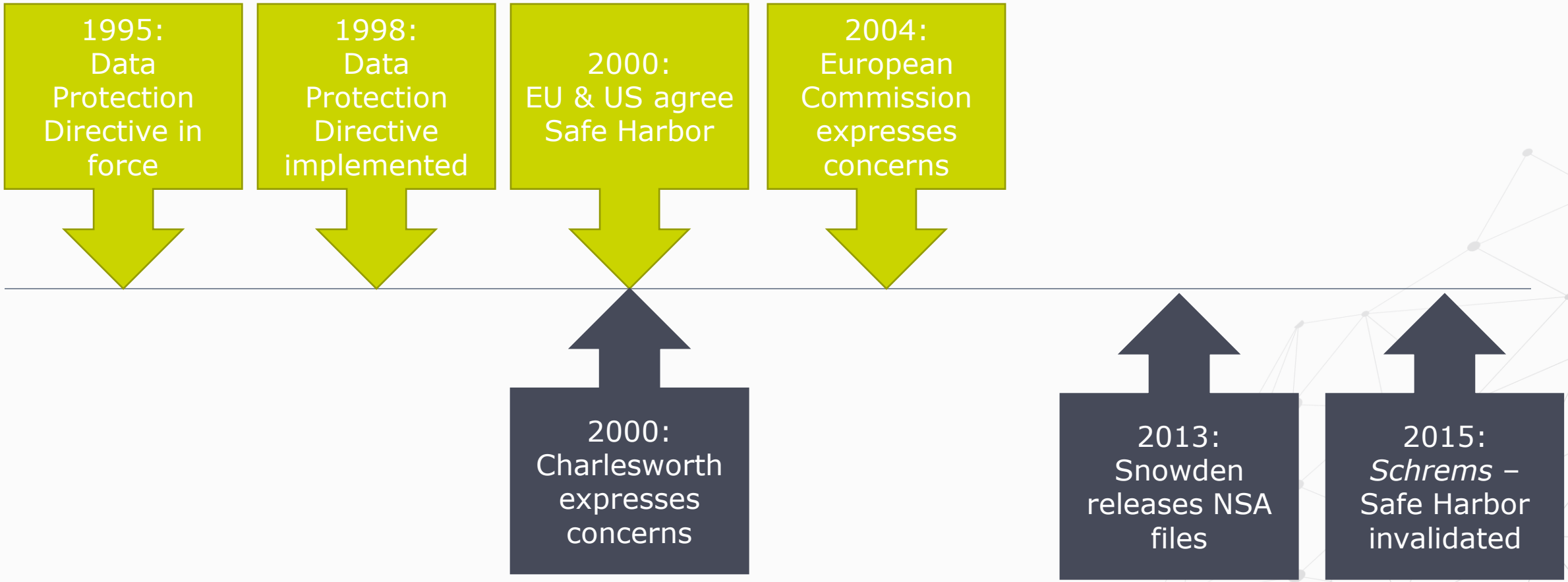
- **IT Governance** is a leading global provider of cyber risk and privacy management and compliance solutions
- **Protect** ● **Comply** ● **Thrive** approach is aimed at helping your organisation achieve resilience in the face of constant change.
- **DQM GRC** was founded in 1996 to help organisations protect and harness the value of their data assets.
- **Confidence in Data** approach is designed to de-risk the use of data and unlock its organisational value

DQM GRC™
CONFIDENCE IN DATA

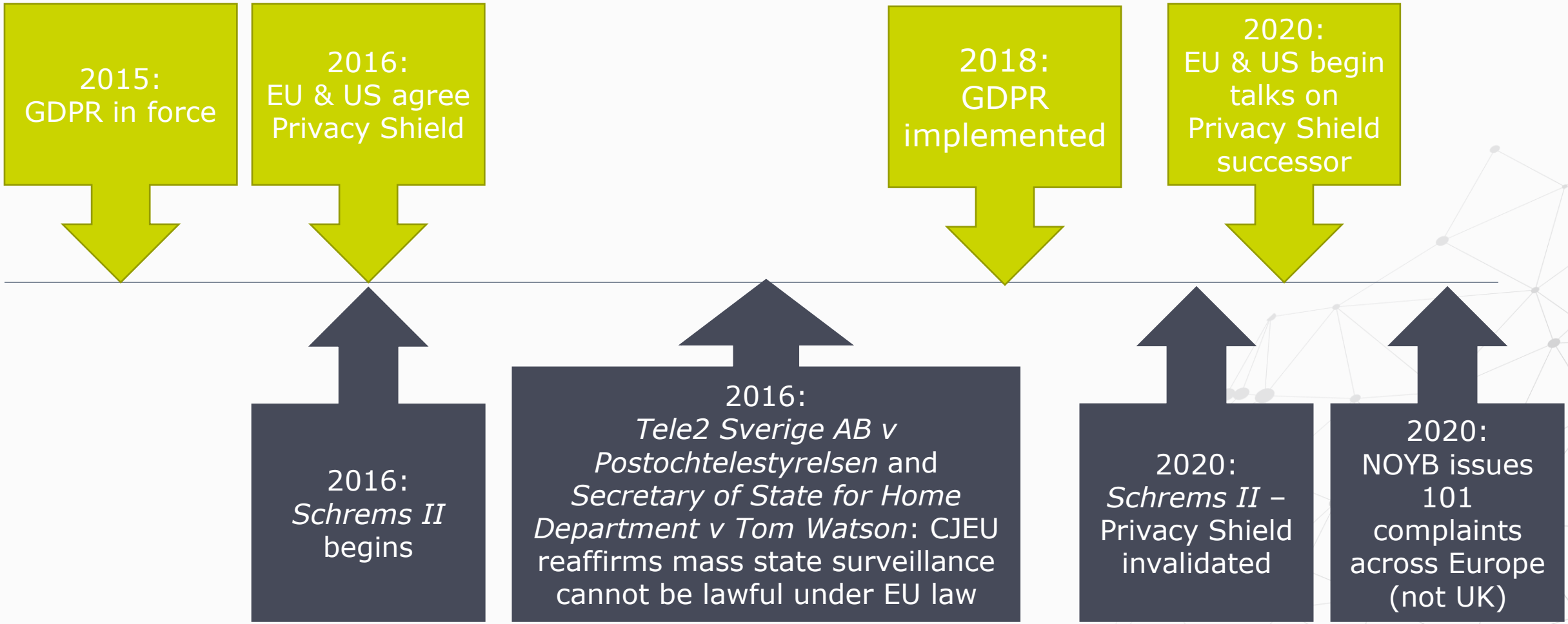
Today's Discussion

- The Schrems II decision regarding transfers of data
- The implications EU and US data controllers face for data transfers
- Data transfers - options
- Data transfers - alternatives
- Practical steps organizations can take now
- What the future of Schrems II might bring

Schrems – Safe Harbor falls



Schrems II – Privacy Shield falls



What is the GDPR

- Effective date: May 25, 2018
- Gives individuals control over how their information is controlled and processed
- Pressures organizations processing EU residents' personal data to tighten data protection processes
- Requires organizations to adopt appropriate **policies, procedures, and processes** to protect personal data
- **Risk-based approach** to data protection
- Many other countries base their laws on GDPR

Does my organization need to comply?

Do I need an EU representative?

Role

- **Represent** the non-EU organization with respect to its GDPR obligations
- Serve as a **local point of contact** for data subjects and supervisory authority
- **Hold a record** of the organization's processing activities
- *NOT* responsible for GDPR compliance

Data transfers – options

Options for data transfers

Routine transfers

- EC Adequacy decision
- ~~Privacy Shield~~
- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)

Occasional transfers

- Article 49 derogation
  - Options aligned to each Lawful Basis of Processing, plus legal claims

Transfers to 3rd countries

- ***Article 45: Adequacy decisions***

- European Commission decides country's laws are Adequate – 13 decisions to date
- The adequacy criteria:
  - the rule of law;
  - respect for human rights and fundamental freedoms;
  - relevant legislation, both general and sectoral, including:
    - concerning public security;
    - defense;
    - national security; and
    - criminal law.
- *Official Journal of the European Union* (published on the EU Commission website - *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*)

Transfers to 3rd countries

- ***Articles 46 & 47: SCCs and BCRs***

- Standard Contractual Clauses adopted by European Commission
  - Sets for Data Controllers and Data Processors
  - Must be included in full
  - Compliance must be assured
  - New clauses coming soon
- Binding Corporate Rules approved by supervisory authority
  - Specific to an organization
  - Only cover transfers within the Group
  - Compliance must be assured

- Transfers must stop immediately if recipient can no longer comply

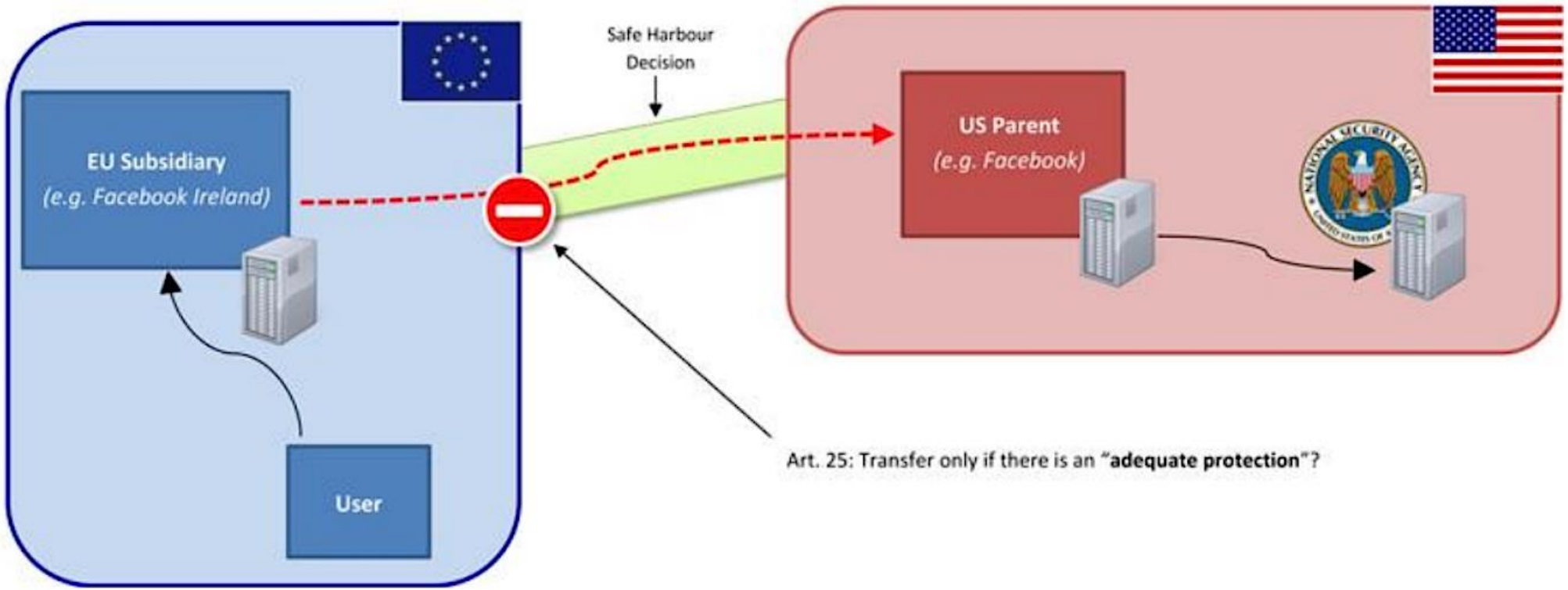
- EU Commission website - *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)*

Transfers to 3rd countries

- ***Articles 49: Derogations***

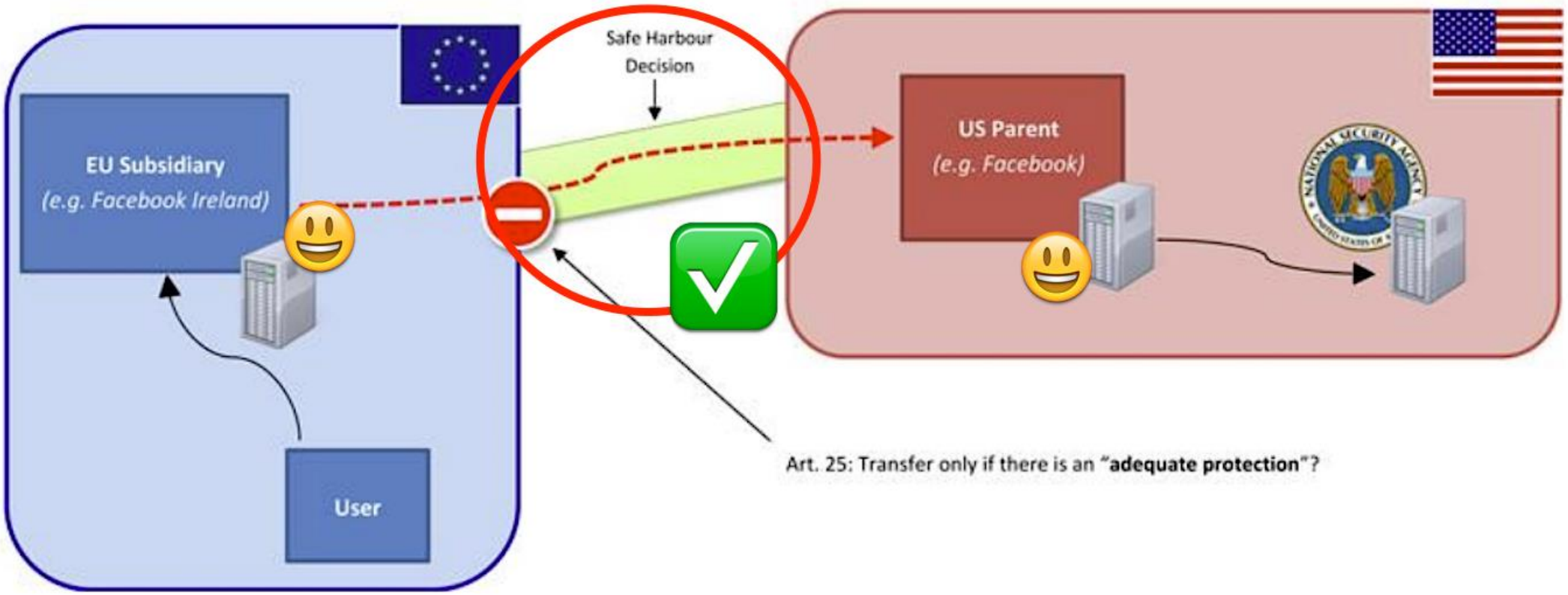
- Available only if data cannot be safeguarded
- For occasional, ad hoc transfers only
- Decision must be made and documented for each transfer

The Schrems I decision regarding transfers of data



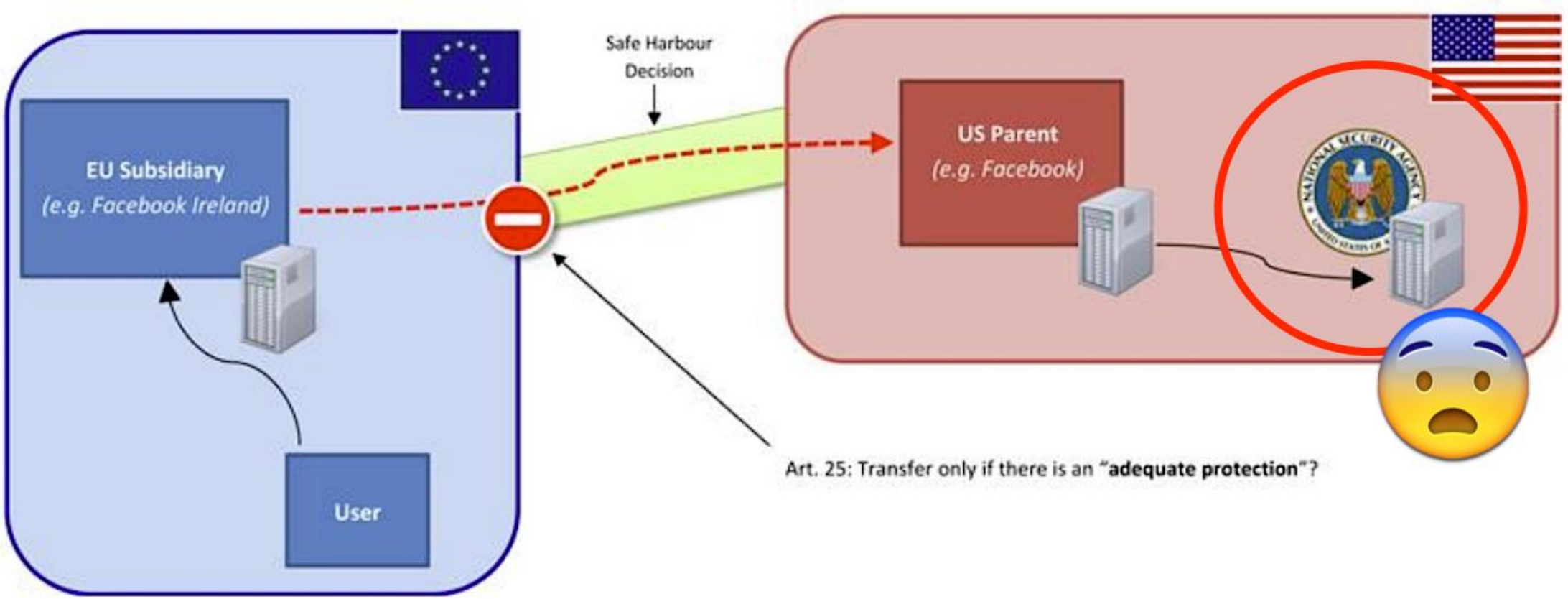
As told by ***Business Insider India***, 2015

The Schrems I decision regarding transfers of data



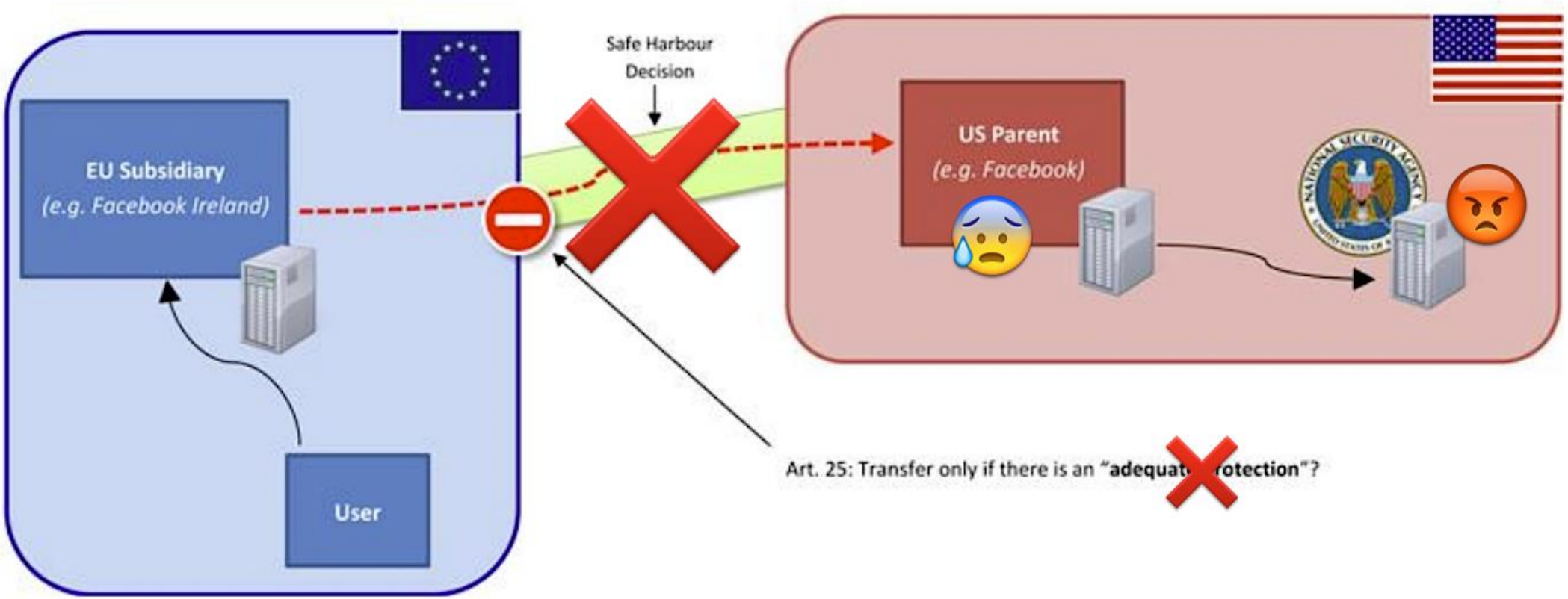
As told by ***Business Insider India***, 2015

The Schrems I decision regarding transfers of data



As told by ***Business Insider India***, 2015

The Schrems I decision regarding transfers of data



As told by ***Business Insider India***, 2015

Review the Schrems timeline: 2016-now

2000:
Principles were developed between 1998-2000

Framework deemed adequate (***"Safe Harbor decision"***)

Self-certification; managed by FTC

2002 review indicated issues

2013:
Max Schrems files a complaint about Facebook in the High Court of Ireland

Concerned USA intelligence services

2015:
Safe Harbor decision **invalid**

2016:
EU-US Privacy Shield adopted by EU Commission

2017:
E.O. 13768

2020:
Privacy Shield **invalid**

SCCs subject to review

Privacy Shield Framework

Review the Schrems timeline: 2016-now

- **First:** Safe Harbor Agreement, July 2016
  - Binding data transfer framework
- **Second:** EU-US Privacy Shield, July 2018
  - Governs the transfer, handling, sharing, and use of EU residents' personal data within the U.S.

- **Schrems II:** Article 45: transfers on the basis of an adequacy decision
- Privacy Shield is incompatible
  - Section 702 of the FISA and E.O. 12333
  - Lack of rights = not an adequate level of protection

- **What does it mean for companies?**
  - Legal uncertainty
  - Injunction (stop intl. data transfers)
  - SCCs must ensure adequate safeguards

What does it mean for companies?

Is anyone going to enforce the ruling?

- Awaiting European Data Protection Board guidance
- Irish Data Protection Commissioner has told Facebook to stop transferring data to US
- Berlin (part of Germany) data protection authority has asked organisations to relocate data back to EU
- Baden-Württemberg (part of Germany) data protection authority has issued detailed guidance
- Netherlands stated organisations should not transfer data to US
- Finland investigating
- ...etc

Implications for EU and US data controllers

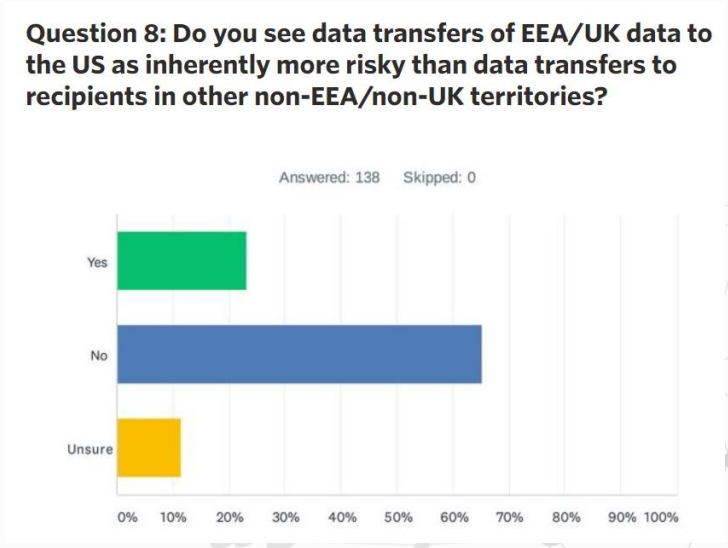
NOYB has written in personal capacities to 30 business asking how they are responding to the CJEU Schrems decision.

Opening Pandora's Box: Companies can't say how they comply with CJEU ruling

Following the Court's judgment in Case-C-311/18 ("Schrems II") on the Privacy Shield and Standard Contractual Clauses, the *noyb* team and some of our members reached out to 33 companies and services that they use on a personal basis to ask them how *they* were approaching international data transfers. The responses that we received ranged across the spectrum: from good, to bad, to shocking. We've now compiled a report for the public that details these responses.

Scroll through the collected responses from companies in this 45-page report (PDF) spanning from Airbnb to Zoom

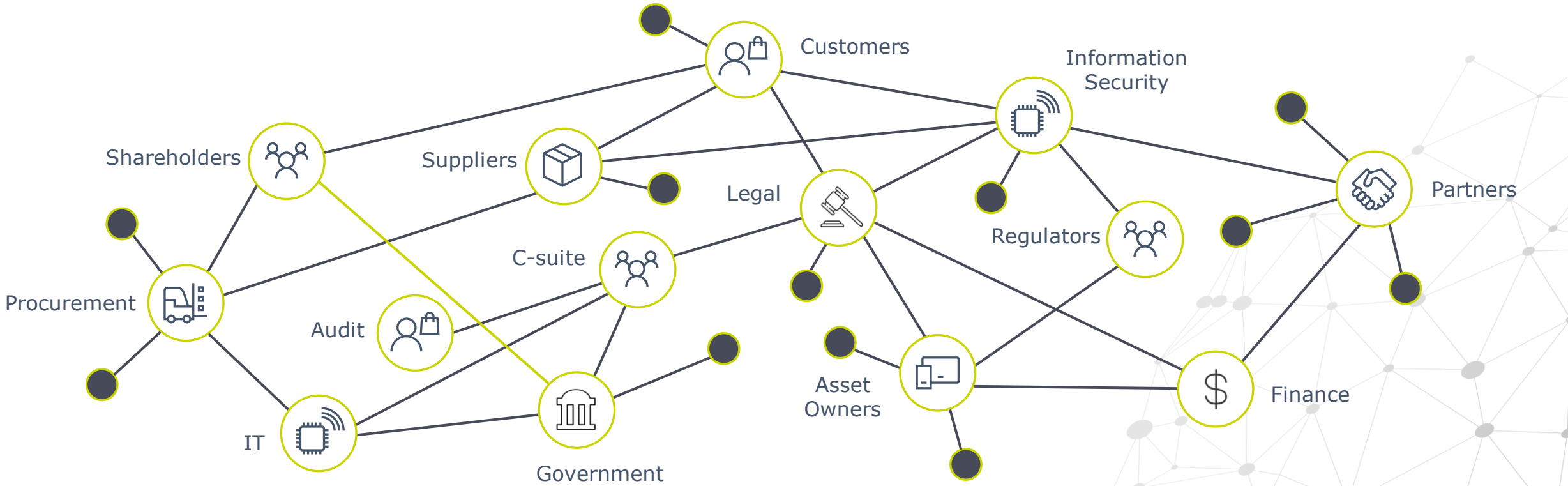
Check out the press release (PDF)



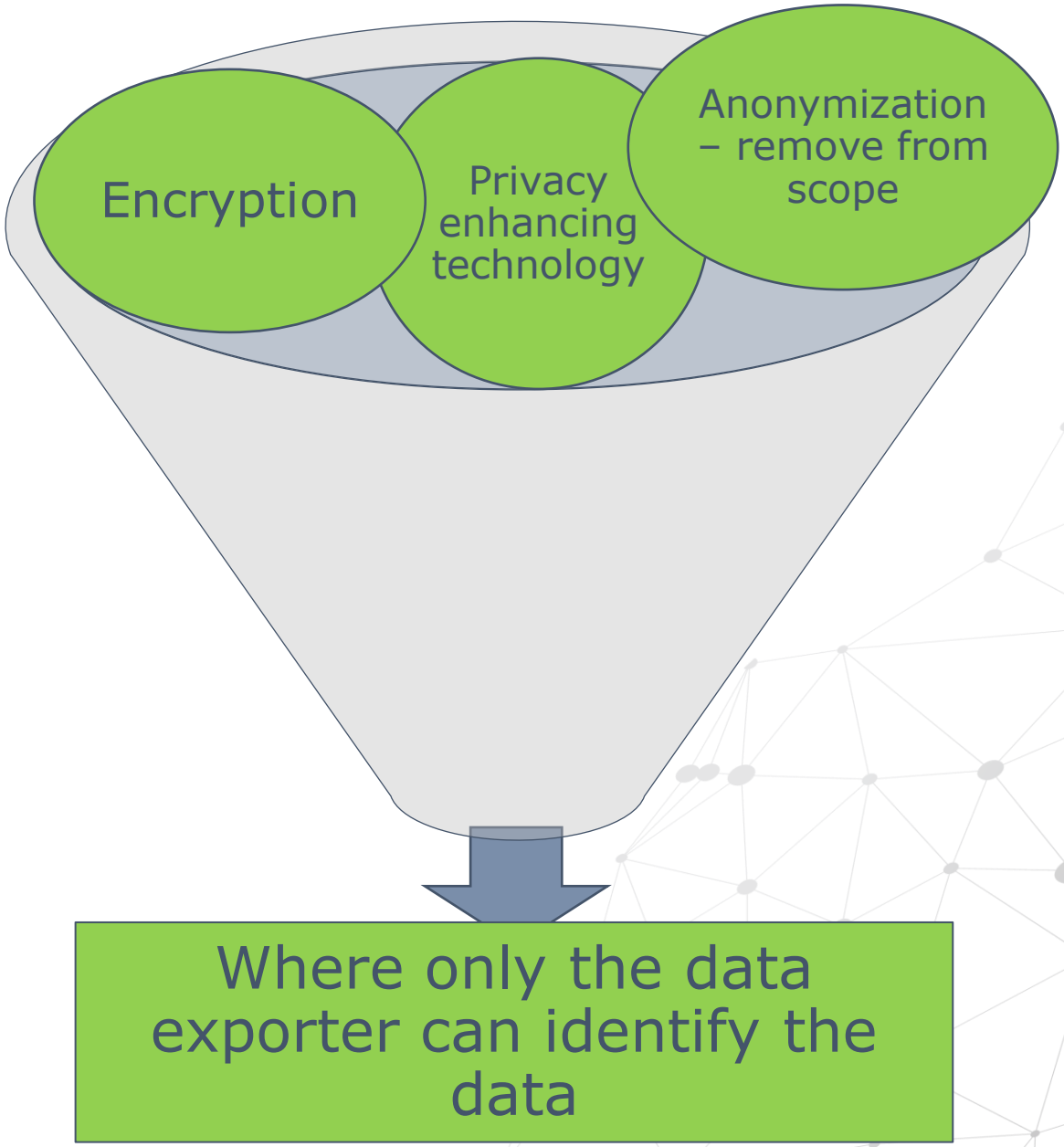
Data transfers - alternatives

Where does the data flow?

Legal basis needed for transfers outside the EU



Transfer the information – not the personal data



Practical steps to take now

Next steps – EU organisations

- Review Article 30 Records of Processing
  - Up to date?
  - Privacy Shield?
  - All requirements for other bases met?
  - 'Necessity' established?
- Risk assess your data transfers
- Consider options
- Implement any necessary changes

Next steps – third country organisations

- Establish geographic origin of data and lead supervisory authority
- Understand your clients' concerns and plans
- Prepare a statement for data exporters
  - Adequacy of legal framework
  - Your compliance with requirements
- Establish business impact of changes and build a plan

Next steps

1. **Identify your GDPR compliance gaps by** conducting a detailed gap analysis

2. **Review our *free* PDF and other materials**: The GDPR compliance checklist

3. Create a personal information inventory and map data flows

4. Ensure data flows are compliant with GDPR Data Transfer Assessment

How we can help

Questions you're going to have to answer, sooner or later – buy our transfer assessment service today to help get yourself out of the firing line….

The data rights testing service is an assessment. We can also offer a service to help clients answer the questions - that's more similar to the data transfer service assessment

How we can help

Remain compliant with the GDPR (General Data Protection Regulation) when transferring personal data outside of the European Union, following the Schrems II privacy ruling.

Gain knowledge of the Regulation and a list of priorities, a practical understanding of the tools, and methods for implementing and managing an effective compliance framework.

This service provides an assessment of your organization's current level of compliance with the Regulation, and helps identify and prioritize the key work areas that your organization must address.

The EU representative service enables companies in North America that fall within the scope of the GDPR to meet their obligations under Article 27.

View our full range of GDPR products here >>

Questions

Protect • Comply • Thrive

Contact us

- Identify the main challenges you're facing; and
- Discuss possible gaps in your privacy and how to comply with Schrems II.

Visit our website
www.itgovernanceusa.com

Email us
servicecenter@itgovernanceusa.com

Call us
1 877 317 3454

Join us on LinkedIn
/company/it-governance-usa-inc/

Follow us on Twitter
/ITG_USA

Like us on Facebook
/ITGovernanceUSA/

Thank you

Protect • Comply • Thrive