IT Governance webinar

Brexit and Schrems: practical implications for UK-EU data transfers

Date: 19 November 2020

Presented by:

- Camilla Winlo, Director of Consulting Services, DQM GRC
- John Potts, Operations Director, GRCI Law

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

Introduction

John Potts

Operations Director

GRCI Law

- Data protection professional with a wealth of experience gained as Head of Information Rights and then Head of Information Law and Security with the UK Metropolitan Police Service.
- UK police service lead for data protection matters relating to the agreement for the exchange of biometric data across EU member states.
- Member of the NPCC GDPR Reform Group, which was responsible for introducing the GDPR and the Law Enforcement Directive to the police service.

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

Today's Discussion

1. Brexit and the Schrems II decision regarding transfers of data
2. The implications UK and EU data controllers face for data transfers
3. Data transfers - options
4. Data transfers - alternatives
5. Practical steps organizations can take now
6. What the future of Brexit might bring

Why are we here?

Data! Data! Data!

Interesting times...

16 July

Schrems II decision – CJEU invalidates Privacy Shield

6 Oct.

CJEU rules UK Regulation of Investigatory Powers Act (RIPA) unlawful

8 Oct.

DCMS writes to organisations warning that they may need to take extra steps to keep data flowing after Brexit

11 Nov.

EDPB issues new guidance on international transfers

12 Nov.

EDPB issues new SCCs for consultation

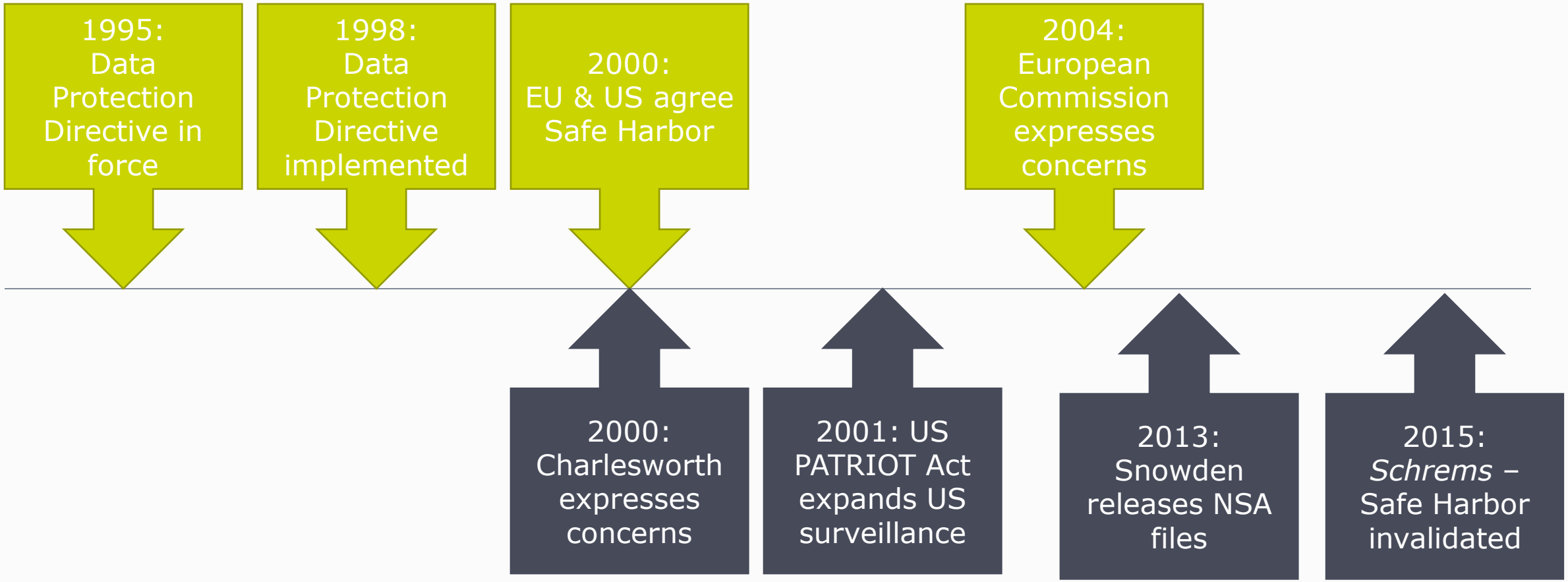
10 Dec.

SCC consultation period ends.

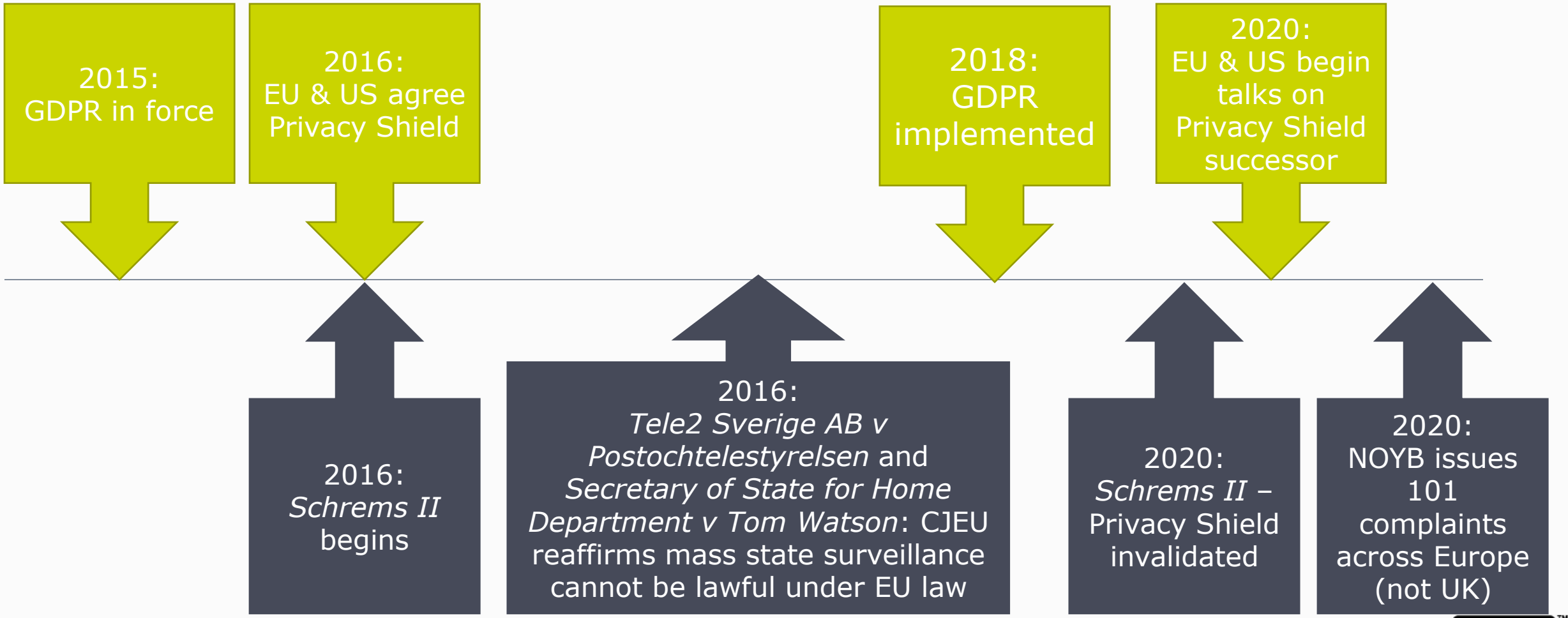
31 Dec.

UK will leave EU

Schrems – Safe Harbor falls



Schrems II – Privacy Shield falls



Brexit – future status of the UK

Adequate

Brexit – future status of the UK

Third Country

- EU does not make a decision in time,

OR

- EU decides UK is not Adequate

What do we need to do if the UK becomes a Third Country?

EU Representative?

Lead Supervisory Authority?

Standard Contractual Clauses?

Implementation Actions

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

Do I need… EU and UK supervisory authorities?

Role

- **Monitor and enforce** compliance with the GDPR
- Provide **guidance** and promote **awareness**
- **Cooperate** with other supervisory authorities
- Receive **complaints** from data subjects and other bodies
- ICO in UK
- Most appropriate in EU

Do I need... Standard Contractual Clauses

Role

- Basis for **routine transfers**
- **Ensure** compliance with GDPR in third countries
- Specify **responsibilities**
- **Ensure** data subjects can exercise their rights
- Data Controllers **accountable for compliance**

Data transfers – options

Options for data transfers

Routine transfers

- Adequacy decision
- ~~Safe Harbor~~
- ~~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 third countries

Article 45: Adequacy decisions

- European Commission decides country's laws are Adequate – 12 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 third countries

Articles 46 & 47: SCCs and BCRs

- Standard Contractual Clauses adopted by European Commission / UK Parliament
  - Sets for Data Controllers and Data Processors
  - Must be included in full
  - Compliance must be assured
  - New clauses issued for consultation but unlikely to be ready for Brexit
- 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)*

European Essential Guarantees for Surveillance Measures

Guarantee A

Processing should be based on clear, precise and accessible rules

Guarantee B

Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

Guarantee C

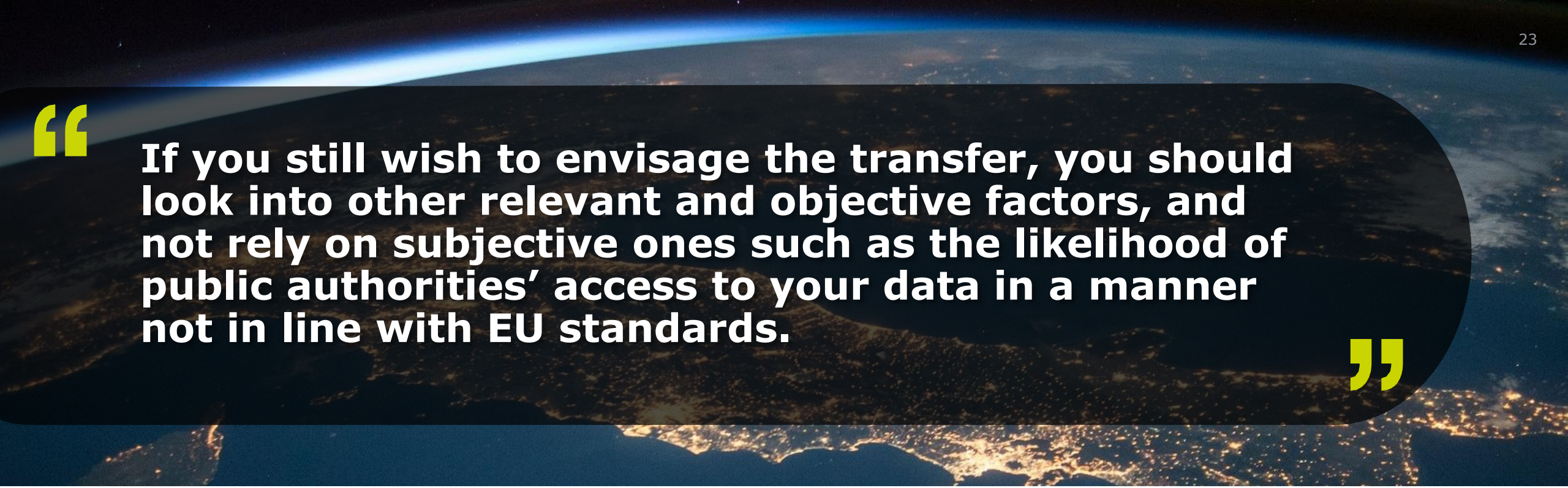
Independent oversight mechanism

Guarantee D

Effective remedies need to be available to the individual

How likely is a country to meet the guarantees?

Six steps for international transfers



> **If you still wish to envisage the transfer, you should look into other relevant and objective factors, and not rely on subjective ones such as the likelihood of public authorities' access to your data in a manner not in line with EU standards.**

Supplementary Measures

EDPB **does not** take a risk-based approach

→

Strong encryption preventing the data being accessed in transit or by the recipient

→

Privacy Enhancing Technologies preventing identification of the individual

Most transfers are off limits

Transfers to third countries

- ***Article 49: Derogations***

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

What does it mean for companies?

Is anyone going to enforce this?

Schrems II:

- EDPB guidelines are really strict
- 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

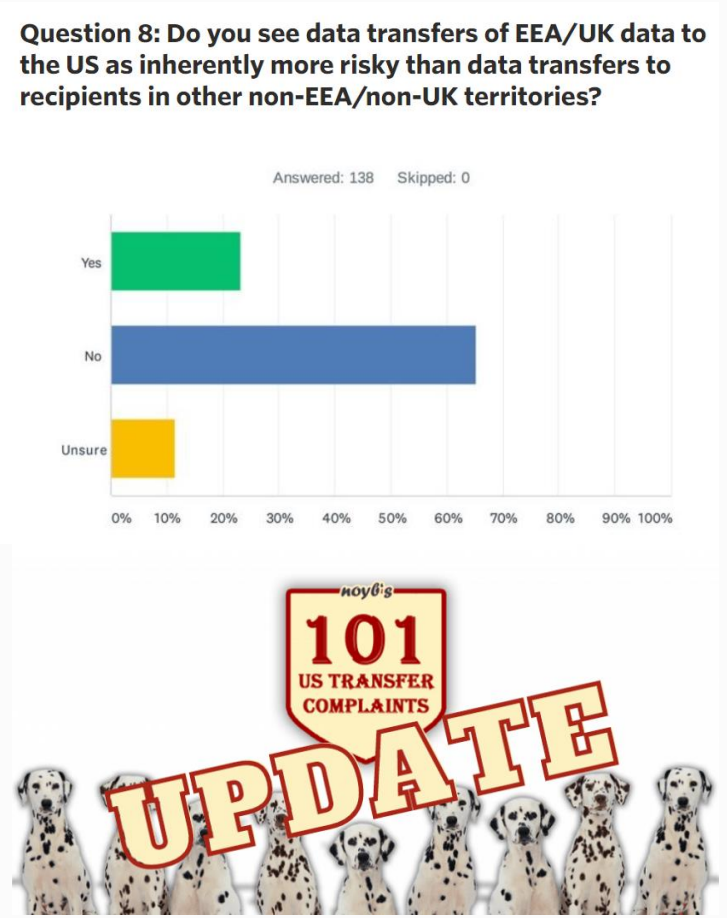
NOYB has written in personal capacities to 30 business asking how they are responding to the CJEU Schrems decision.

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

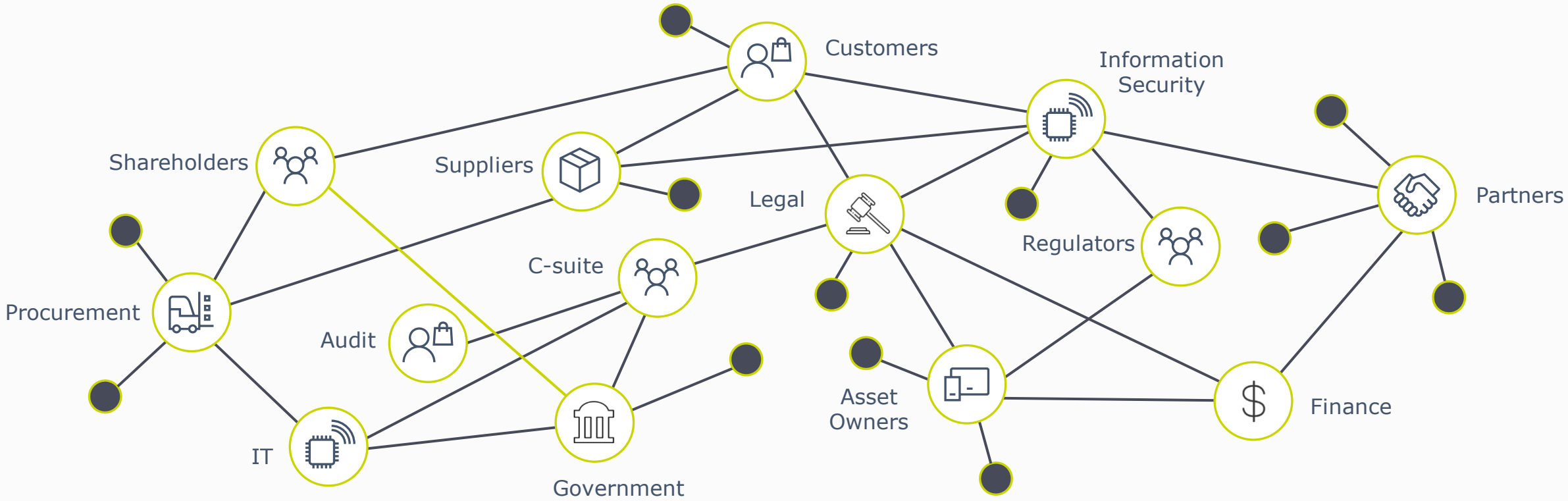
Check out the press release (PDF)



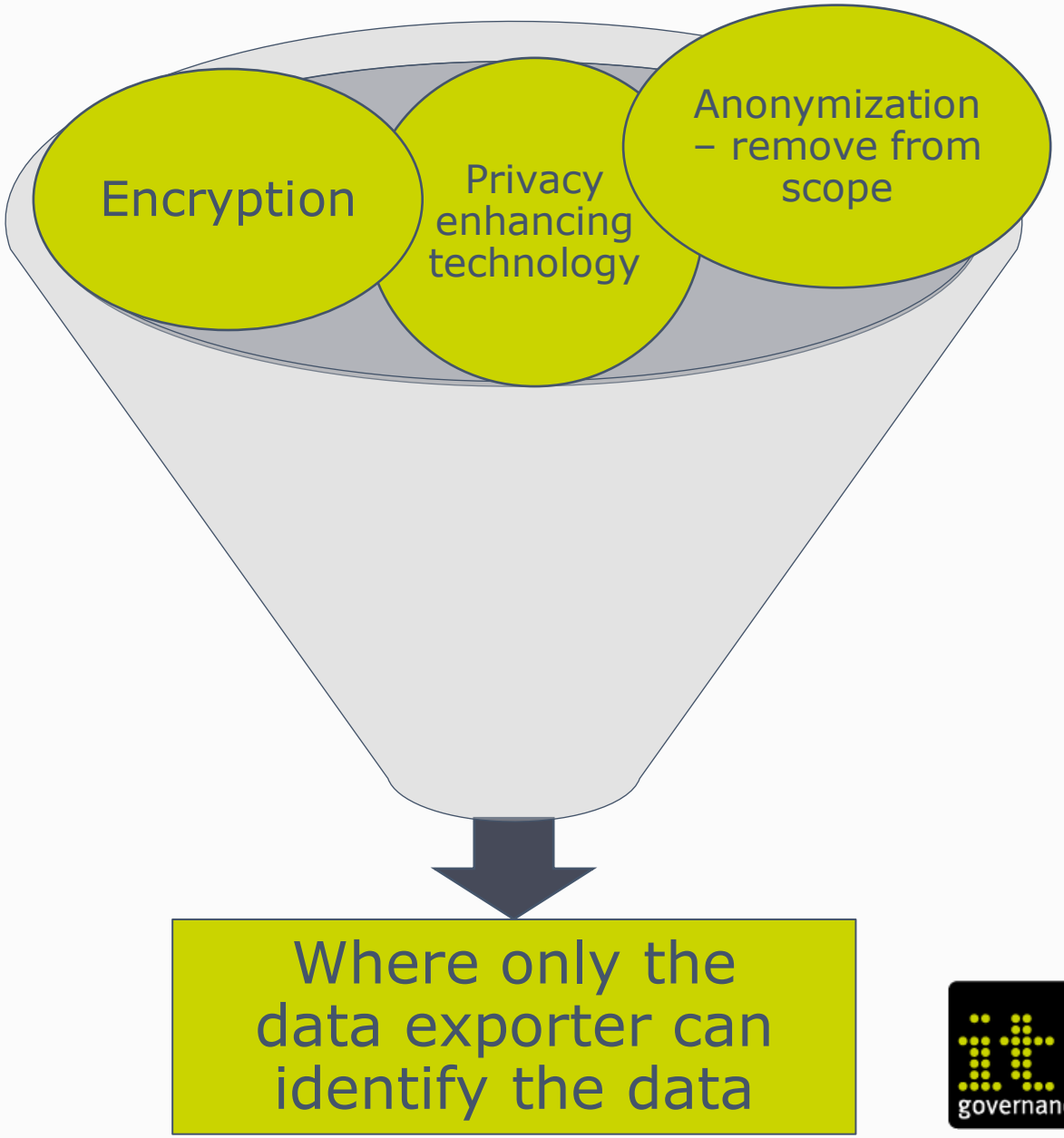
Data transfers - alternatives

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 – UK & third country organisations

- Appoint an EU Representative if needed
- Identify an EU Lead Supervisory Authority if needed
- Complete implementation actions
- Map or review your data flows and process flows
- Establish lawful basis and supplementary measures required and create implementation plan
- Update business continuity plans
- Update DPIAs and Records of Processing

EU–US GDPR Data Transfer Assessment and Action Plan

Next steps – EU organisations

- Appoint a UK Representative if needed
- Register with the ICO and pay the fee if needed
- Complete implementation actions
- Map or review your data flows and process flows
- Establish lawful basis and supplementary measures required and create implementation plan
- Update business continuity plans
- Update DPIAs and Records of Processing

EU–US GDPR Data Transfer Assessment and Action Plan

Next steps

Appoint an **EU Representative** or **UK Representative**

Identify implementation actions with **our Brexit Checklist** and **GDPR Data Transfer Assessment**

Map your data flows and update your docs with a tool such as **Cyber Comply**

Update your business continuity plans **Business Continuity Health Check**

How we can help

Gain an overview of the key changes to GDPR and DPA 2018 after Brexit and look at the practical implications of those changes.

Appoint an EU Representative to legally handle all matters relating to your organisation's data. This service will enable you to meet your Article 27 obligations.

This service will help you remain compliant with the GDPR when transferring personal data outside of the European Union, following the Schrems II privacy ruling.

Assess your organisation's data protection preparations following Brexit and identify any gaps with this two-day GDPR and DPA 2018 assessment.

Centralise your compliance activities to improve control and compliance with regulations and frameworks.

Contact us

Visit our website
www.itgovernance.co.uk

Email us
servicecentre@itgovernance.co.uk

Call us
+44 (0)333 800 7000

Join us on LinkedIn
/company/it-governance

Like us on Facebook
/ITGovernanceLtd

Follow us on Twitter
/itgovernance