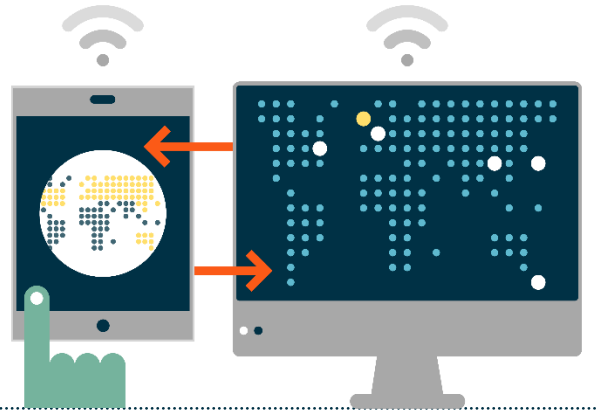
Data transfers – from Schrems II to the recent decisions of the European DPAs

7th Data Privacy & Protection Conference

5th July 2022

What is a "data transfer"?

- **"Transfer"**
  - occurs when a controller or processor subject to GDPR ("exporter") discloses by transmission or otherwise makes personal data available to another controller, joint controller or processor ("importer") outside European Economic Area ("EEA")
  - more than just a physical transfer of personal data (for example, from a server in one country to another)
  - includes **access** to personal data from outside the originating country
- For data storage, it is important to know not just where the **primary server** is located, but also where the **back-up server** is located + who may access to personal data and from which countries
- GDPR will still apply to transferred data



When can transfers be made lawfully?

Transfers of personal data outside the EEA to "third countries" are restricted UNLESS

Adequacy decisions

- So-called "whitelist" (including, *inter alia*, UK, Canada, Japan, Israel)
- Included **EU-US Privacy Shield** (until July 2020)

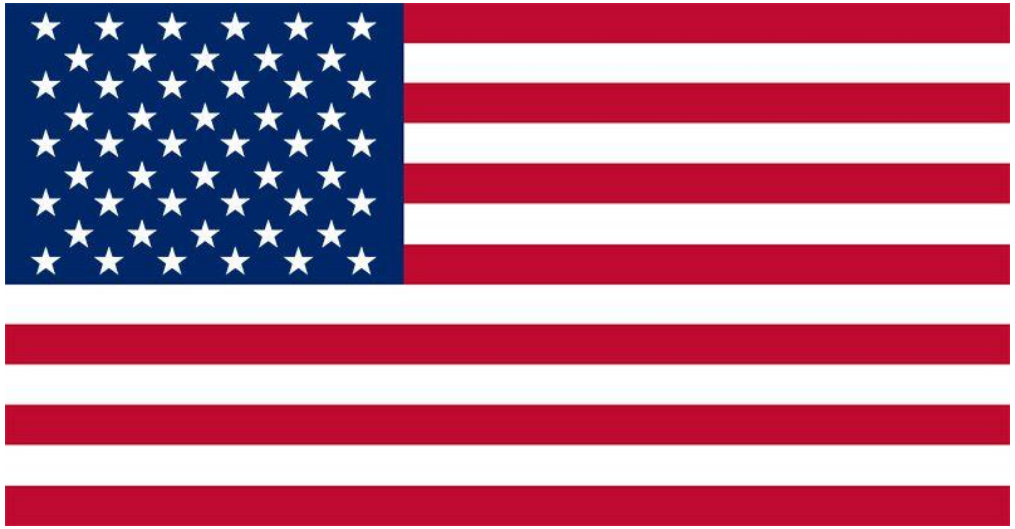
Safeguards

- **Standard Contractual Clauses** ("SCCs" / "Model Clauses")
- Binding Corporate Rules ("BCRs")
- Code of conduct
- Certification mechanisms

Derogations

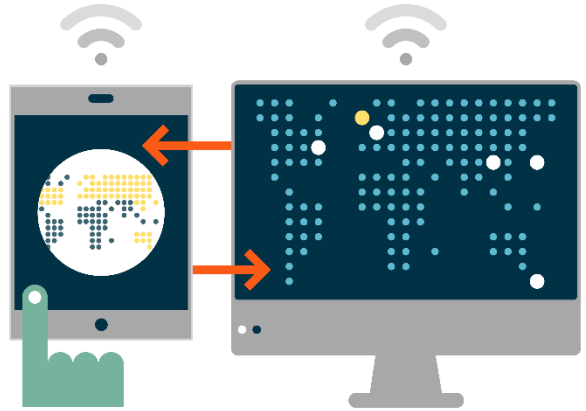
- Explicit consent
- Necessary (specific instances)
- Only on occasional circumstances

Data transfers to US



Data transfers to US used to rely on the so-called "EU-US Privacy Shield", approved following an adequacy decision.

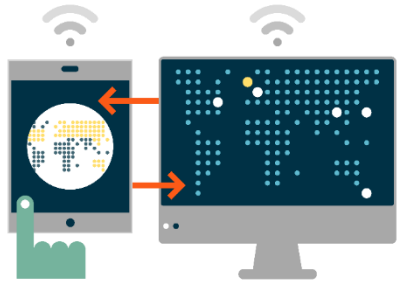
However, the European Court of Justice declared the EU-US Privacy Shield invalid on 16 July 2020 (so-called "**Schrems II**" judgment)



Schrems II

EU-U.S. Privacy Shield

- The CJEU said that the EU-U.S. **Privacy Shield** did not ensure an adequate level of data protection for personal data transferred to the U.S.:
  - Mass surveillance programs of the U.S. authorities, which businesses must adhere to by law, violate the fundamental rights of EU citizens (not limited to what is strictly necessary)
  - EU citizens do not have adequate rights of redress in the U.S. in respect to their personal data (no actionable right before the courts against U.S. authorities)
  - The standards and safeguards provided by both U.S. law and the Privacy Shield fall **far below** those of the GDPR
- Transfers based on the EU-U.S. Privacy Shield are **unlawful**

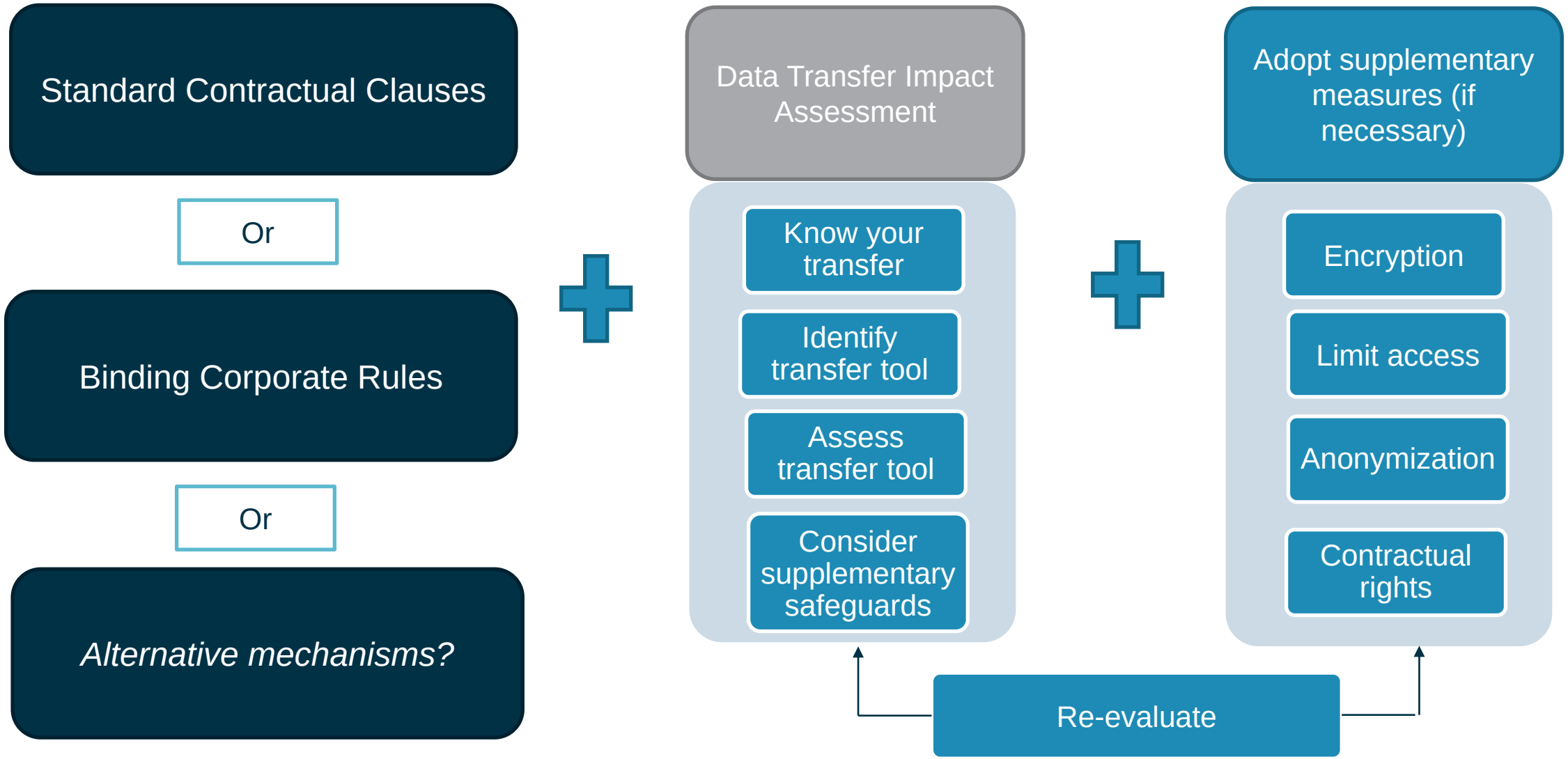


Schrems II

SCCs

- SCCs are valid, but may not be enough by themselves:
  - Exporters and importers must **assess** whether the SCCs can be complied with on a "case-by-case" basis – **Transfer Impact Assessments (TIA)** are becoming more and more commonplace.
  - Assessment must look at a range of factors, including the laws of the importing country, and how they apply to the importer's processing activities.
  - If SCCs are not enough by themselves, have to consider "**additional safeguards**" or "**supplementary measures**".

Appropriate safeguards



1 month after the Schrems II judgment

Timeline

- On **17 August 2020** the NOYB announced the filing of 101 complaints before the data protection authorities of all European Member States. NOYB declared that "*a quick analysis of the HTML source code of major EU webpages shows that many companies still use Google Analytics or Facebook Connect one month after a major judgment by the Court of Justice of the European Union (CJEU) - despite both companies clearly falling under US surveillance laws*".

- On **4 September 2020**, the European Data Protection Board (EDPB) created a task force in order to have a unique approach across Europe to the 101 complaints lodged by NOYB.

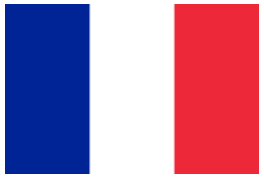
- On **10 November 2020**, the EDPB adopted the *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* for public consultation. "*To help exporters (be they controllers or processors, private entities or public bodies, processing personal data within the scope of application of the GDPR) with the complex task of assessing third countries and identifying appropriate supplementary measures where needed, the European Data Protection Board (EDPB) has adopted these recommendations. These recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place*".

- On **4 June 2021**, by means of the Commission Implementing Decision (EU) 2021/914 a new set of Standard Contractual Clauses was adopted.

Timeline

- On **18 June 2021** the EDPB adopted the final version of the Recommendations 01/2020.
- **During 2022** the first decisions following the 101 complaints began to be published.
- On **13 January 2022**, the Austrian authority (DSB) issued the first decision on NOYB's complaints and declared the transfer of personal data related to the use of Google Analytics unlawful. Additional technical and organisational measures taken by Google are not sufficient where U.S. authorities can still access citizens' data.

- **10 February 2022**, the French authority (CNIL) announced the first of three decisions related to NOYB complaints. The French authority also found that the transfer of personal data to the United States made as part of the Google Analytics service failed to comply with the GDPR. One was is given to comply with the decision. According to the CNIL, the investigation would also cover other tools involving the transfer of data abroad, and further action may be taken in the future. The CNIL issued two more decisions on **2 March 2022**.



- On **25 March 2022**, the European Commission and the United States announced that they have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the Schrems II decision of July 2020.

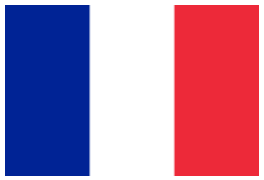
Timeline

- On **6 April 2022**, the EDPB published a statement in which it recalled that the announcement about the Trans-Atlantic Data Privacy Framework was not a valid legal basis and that it would be vigilant to ensure that any new international agreement properly handles the issues raised by the European Court of Justice.

- On **22 April 2022** the Austrian authority clarified that Google Analytics involves the processing of personal data and that the measures taken by Google are not sufficient to prevent access to the information by US government authorities. It also specified that the risk-based approach (how likely U.S. authorities' access is) does not apply to evaluating transfers to third countries, but an analysis on objective factors needs to be put in place (rather considering how likely the US authorities' access might be). The Italian Data Protection Authority also agreed with this view.

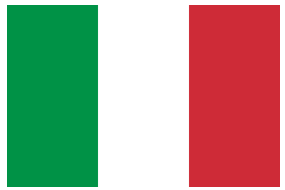
- According to reports on NOYB's website, the Spanish Authority and the Luxembourgish Authority have both closed complaints procedures without commenting on the unlawful use of Google Analytics, as the relevant website stopped using Google Analytics.

- On **7 June 2022** the French authority published guidance on bringing analytics tools into compliance by suggesting the adoption of a proxy server between the website and Google's servers. However, the technical solution put forward by the CNIL must comply with certain requirements so that in no way can the data arriving at Google be linked to identifiable individuals. The CNIL also warned that adopting such a solution may be costly, complex, and may not meet the website operator's operational needs.



Timeline

- By means of the order of 9 June 2022 (published on 23 June 2022), the Italian Data Protection Authority (*Garante per la protezione dei dati personali*):
- declared unlawful the extra-EEA transfer of personal data of website users effected by means of Google Analytics;
- required the website operator to render the processing compliant with the GDPR within 90 days by taking appropriate additional measures;
- required the suspension of the data transfer to Google LLC in the absence of appropriate additional measures taken within the above-mentioned period;
- issued a reprimand to the website operator (without issuing monetary sanctions).



Main issues

- How to carry out a TIA for transfers to US and in general?
- Is consent a valid legal basis for data transfers?
- What will happen?

and a provocative question

Thank you!