THE HOTTEST TOPICS IN CROSS BORDER DATA TRANSFERS

PRIVACY + SECURITY FORUM

SPRING ACADEMY

24 March 2022

orrick

Speakers

Shannon Yavorsky
Partner
Cyber, Privacy & Data Innovation
Orrick, San Francisco / London

Christian Schröder
Partner
Cyber, Privacy & Data Innovation
Orrick, Germany

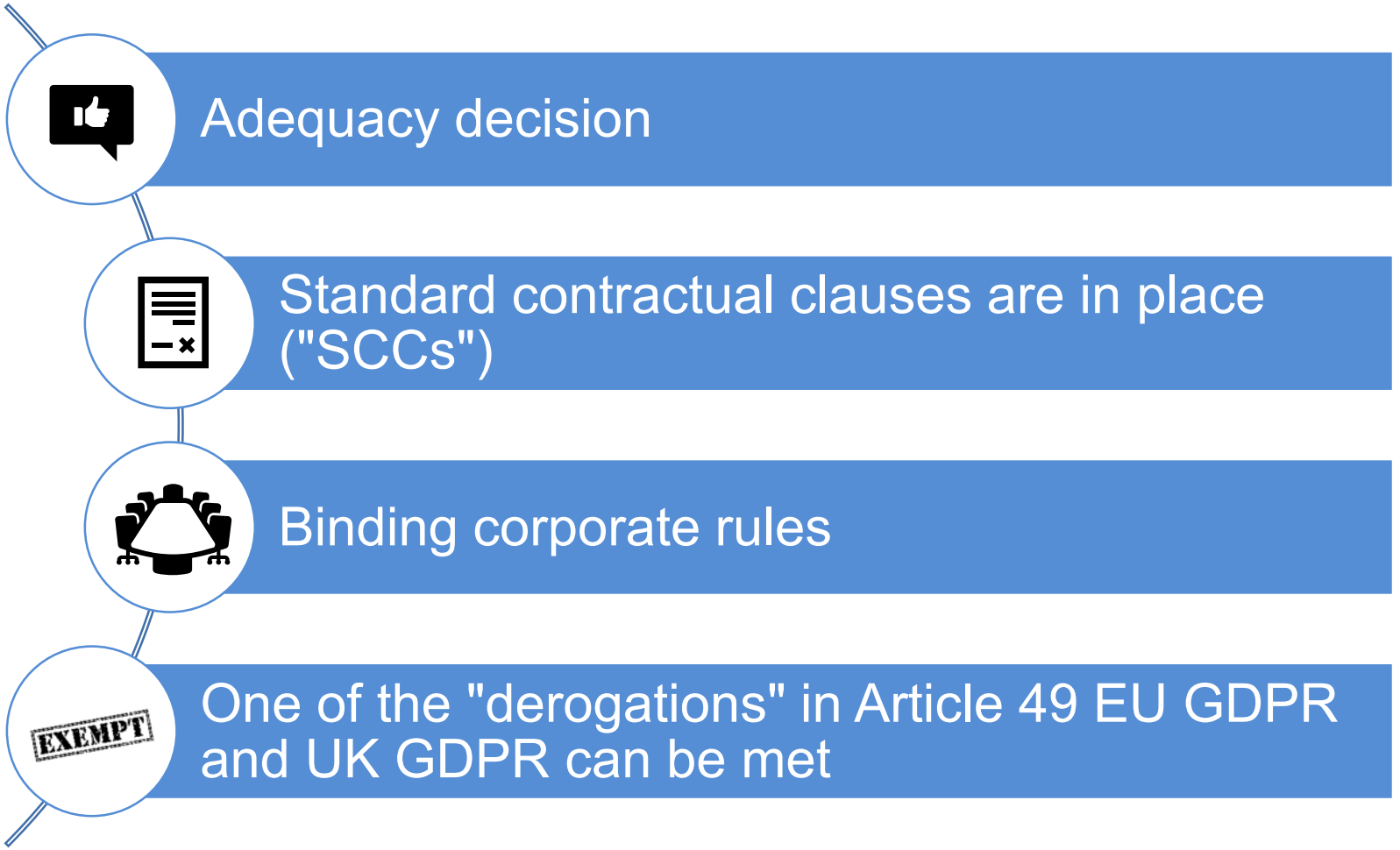
Brandi Bennett
Senior Counsel, Global Data Privacy
Legends International

Cecilia Alvarez
EMEA Privacy Policy Director
Meta

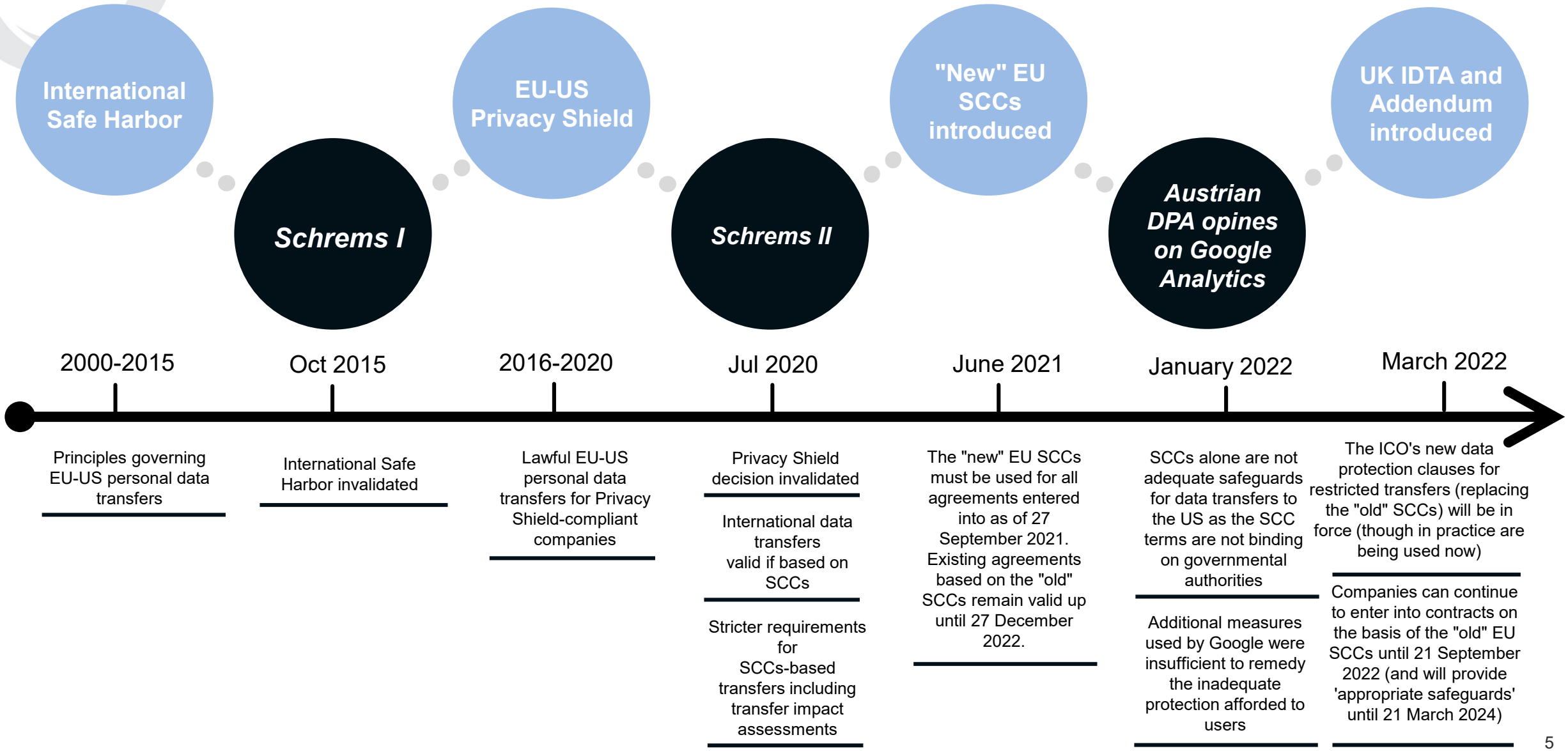
Content

International data transfers

Data transfers to non-EU countries are only permitted under certain circumstances, as set out in Chapter V of the EU GDPR and UK GDPR. For example:

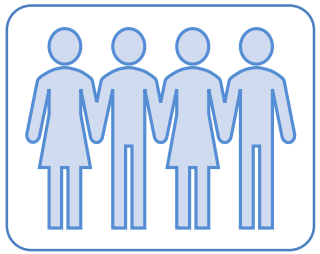


Where are we now with international data transfers?



The Austrian DPA's Google Analytics decision

In summary, the Austrian DPA ruled that the use of Google Analytics violated the EU GDPR in relation to international data transfers (in light of the *Schrems II* judgment)



The data was "personal"

Unique user IDs

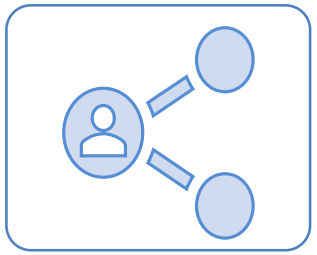
URLs

Device information

IP addresses

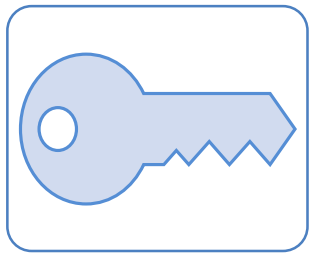
This decision was the first of 101 complaints made by NOYB to European DPAs. It is limited to Austria but there are still many outstanding complaints and it is anticipated this decision will be reflected elsewhere:

- Norwegian and Danish DPAs have responded to the Austrian decision.
- Dutch investigation expected to completed soon.
- French DPA has ordered an unnamed French website manager to comply with GDPR and if necessary, to stop using Google Analytics.



There was a transfer to a third party based outside of the EU

The personal data was processed and transferred to Google LLC in the US through Google Analytics thus triggering "international data transfer" obligations under the EU GDPR



Insufficient steps were taken by Google (the processor) to protect the personal data

The SCCs alone were not sufficient (note: "old" EU SCCs used but "new" EU SCCs still unable to address shortcomings)

Supplementary measures (encryption of data (however, Google holds the key)), regular publication of transparency reports and possible notification of individuals affected by requests) used by Google did not provide appropriate safeguards for the transfer of personal data to the US as intelligence agencies would have generally been able to access the transferred personal data

Whilst no guidance was given by the Austrian DPA, potential ways to mitigate could be:

Ask for consent to the use of Google Analytics and to international data transfers (e.g. in cookie banners)

and

Turn on any Google Analytics data anonymisation features (though this is not true "anonymisation")

and

Find alternative analytics providers in the EU

What do the "new" EU SCCs cover?

More than two parties can adhere to contract terms with the "new" EU SCCs and additional controllers and processors can be added to the contract

Parties must warrant that at the time of agreeing to the "new" EU SCCs, they have no reason to believe that the laws and practices application to the data importer are not in line with "new" EU SCC requirements (note: Reflects *Schrems II*)

Obligation to conduct a **transfer impact assessment** which assesses of the relevant laws and practices in the data importer's country based on the circumstances of the transfer (note: Reflects *Schrems II*)

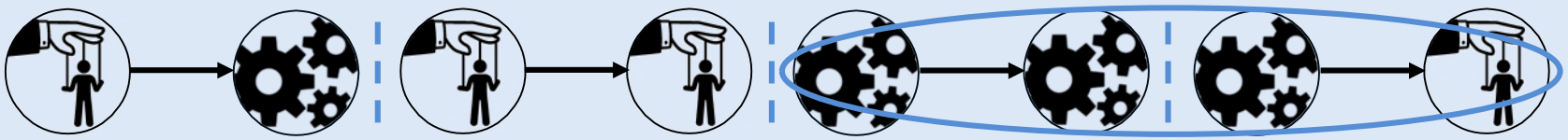
Obligations on the importer in relation to government access requests (e.g. notifying the exporter and information about a request, if they are able to under applicable law; assessing whether the request can be challenged and if it can, doing so) (note: Reflects *Schrems II*).

Modules two and three (for controller to processor transfers, and processor to subprocessor transfers) already contains Article 28 terms

In practice: Parties should carry out a data / transfer mapping exercise prior to transferring any personal data to understand, potentially limit and helping monitor on an ongoing basis transfer flows – the "new" EU SCCs require a lot of detail

In practice: All new intra-group agreements and vendor agreements involving international data transfers now need to contain the "new" EU SCCs

The new SCCs are "modular". Organisations need to establish what "module" of the SCCs needs to be used. This depends on whether a party to the SCCs acts as a controller or a processor:



These data transfers were not considered in the "old" SCCs

Why is there already a need for "new new" EU SCCs?

1. The new SCC cover transfer constellations in which the importer is not subject to the GDPR	2. Chapter V applies to importers subject to the GDPR by virtue of Article 3(2) GDPR as well	3. Importers subject to the GDPR by virtue of Article 3(2) GDPR are not covered by the new SCCs
Article 1 of the SCC Implementing Decision states that the SCCs covers only the transfer by a controller/ processor subject of the GDPR to a controller/ (sub)processor not subject to the GDPR.	The EDPB clarified that a transfer merely requires that the importer is in a third country, irrespective of whether it is also subject to the GDPR by virtue of Article 3.	Importers (be it controller or processor) subject to the GDPR by virtue of Article 3(2) GDPR are not covered by the current SCCs, hence the need for additional, supplementary SCCs that address this specific transfer constellation.

The EU Commission has confirmed to be in development of additional SCCs for Article 3(2) importers

Recommendations for international data transfers

The "new" EU SCCs help address some of the concerns raised in the *Schrems II* judgment, but that's not the end of the story…

Follow the EDPB's 'six-step test'

1. Know your transfer (i.e. transfer mapping)
2. Identify your transfer tools (e.g. SCCs)
3. Is the Article 46 EU GDPR and UK GDPR transfer tool effective?
4. Adopt supplementary measures
5. Procedural steps
6. Re-evaluate data transfers at intervals

Step 3

"Transfer impact assessment"

These assessments should be **reviewed on an ongoing basis** and demonstrate the European Essential Guarantees are respected in the importer's country:

- Data is being processed based on clear, precise and accessible rules
- There are legitimate interests being pursued
- There is an independent oversight mechanism in place
- There are effective remedies available to the individual

Step 4

Ensuring data is adequately protected

This covers technical, organisational and contractual matters and can include:

- Ensuring data is pseudonymised or anonymised (if possible)
- Encrypting data (key retained by the exporter only)
- Requiring contracting parties to provide guarantees
- Draft technical measures into contracts

Transfer impact assessments in a nutshell…

- Exporters must assess, in collaboration with the importer, if there is anything in the law and/or practices in force in the importer's country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool (e.g. SCCs), in the context of the specific transfer.
- The assessment required must be based first and foremost on legislation publicly available, but can take into whether the laws are likely to apply in practice based on the circumstances of the transfer (and in addition, the practical experience of the importer).

What are we seeing practically?

Importers

- Providing FAQs to exporter customers for up-front reassurance and contractual addendums (e.g. Microsoft's 'Defending Your Data' initiative)
- Assisting exporters to carry out transfer impact assessments (contractually obliged to do so under the "new" EU SCCs)

Exporters

- Issuing requests for information to carry out assessments of international transfers (see NOYB's model requests)
- Data and transfer mapping - reviewing Article 30 GDPR records of processing to assess transfers and controller/processor positioning

Data localisation

- For example, Microsoft will allow its EU cloud services customers to keep data in the EU ('EU Data Boundary')

→ **However, data localisation can be expensive and doesn't necessarily solve the issue**

Direct Collection

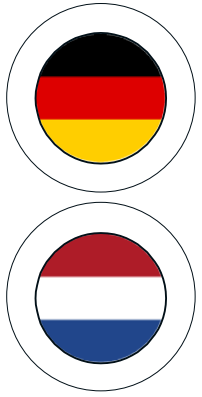
- The EDPB clarified that a so-called “direct collection” of personal data from individuals in the EU does not constitute a transfer within the meaning of Art. 44 GDPR.

→ **Companies should still be mindful of other GDPR principles, including Art. 32 & 48.**

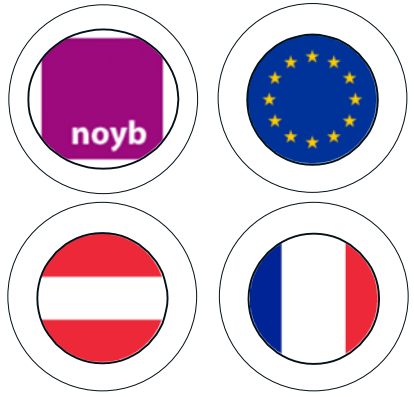
'Transfer impact assessments' and FAQs are not static documents and are intended to be reviewed on an ongoing basis - they should not "sit on the shelf".

Regulatory response to *Schrems II* – so far…

Bavarian DPA calls for German company to cease the use of the 'Mailchimp' tool



Advice from Berlin, Hamburg and Dutch DPAs to halt transfers to the US



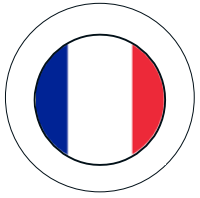
NOYB filed 101 complaints concerning the use of Google Analytics and Facebook Connect in 30 EU/EEA states

The Austrian DPA found that the use of Google Analytics on the basis of SCCs did not provide for appropriate safeguards (January 2022)

The French DPA (CNIL) came to similar conclusions (February 2022)

Other DPAs (Denmark, Norway, Guernsey, Netherlands) are expected to follow this decision

The EDPS reprimanded the European Parliament for using Google Analytics and other tracking tools that transfer data to the U.S. on its websites used for conducting COVID-19 tests (January 2022)



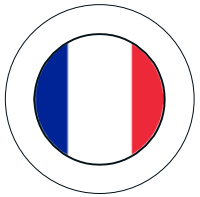
Conseil d'Etat's refusal to suspend Microsoft's hosting of public health data lake, despite CNIL opinion

Conseil d'Etat's ruling that personal data on an AWS-hosted platform to book COVID-19 vaccinations was sufficiently safeguarded (note: processor in the EU a subsidiary of a US company – no transfer of data to the US)

Suspension of data flows to the US (Census 2021)

What to expect in the future?

Continued enforcement of Schrems II



The CNIL has announced it will look further into transfer compliance when employing cloud computing (February 2022)

In addition, 8 out of 15 DPAs listed the topic of international data transfers as one of their priorities in their respective strategic plans for 2022

The majority of NOYB's 101 complaints is yet to be decided on, which gives the EDPB's "101 taskforce" the opportunity to further align the views taken by European DPAs on Google Analytics and Facebook Connect

In Germany, court decisions are slowly emerging that suspended unlawful transfers or awarded damages for using tools that rely on unlawful transfers

Private enforcement is therefore expected to ramp up in the near future in European Member States as well

Other transfer mechanisms

Privacy Shield 2.0

Negotiations on a new Privacy Shield framework are said to be in the final stages of negotiation.
However, there are still many obstacles to pass, including a lack of progress in privacy issues in the U.S. on the federal level.

Codes of Conduct

The EDPB adopted its Guidelines on CoC as a transfer mechanism in February 2022

An Update on Binding Corporate Rules

The EDPB is expected to update its BCR requirements some time in 2022 to

QUESTIONS?


orrick