EU-US Data Transfers:

What you need to know

Emily Jones, Christopher Götz, Olivia Ward and Jan Zücker

24 August 2023

Overview

Agenda

Emily Jones
Partner
San Francisco, US

Christopher Götz
Partner
Munich, Germany

Olivia Ward
Supervising Associate
San Francisco, US

Jan Zücker
Associate
Düsseldorf, Germany

1 Introduction/ Background

2 What is the EU-US DPF?

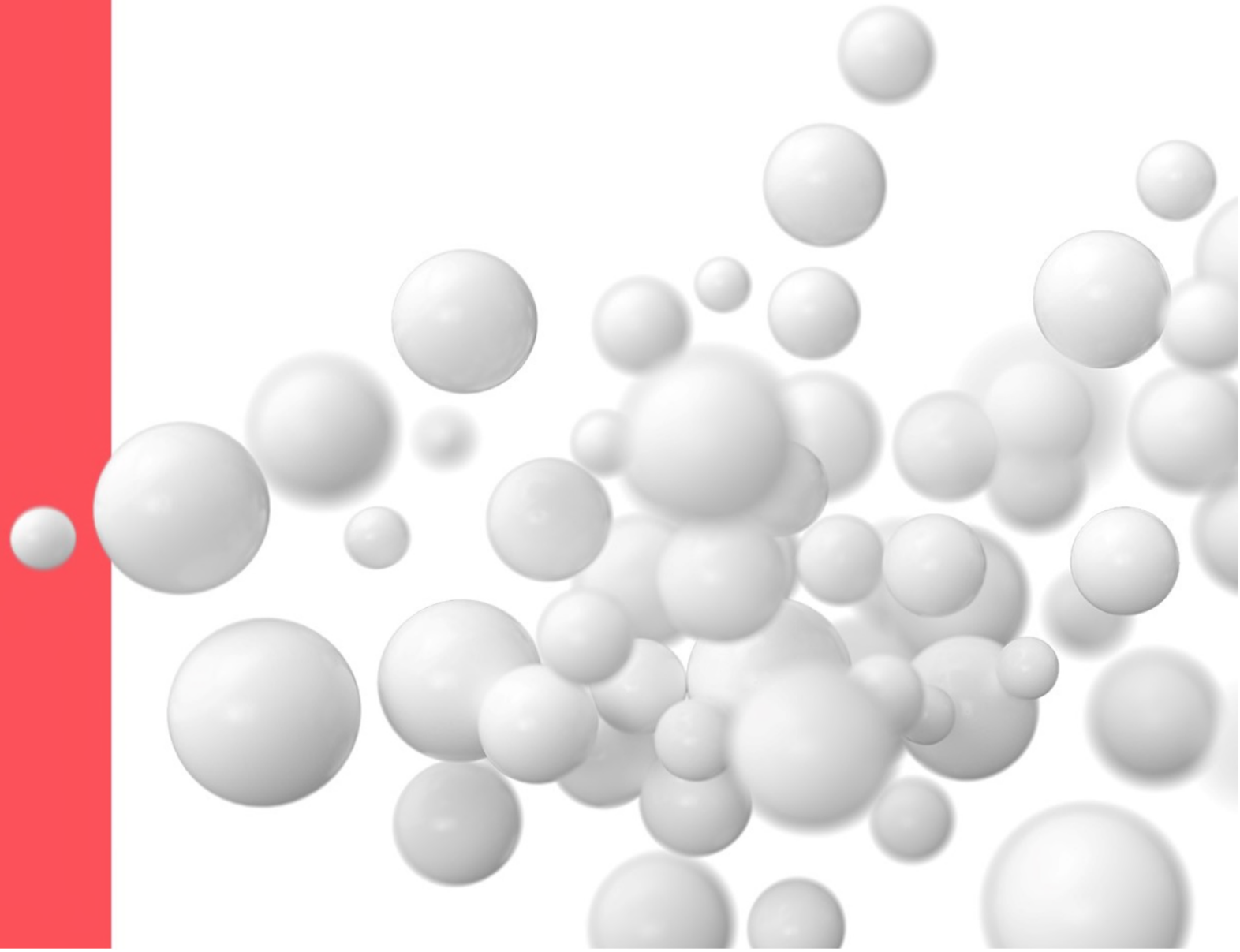
3 Eligibility and sign-up

4 Should I self-certify?

5 Perception of EU-US DPF in Europe

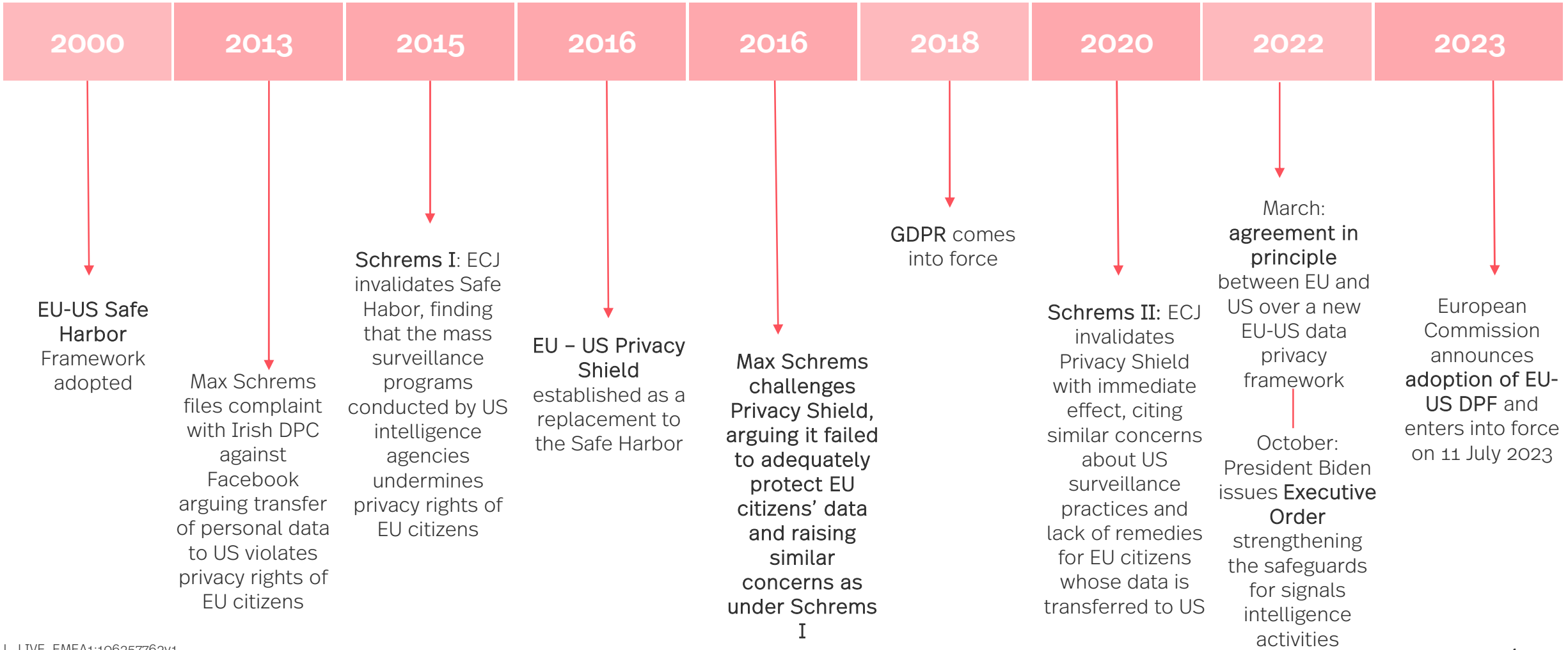
6 Impact on transfers from the UK and Switzerland

Background

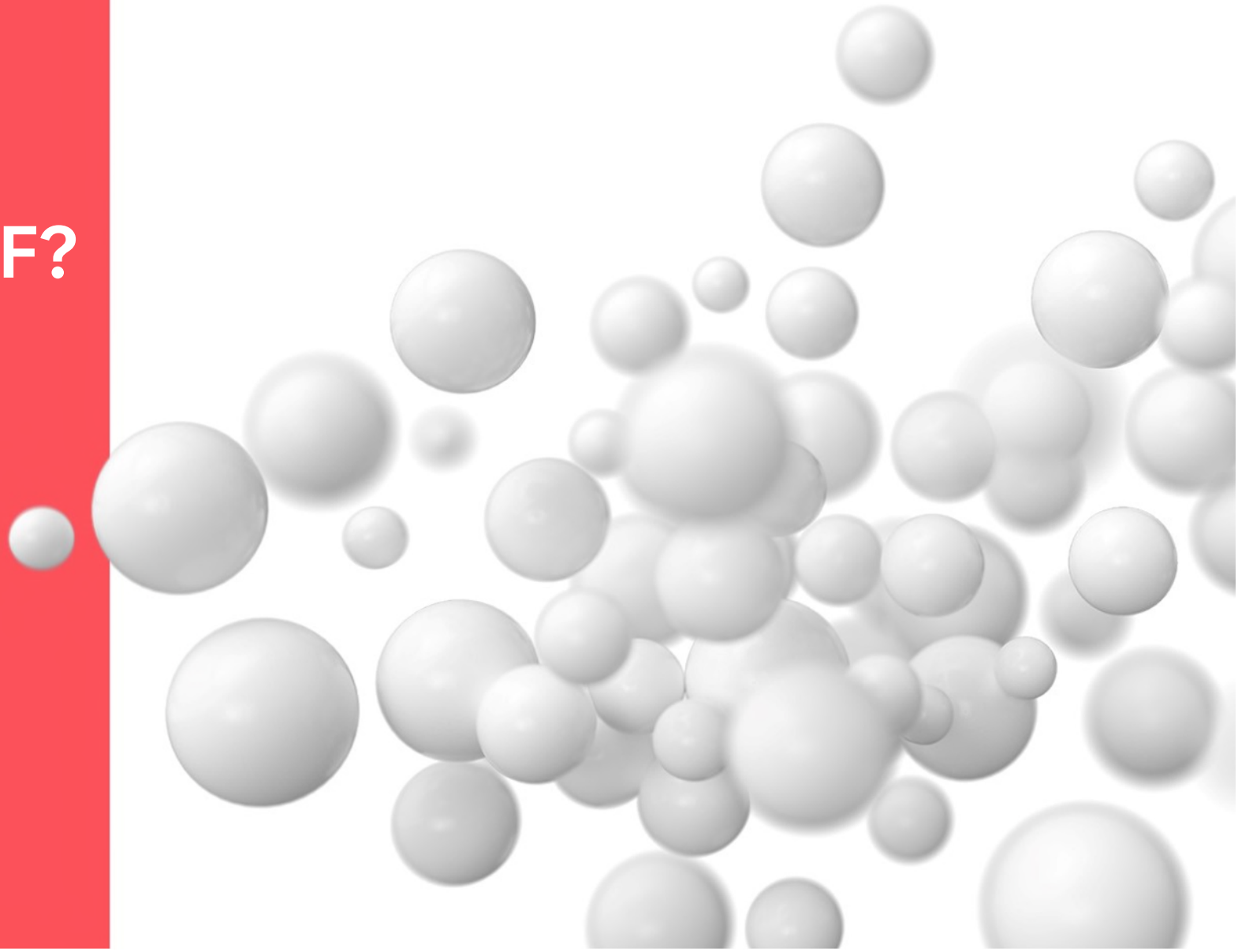


Background

The story so far...



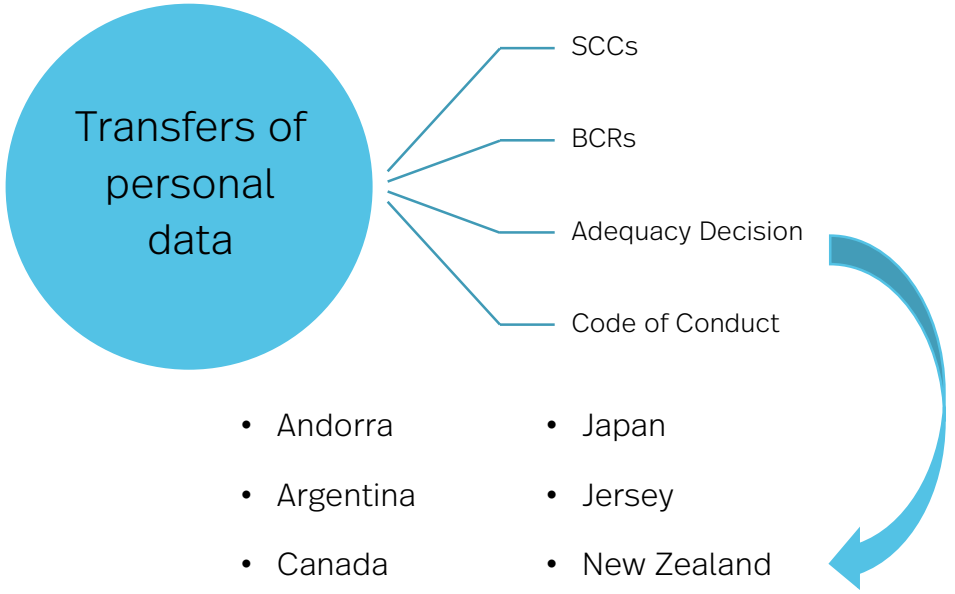
What is the EU-US DPF?



What is the EU-US DPF?

What is the EU-US DPF in essence?

- It is an adequacy decision (a tool to transfer personal data from the EU to third countries offering a comparable level of protection to that of the EU). Other transfer tools include Standard Contractual Clauses, Binding Corporate Rules and Codes of Conduct.
- The adequacy decision concludes that the US ensures an adequate level of protection (compared to that of the EU) for personal data transferred from the EU to US companies participating in the EU-US DPF



- Andorra
- Argentina
- Canada
- Faroe Islands
- Guernsay
- Israel
- Isle of Man
- Japan
- Jersey
- New Zealand
- Republic of Korea
- Switzerland
- United Kingdom
- Uruguay
- **United States (those participating in DPF)**

What is the EU-US DPF?

How does the EU-US DPF differ to the Privacy Shield?

- Schrems II challenge was not focused on the Privacy Shield itself but on concerns about access and surveillance by US state and law enforcement agencies.
- The EU-US DPF addresses some of those concerns raised by introducing new binding safeguards to ensure that:
  - ✓ data can be accessed by US intelligence agencies only to the extent of what is necessary and proportionate; and
  - ✓ there is an independent and impartial redress mechanism to handle and resolve complaints from Europeans concerning the collection of their data for national security purposes.
- EU-US DPF emphasises a higher standard of protection, reflecting GDPR principles of purpose limitation, data minimisation and stricter necessity and proportionality tests for use of data.
- It also provides more robust rights to data subjects, including enhanced transparency about data usage, right to rectification, right to erasure (the so-called 'right to be forgotten'), and a more accessible mechanism to lodge complaints.
- No substantial change in US surveillance laws though.

What is the EU-US DPF?

What is the scope?

The EU-US DPF applies solely to data transfers to the US, whereas SCCs can be relied on for data transfers to any third country, including the US.

What does this mean practically for EU companies?

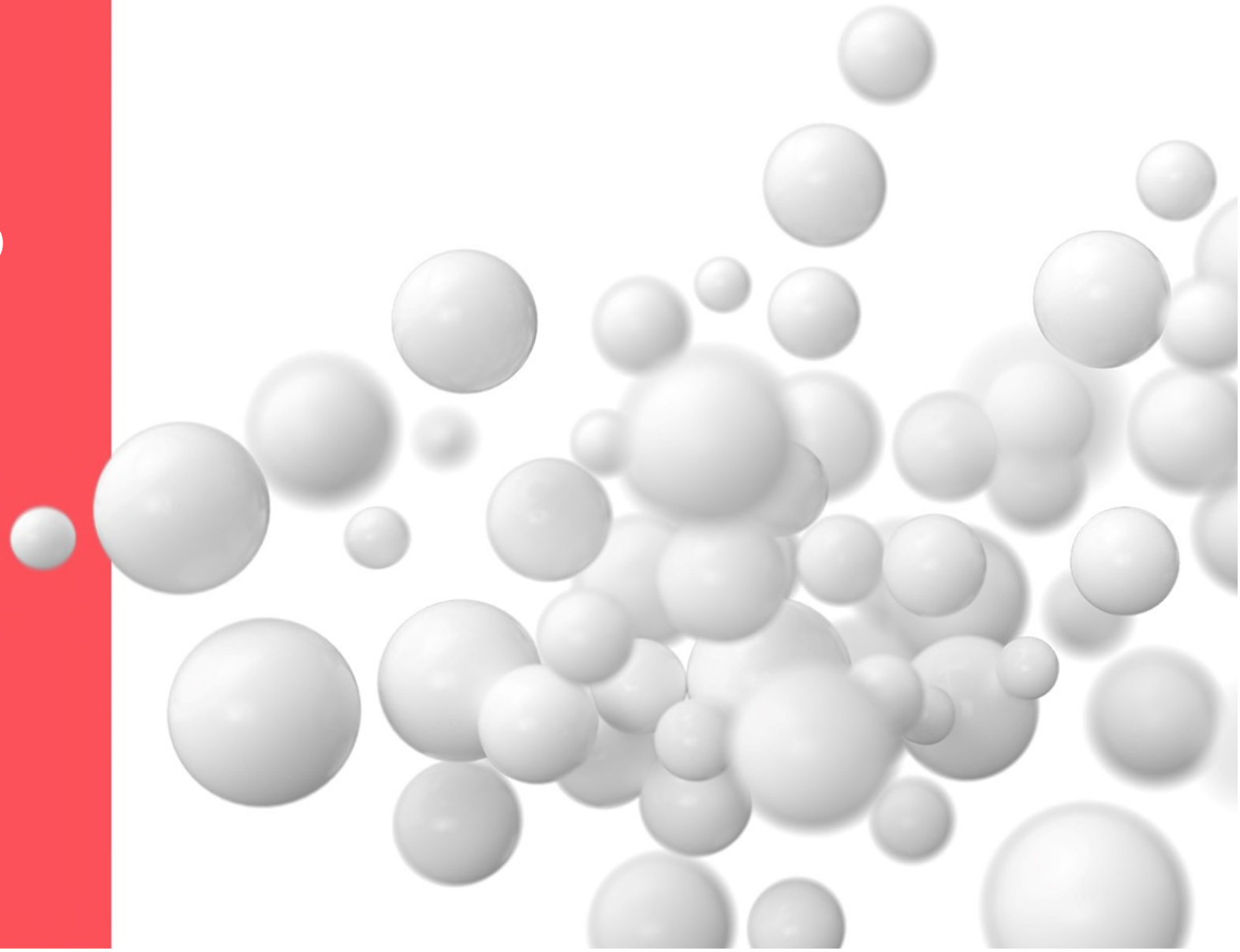
- EU companies do not need to complete a TIA if relying on EU-US DPF, whereas a TIA will be required when relying on the SCCs. However, the Executive Order also applies to transfers based on the SCCs and will thus be helpful for the successful completion of a TIA.
- EU companies can start transferring EU residents' personal data to US entities from the date such entities are self-certified.
- EU-based organisations must adjust their own privacy policies to reflect the EU-US DPF properly as well as the relevant entries in the EU organisation's data processing register.

What is the EU-US DPF?

What does this mean practically for US companies?

- Organisations may begin relying immediately on the EU-US DPF to receive personal data transfers from the EU and European Economic Area
- Companies that remained certified to the Privacy Shield must comply with the new EU-U.S. DPF principles by 17 October 2023. The three-month transitional period is built in for companies previously certified under the Privacy Shield to update privacy policies to reflect the new DPF, and for those looking to self-certify to begin the process.
- Those new to the framework can initiate the self-certification process online. They'll be required to provide details about their privacy policy, reasons for data transfers, reporting mechanisms and more. Once they receive confirmation from the Department of Commerce, companies can proceed with data transfers under the DPF.

Eligibility and sign-up



Eligibility and sign-up

Who is eligible to sign up

- Only US legal entities subject to the jurisdiction of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DOT) are currently eligible to sign up.
- Those companies not subject to the jurisdiction of either the FTC or DOT (for example, banking, insurance, and telecommunications companies) are unable to participate in the EU-US DPF.

New certification

- US companies can certify by committing to comply with a detailed set of privacy obligations and must develop a compliant privacy policy statement.
- Required to submit a number of documents and statements and there is a moderate filing fee.

Re-certifying

- Organisations certified under the Privacy Shield (and wishing to join the EU-US DPF) must comply with the EU-US DPF Principles. Those certified under the Privacy Shield but not wishing to join the EU-US DPF must complete the withdrawal process.
- Organisations are required to annually re-certify
- US Department of Commerce's International Trade Administration (ITA) will remove a company from the list if the company voluntarily withdraws or fails to complete its annual re-certification.

Eligibility and sign-up

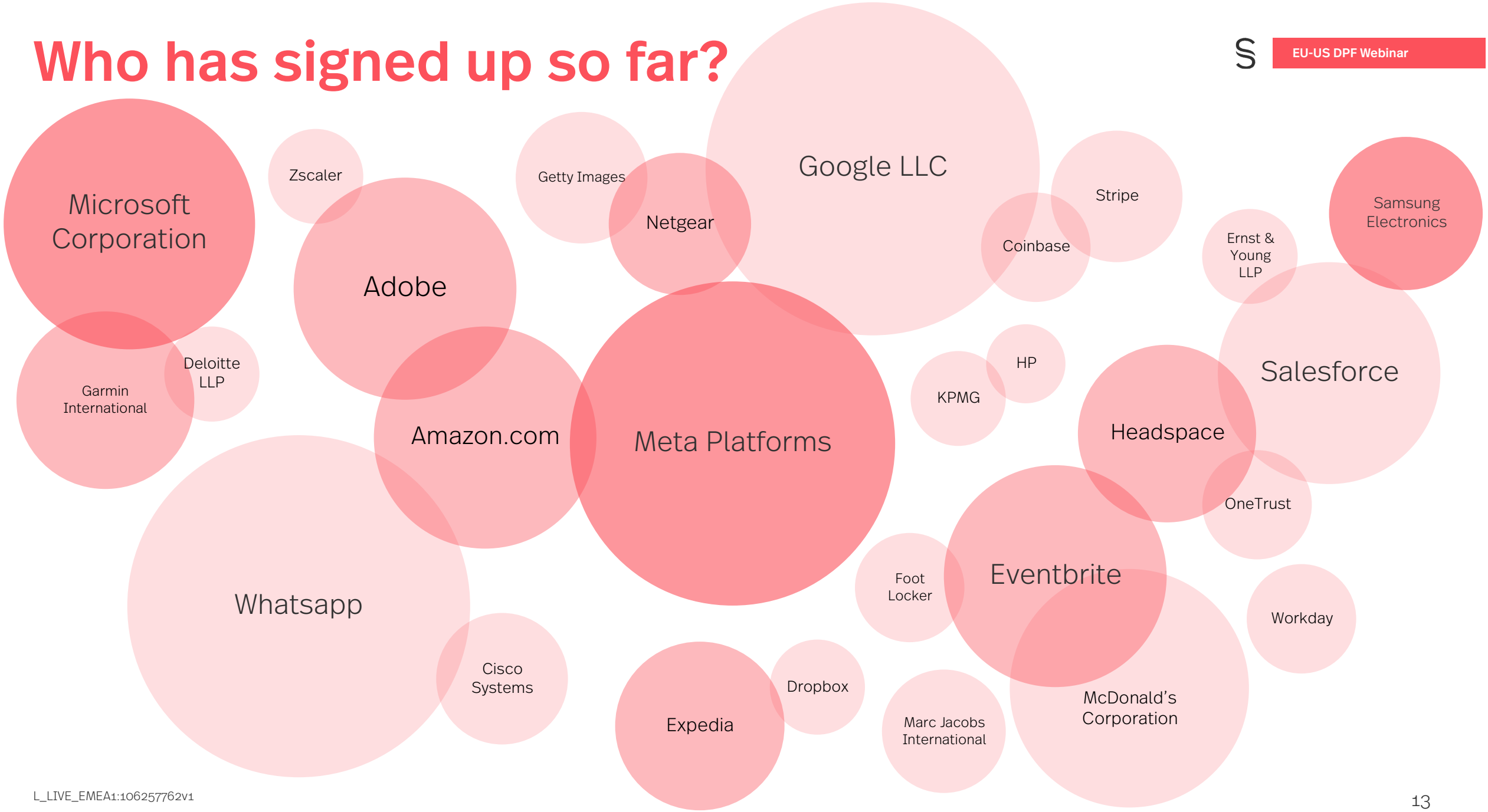
Impact on Google Analytics and suppliers

EU-US DPF makes using software that sends data across the Atlantic, such as Google Analytics and Facebook Ads, legal again, once those vendors are certified.

Who administers the EU-US DPF?

- The US Department of Commerce processes applications for certification and monitors whether participating companies continue to meet the certification requirements.
- Compliance by US companies with their obligations under the EU-US DPF will be enforced by the US Federal Trade Commission.

Who has signed up so far?



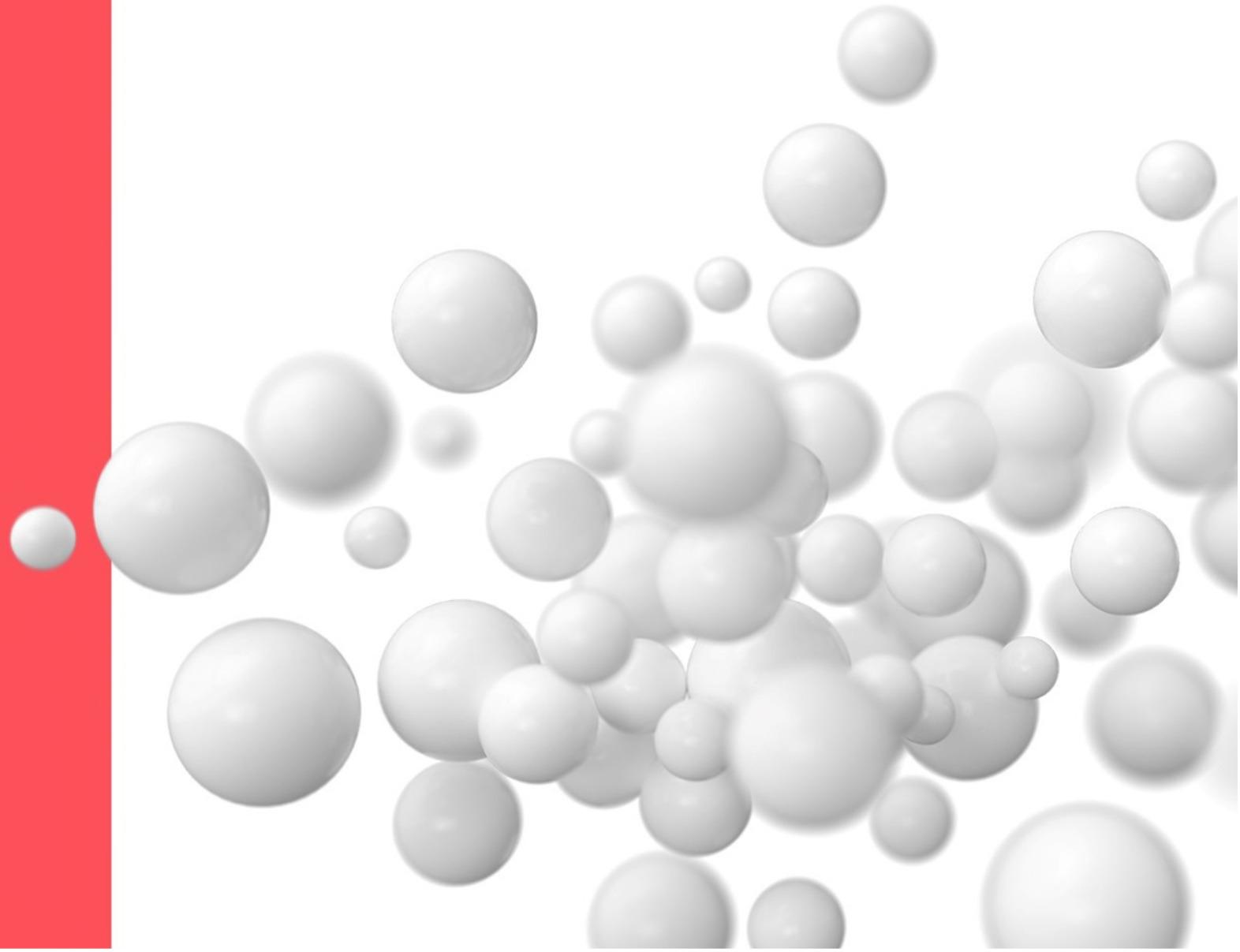
Eligibility and sign-up

Brief guide to self-certification

Steps to providing its initial self-certification submission include:

- confirming the organisation's eligibility to participate;
- developing a DPF-compliant privacy policy statement conforming to the DPF Principles;
- identifying the organisation's independent dispute resolution mechanism for the personal data covered by the self-certification;
- providing accurate information about location of the organisation's applicable privacy policy;
- making the required contribution for the for the Annex I Binding Arbitration Mechanism to cover the arbitral costs, including arbitrator fees;
- ensuring procedures are in place for verifying that the attestations and assertions that it makes about its DPF privacy practices and that those privacy practices have been implemented as represented and in accordance with the DPF Principles; and
- designating a contact for handling DPF complaints, access requests, or any other issues.

Should I self-certify?



Should my business self-certify?

5 key points to consider

§ 5 key points

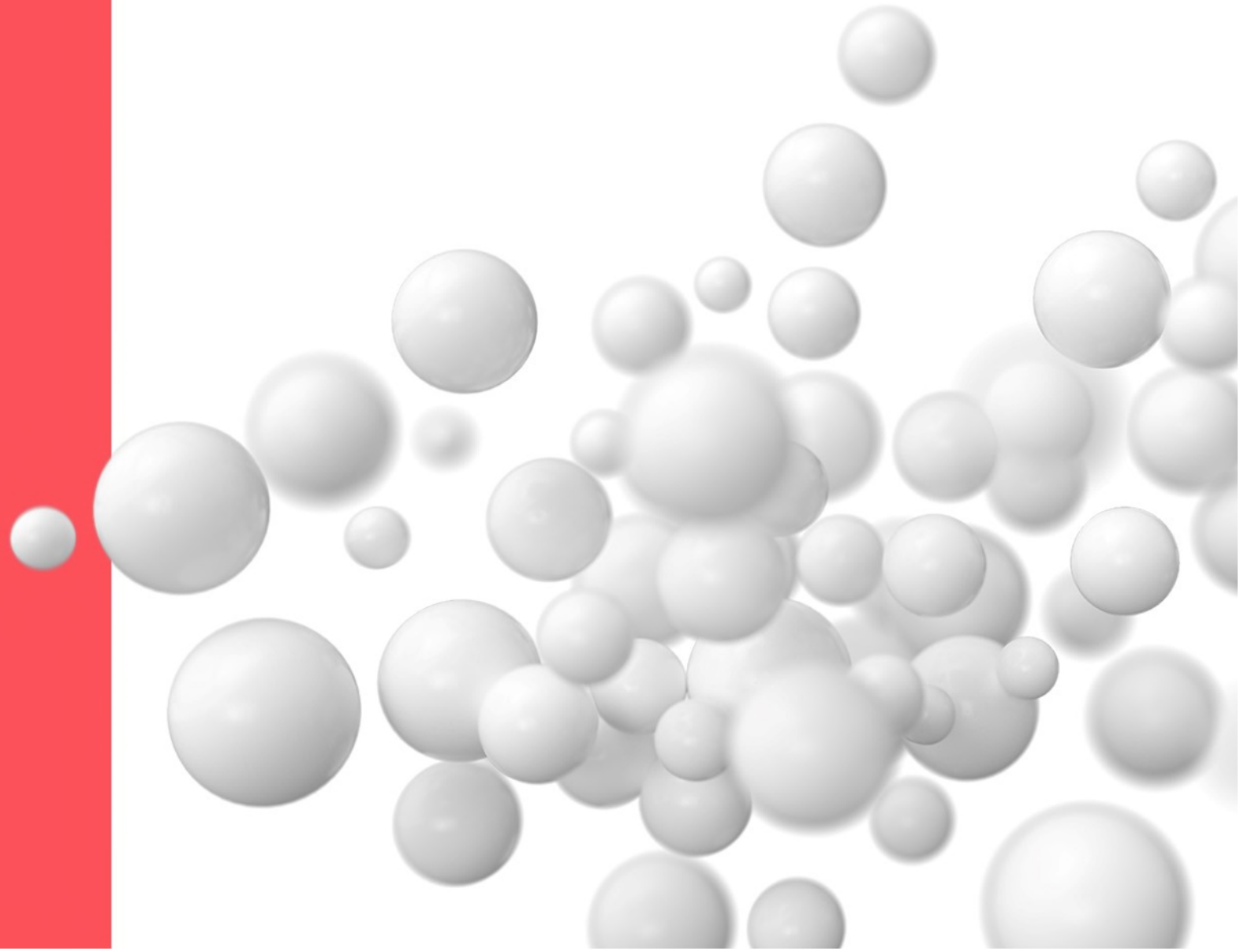
1. Did the business self-certify for the Privacy Shield and therefore would it be easy to transition to the new framework?
2. What are the business benefits in self-certifying compared to the cost and effort involved?
3. If the business hasn't self-certified before, is it eligible?
4. What is the impact on other data transfer mechanisms that the business uses and would it be helpful to add an extra option for transfers?
5. Can the business manage all of the relevant on-going obligations to maintain the self-certification?

Additional points to note

- Certification signals a serious commitment to data privacy which is beneficial from an external perception standpoint.
- The DPF provides certain benefits over the SCCs, particularly for companies in the US that receive personal data from a large volume of clients in the EU and are looking to streamline their contracting process in the short term.
- Privacy advocate Max Schrems has already confirmed his group, NOYB, will be pursuing a legal challenge.
- EU organisations using SCCs and BCRs can now show in transfer impact assessments that requirements relating to national security and government access are fulfilled and compliant under the DPF's enhanced protections
- Any individual transfer must be made under a specific transfer mechanism – either SCCs OR the EU-US DPF – both mechanisms cannot apply at the same time to the same transfer. BUT, vendors can offer both mechanisms to a customer then allow the customer to choose which mechanism they prefer for the transfers made by that customer.

- **10 October 2023:** Company Privacy Policies related to the EU-US DPF must be updated by this date to comply
- **17 October 2023:** Company Privacy Policies related to the Swiss-US DPF must be updated by this date to comply

Perception of EU-US DPF in Europe



Perception in Europe

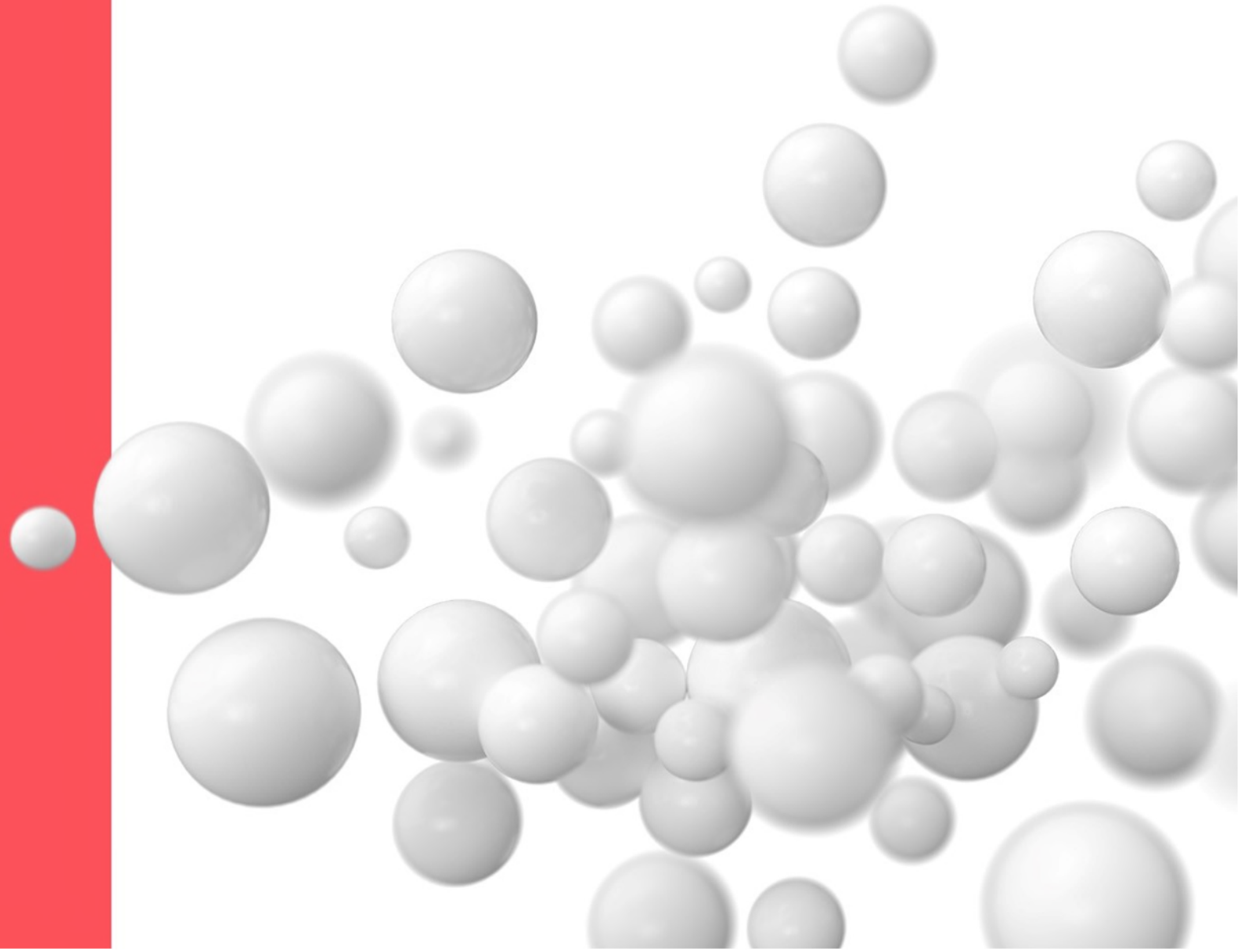
"[The European Parliament] calls on the Commission to act in the interest of EU businesses and citizens by ensuring that the proposed framework provides a solid, sufficient and future-oriented legal basis for EU-US data transfers; expects any adequacy decision, if adopted, to be challenged before the CJEU; highlights the Commission's responsibility for failure to protect EU citizens rights in the scenario where the adequacy decision is again invalidated by the CJEU"

Before the EU-US DPF's implementation, the European Data Protection Board and the European Parliament raised concerns about the privacy safeguards afforded by the agreement. The EP called on the European Commission to renegotiate or challenge the EU-US DPF before the CJEU.

"The European Commission will now have to decide whether there is equivalent protection for personal data in the USA. It is already questionable whether the Commission is even able to reassess the level of data protection in the US and issue an adequacy decision based solely on the Executive Order. The large number of open questions still to be clarified raises doubts. In this elementary data protection issue, however, the citizens of the EU need legal certainty just as much as the European and foreign companies affected by it. Should the European Commission allow the fundamental rights of EU citizens to take a back seat to economic interests for the third time in a row?"

Stefan Brink, the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg

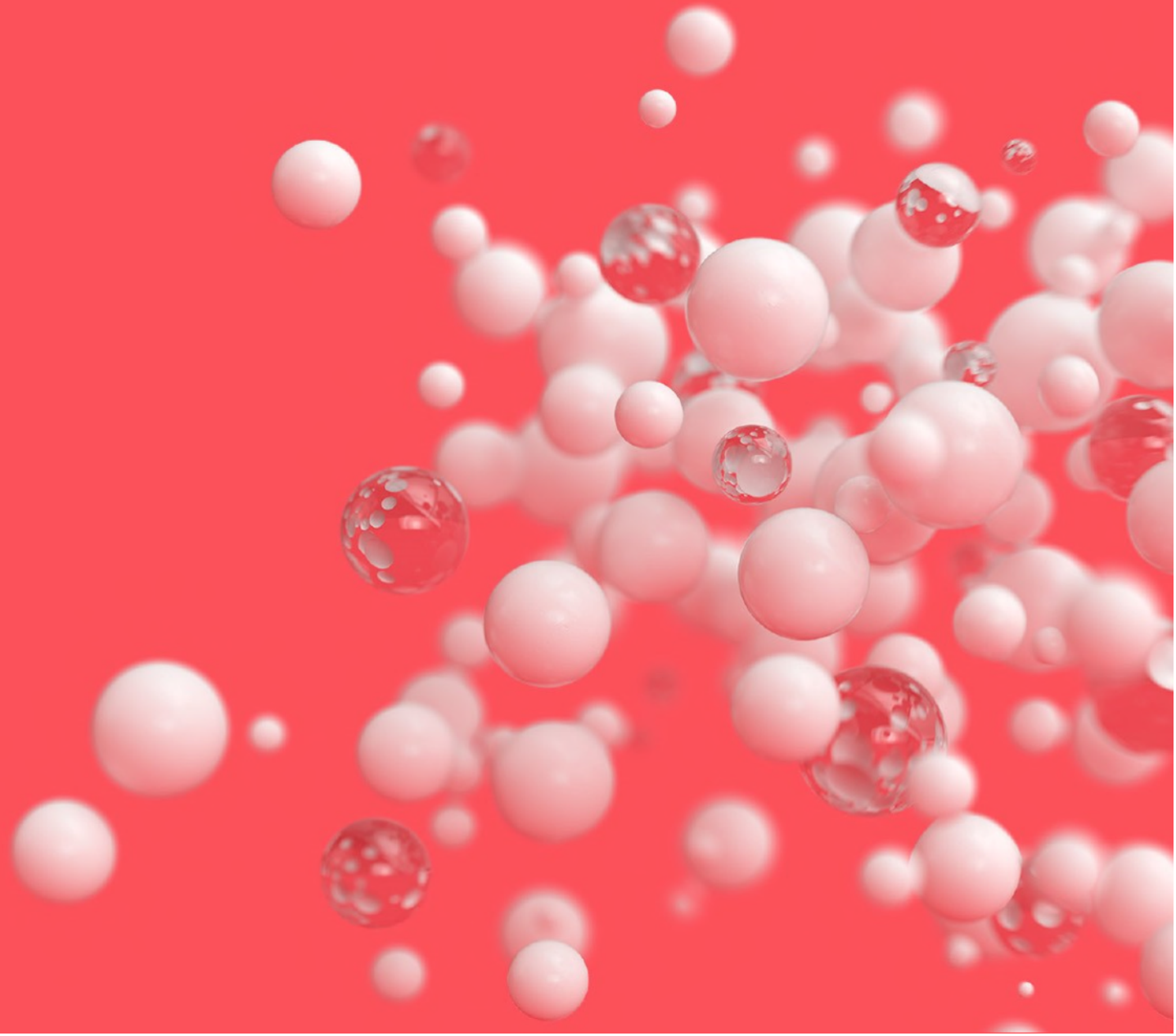
Impact on transfers from the UK and Switzerland



Impact on transfers from UK and Switzerland

	The UK	Switzerland
US company currently signed up to Privacy Shield that will convert to the new DPF	• Eligible US organisations receiving data must supplement their converted EU-US Privacy Shield self-certification by applying for self-certification under the UK Extension to the EU-US DPF. • However, they may not begin relying on the UK Extension for transfers until after approval of the UK-US Data Bridge, and will also need to submit an application to convert EU-U.S. Privacy Shield participation for UK-US transfers. • In the meantime, transfers must be made via alternative UK transfer mechanisms (e.g. IDTA)	• The US organisation receiving data must update its privacy policy no later than 17 October 2023 to reflect compliance with the Swiss-US DPF. However, it may not begin relying on the Swiss-US DPF for transfers until after the pending Swiss adequacy decision. • In the meantime, transfers should be made using alternative Swiss transfer mechanisms.
An entirely new participant of the DPF	• Eligible US companies receiving data may begin applying to self-certify under the UK Extension to the EU-US DPF. Participants must also self-certify under the EU-US DPF. • However, they may not begin relying on the UK Extension for transfers until after approval of the UK-US Data Bridge. • In the meantime, transfers must be made via alternative UK transfer mechanisms (e.g. IDTA)	• Eligible US companies receiving data may submit applications to self-certify on the new DPF website. They may rely on the framework for transfers only after approval – and after the pending Swiss adequacy decision is finalised. • In the meantime, transfers should be made using alternative Swiss transfer mechanisms.
A US entity not planning on self-certifying to the DPF	Transfers must be made using alternative transfer mechanisms (e.g. SCCs or BCRs)	Transfers must be made using alternative transfer mechanisms (e.g. SCCs or BCRs)

Q&A



simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL