FROM GDPR TO PIPL: UNLOCKING CROSS-BORDER DATA TRANSFER STRATEGIES

OUR TEAM

PARTNER
CYBERSECURITY & DATA PRIVACY

ANA BRUDER

FRANKFURT +49 69 7941 1778
ABRUDER@MAYERBROWN.COM

PARTNER
CO-LEADER OF INTELLECTUAL PROPERTY

GABRIELA KENNEDY

HONG KONG +852 2977 1790
GABRIELA.KENNEDY@MAYERBROWN.COM

PARTNER
CYBERSECURITY & DATA PRIVACY

ARSEN KOURINIAN

LOS ANGELES +1 213 229 5141
AKOURINIAN@MAYERBROWN.COM

PARTNER
LEADER OF LONDON OFFICE
INTELLECTUAL PROPERTY

OLIVER YAROS

LONDON +44 20 3130 3698
OYAROS@MAYERBROWN.COM

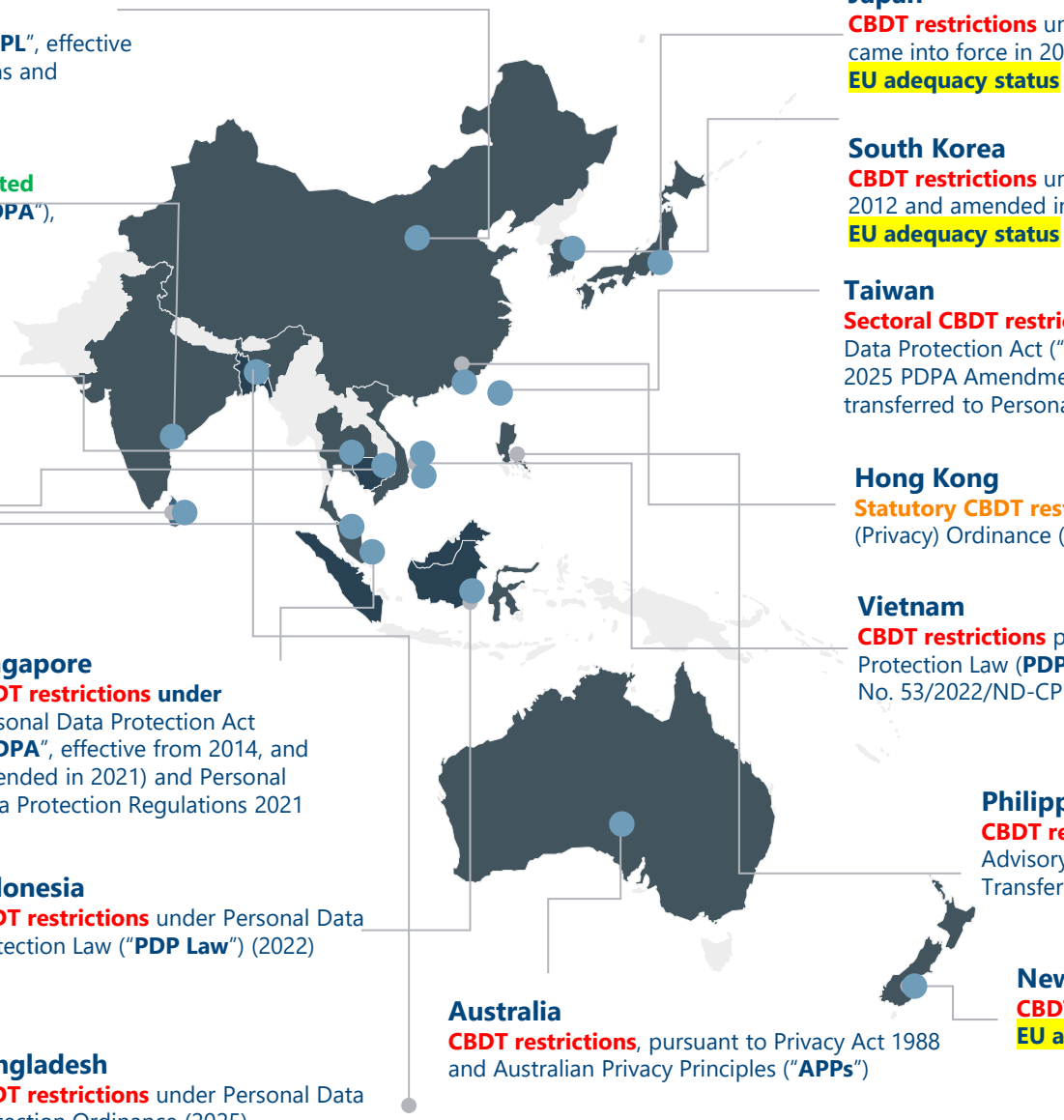
AGENDA

1. Asia Cross-Border Data Transfer Considerations
2. EU and UK Cross-Border Data Transfer Considerations
3. US Cross-Border Data Transfer Considerations
4. Bringing it All Together: Unlocking Your Strategy for Addressing Cross-Border Transfers

01

APAC CROSS-BORDER DATA TRANSFER

APAC REGULATORY LANDSCAPE : CROSS BORDER DATA TRANSFER (CBDT)



China
CBDT restrictions under Personal Information Protection Law ("**PIPL**", effective 2021), other data laws (DSL and CSL) and other relevant regulations and implementing measures

India
No CBDT restrictions except for sectoral restrictions or restricted countries, under Digital Personal Data Protection Act, 2023 ("**DPDPA**"), IT Act and SPDI Rules, and sectoral regulations

Thailand
CBDT restrictions under Personal Data Protection Act ("**PDPA**", effective 2022) **Whitelist approach (jurisdictions with adequate protection)**

Cambodia
Currently no statutory restrictions except for sectoral/industry-specific rules. Draft law on personal data protection (2025)

Sri Lanka
CBDT restrictions under Personal Data Protection Act ("**PDPA**") (effective 2023 with amendments in 2025)

Malaysia
CBDT restrictions under Personal Data Protection Act 2010 ("**PDPA**", came into force in 2013 and amended in 2025), Data Sharing Act (2025) and Guidelines for Cross Border Personal Data Transfer (2025). **2025 PDPA amendments removed previous whitelist approach.**

Singapore
CBDT restrictions under Personal Data Protection Act ("**PDPA**", effective from 2014, and amended in 2021) and Personal Data Protection Regulations 2021

Indonesia
CBDT restrictions under Personal Data Protection Law ("**PDP Law**") (2022)

Bangladesh
CBDT restrictions under Personal Data Protection Ordinance (2025)

Australia
CBDT restrictions, pursuant to Privacy Act 1988 and Australian Privacy Principles ("**APPs**")

Japan
CBDT restrictions under Act on the Protection of Personal Information ("**APPI**", came into force in 2005 and amended in 2016-2017)
EU adequacy status

South Korea
CBDT restrictions under Personal Information Protection Act ("**PIPA**", came into force in 2012 and amended in 2023 and 2025)
EU adequacy status

Taiwan
Sectoral CBDT restrictions issued by industry regulators pursuant to Personal Data Protection Act ("**PDPA**", came into force in 2012 and amended in 2023). New 2025 PDPA Amendments (may take effect in 2026): power to restrict CBDT will be transferred to Personal Data Protection Commission (PDPC)

Hong Kong
Statutory CBDT restrictions not yet in force: Section 33 under Personal Data (Privacy) Ordinance ("**PDPO**", effective from 1996, amended in 2012 and 2021)

Vietnam
CBDT restrictions pursuant to of Decree No. 356/2025/ND-CP (2026), Personal Data Protection Law (**PDPL**) (2026), Data Law (**2025**), Cybersecurity Law (2018) and Decree No. 53/2022/ND-CP

Philippines
CBDT restrictions under Data Privacy Act 2012 ("**DPA**"). See also NPC Advisory No. 2024-01 on Model Contractual Clauses For Cross-border Transfers of Personal Data

New Zealand
CBDT restrictions under Privacy Act 2020, amended in 2025
EU adequacy status

APAC REGULATORY LANDSCAPE: CROSS-BORDER DATA TRANSFER

	Governing Law	Transfer Mechanisms
China	Cybersecurity Law (**CSL**) Data Security Law (**DSL**) Personal Information Protection Law (**PIPL**)	Three CBDT mechanisms: • Security assessment (mandatory in certain circumstances) • Personal information protection certification • Standard contract + Separate consent and Personal Information Protection Impact Assessment (PIPIA)
Hong Kong	Personal Data (Privacy) Ordinance (**PDPO**)	Currently no statutory restrictions on cross-border transfers (Section 33 not yet in force). PCPD guidance : • Separate, voluntary written consent • Recommended Model Contractual Clauses
Singapore	Personal Data Protection Act 2012 (**PDPA**)	CBDT mechanisms include: • Obtaining data subject's express or deemed consent to CBDT (subject to prescribed requirements/restrictions) • Ensuring that the recipient of CBDT is subject to legally obligations to protect data comparable to the PDPA standards via: (a) any law; (b) any contract (subject to prescribed requirements); (c) any binding corporate rules (subject to prescribed requirements); or (d) any other legally binding instrument. • Transfers in the vital interests of data subjects or in the national interest • Transfers to certain certified recipients (APEC CBPR/PRP)
Japan	Act on the Protection of Personal Information (**APPI**)	CBDT mechanisms include: • Data subject consent with prescribed information • PPC-approved certification (e.g. APEC CBPR) • Recipient country has APPI-equivalent standards • EU adequacy status
South Korea	Personal Information Protection Act (**PIPA**)	CBDT mechanisms include: • Separate consent • Necessary for contract performance (with disclosure in privacy policy) • Recipient holds PIPC-recognised certification and implements measures required by PIPC • PIPC recognises equivalent protection in recipient country • EU adequacy status
India	Digital Personal Data Protection Act, 2023 (**DPDPA**); IT Act and SPDI Rules	Under the DPDPA: transfers permitted to all countries except those notified (restricted) by the Government. Under IT Act/SPDI Rules: transfer permitted if transferee ensures equivalent protection and transfer is necessary for lawful contract or consented to. Sectoral regulations contain restrictions on transfer of personal information outside India e.g. regulated entities (banks, financial institutions, telecom providers).

OVERVIEW OF CHINA DATA LAWS

	Cybersecurity Law ("CSL") **(effective since 1 June 2017)** CSL Amendments effective from 1 January 2026	**Data Security Law** **("DSL")** **(effective since 1 September 2021)**	**Personal Information Protection Law** **("PIPL")** **(effective since 1 November 2021)**
Purpose of regulation	High level framework for cybersecurity regulation and some general data protection obligations	Contains detailed data security-specific obligations	Detailed data privacy-specific obligations
Type of entities covered	Network Operators and Critical Information Infrastructure Operators ("**CIIOs**")	Covers all entities carrying out data processing activities within the PRC	Covers all entities handling personal information of individuals who are within the PRC
Type of data covered	All data in electronic form	All types of data (electronic and non-electronic), with additional focus on "Important Data" and "Core National Data"	Personal information only

General Guidelines, Implementing Measures and Provisions issued on the basis of one or all of the China Data Laws
e.g. Provisions on Promoting and Regulating Cross-Border Data Transfers (effective since 22 March 2024);
Network Data Security Management Regulations (effective since 1 January 2025)

Sector-specific provisions issued pursuant to one or all of the China Data Laws, but applying to specific industries

CHINA CROSS-BORDER DATA TRANSFER MECHANISMS

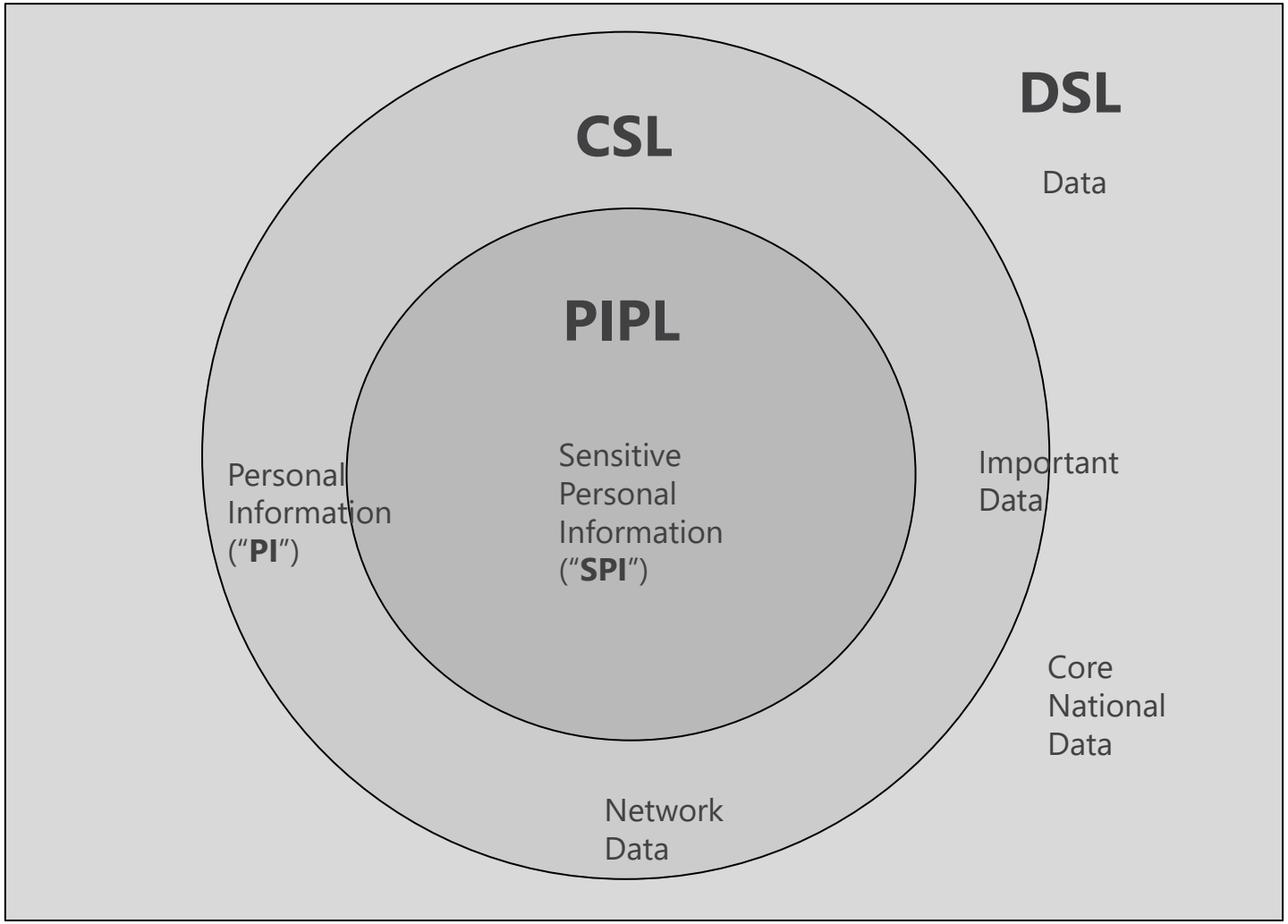
SECURITY ASSESSMENT

CERTIFICATION

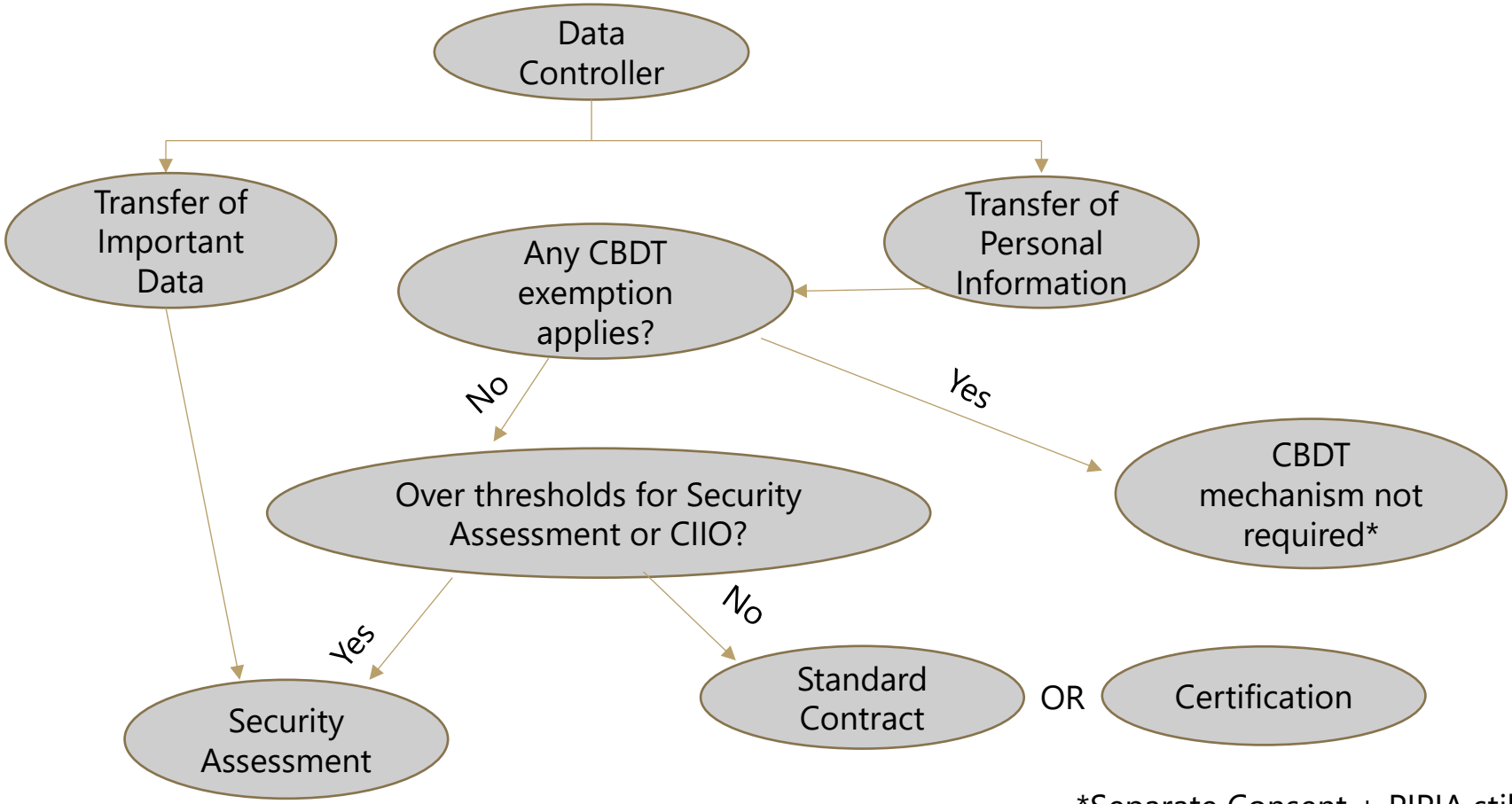
STANDARD CONTRACT

+ Separate Consent + Personal Information Protection Impact Assessment (PIPIA)

CHINA - TYPES OF DATA



CHINA CROSS-BORDER DATA TRANSFER MECHANISMS



*Separate Consent + PIPIA still required

CHINA: TRANSFER MECHANISM – EXEMPTIONS

- Data from international trade, cross border transport, academic cooperation, cross border manufacturing, or cross border marketing **not containing personal information or important data**
- **Personal information generated and collected abroad** and processed in China, without adding local personal information or important data
- Transfer of personal information for **performance of contract** to which the data subject is a party (e.g., cross border e-commerce, shipping, payments)
- Transfer of employee data necessary for **cross border HR management** under lawful labour policies and collective employment contracts
- Transfers necessary in an **emergency**, to protect an individual's health and safety, or safety of property
- Non-CIIO data controller transfers data fewer than **100,000** individuals (excluding sensitive personal information) since 1 January of the current year
- Cross-border data transfers by data controllers within **Free Trade Zones** involving data falling outside the negative list

CHINA: TRANSFER MECHANISM – NEW THRESHOLDS

- Data controllers or Critical Information Infrastructure Operators (**CIIOs**) are subject to **Security Assessment** in these scenarios:
  - Cross-border data transfer of Important Data
  - CIIO exports personal information
  - Non-CIIOs data controllers who have cumulatively exported:
    - personal information (excluding sensitive personal information) of more than **1 million** people; or
    - sensitive personal information of more than **10,000** people

    since 1 January of the current year

CHINA: TRANSFER MECHANISM – NEW THRESHOLDS

- Non-CIIO data controllers are subject to **Certification** or shall enter into a **Standard Contract** if they have cumulatively exported:
  - the personal information (excluding sensitive personal information) of more than **100,000** people but fewer than **1 million** people; or
  - the sensitive personal information of fewer than **10,000** people since 1 January of the current year

CHINA: ACCESS TO DATA UNDER FOREIGN COMPULSION

CSL	DSL	PIPL
N/A	Providing ***data*** stored in the PRC to foreign judicial or law enforcement agencies without the approval of the PRC "*competent authorities*" is prohibited	Providing ***PI*** stored in the PRC to foreign judicial or law enforcement agencies without the approval of the PRC "*competent authorities*" is prohibited

APEC CROSS-BORDER DATA TRANSFER FRAMEWORK

APEC Cross-Border Privacy Rules ("CBPR")

- Government-backed data privacy certification that ensures certified organisations have in place data protection policies consistent with the APEC Privacy Framework
- Voluntary, accountability-based system serves to facilitate data flows across the APEC region

9 participating jurisdictions

- United States, Canada, Mexico, Japan, Singapore, Chinese Taipei, Australia, South Korea and the Philippines

Requirements for joining APEC CBPR

- Submit a formal notice to participate
- Designate a local Privacy Enforcement Authority
- Identify at least one Accountability Agent (approved by APEC)
- Submit an APEC CBPR system programme requirements enforcement map

Accountability Agents

- Accountability Agents work with stakeholders to ensure that cross-border data transfers meet the standards required by the APEC Privacy Framework and resolve any disputes if possible.

APEC

Asia-Pacific Economic Cooperation

APEC CROSS-BORDER DATA TRANSFER FRAMEWORK

Global CBPR and Privacy Rules for Processors (PRP) Program

- Officially launched on 2 June 2025
- Built on the existing APEC CBPR framework
- Apart from the 9 APEC members, a number of other jurisdictions (e.g. UK, Dubai International Financial Centre) joined as Associate members.

118 Certified Organizations

- including **Apple Inc., Cisco Systems, Inc., Cloudflare, Inc., International Business Machines Corporation (IBM), Salesforce, Inc., The Coca-Cola Company**
- Businesses must be re-certified annually.

Accountability Agents

- Accountability Agents certify that the privacy policies and practices of participating companies comply with the Global CBPR and Global PRP Systems Program requirements.
- 5 in the United States, 1 in South Korea, 1 in Singapore, 1 in Japan, 1 in Chinese Taipei (9 in total)

Global CBPR Forum

02

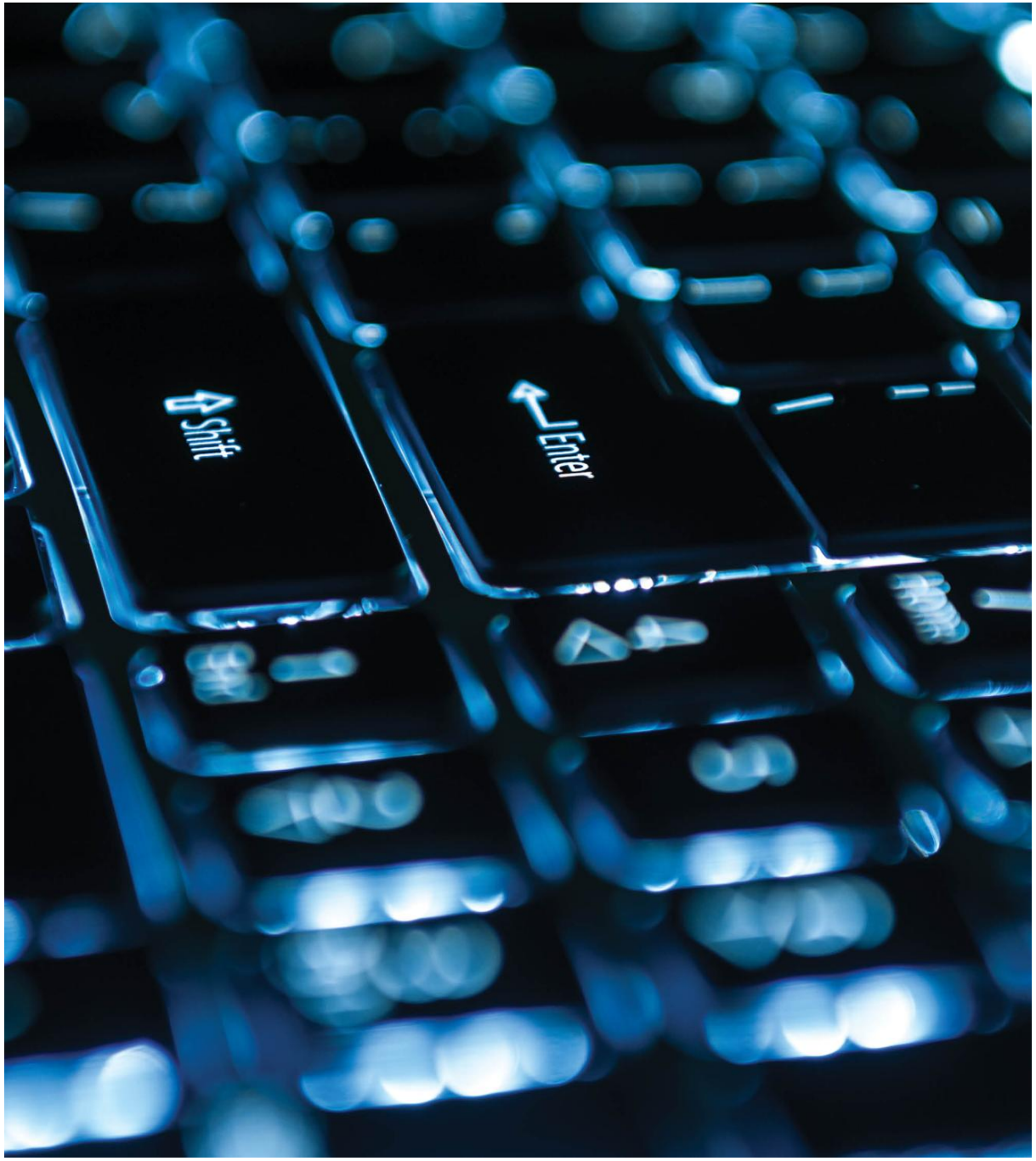
EU AND UK CROSS-BORDER DATA TRANSFER CONSIDERATIONS

GDPR TODAY: INCREASING SCRUTINY OVER INTERNATIONAL DATA TRANSFERS

- **Schrems II decision of the Court of justice of the European Union (July 2020):**
  Invalidated EU-US Privacy Shield. Upheld Standard Contractual Clauses (SCCs) but made data transfers significantly harder.
- **New EU SCCs for data transfers (June 2021):**
  Required pre-existing arrangements to be repapered.
- **EDPB recommendations** issued (June 2021):
  Requires **transfer impact assessments** and **supplementary measures** to be adopted:
  - **Pseudonymization or encryption**, with the **key** held in Europe under control of the data exporter → Can be difficult to implement in practice.
- **Enforcement:**
  - At first, isolated cases of enforcement ordering the transfer of data to the US to stop, but no fines.
  - 12 May 2023: US social media company fined by DPC USD 1.3 billion for failing to implement supplementary measures.
  - 2 May 2025: China social media company fined by DPC €530 million for failing to verify, guarantee and demonstrate supplementary measures.

GDPR - DATA TRANSFER MECHANISMS

- **Adequacy decisions** (Art. 45 GDPR): transfers to countries that have been recognized as providing an adequate level of protection do not need specific authorization.
  - European Commission and the UK Government have each given an adequacy decision to one another (valid until December 2031).
  - 15 countries have been granted adequacy under the EU GDPR.
  - 11 countries have been granted adequacy under UK GDPR.
- In the absence of an adequacy decision, **safeguards** (Art. 46 GDPR) are needed, such as:
  - **Standard Contractual Clauses** + Transfer impact assessment (post-Schrems II); or
  - Binding Corporate Rules.
    - Supplementary measures required post-Schrems II (Pseudonymization or encryption, with the key held in Europe under control of the data exporter).
- The UK DUAA enables a more **proportionate, outcomes-focused assessment** allowing adequacy to be inferred based on the specific transfer context, enforceability of safeguards, and practical risk to individuals' rights.
- If additional safeguards cannot be implemented in a specific case, **derogations** (Art. 49 GDPR) may apply (e.g., consent).



DATA PRIVACY FRAMEWORK CERTIFICATION

- Developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration.
- Provides a mechanism for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland.
- Through DPF, organizations can receive personal data from these regions without relying on an alternative basis, such as EU/UK Standard Contractual Clauses or Binding Corporate Rules.

DATA PRIVACY FRAMEWORK CERTIFICATION

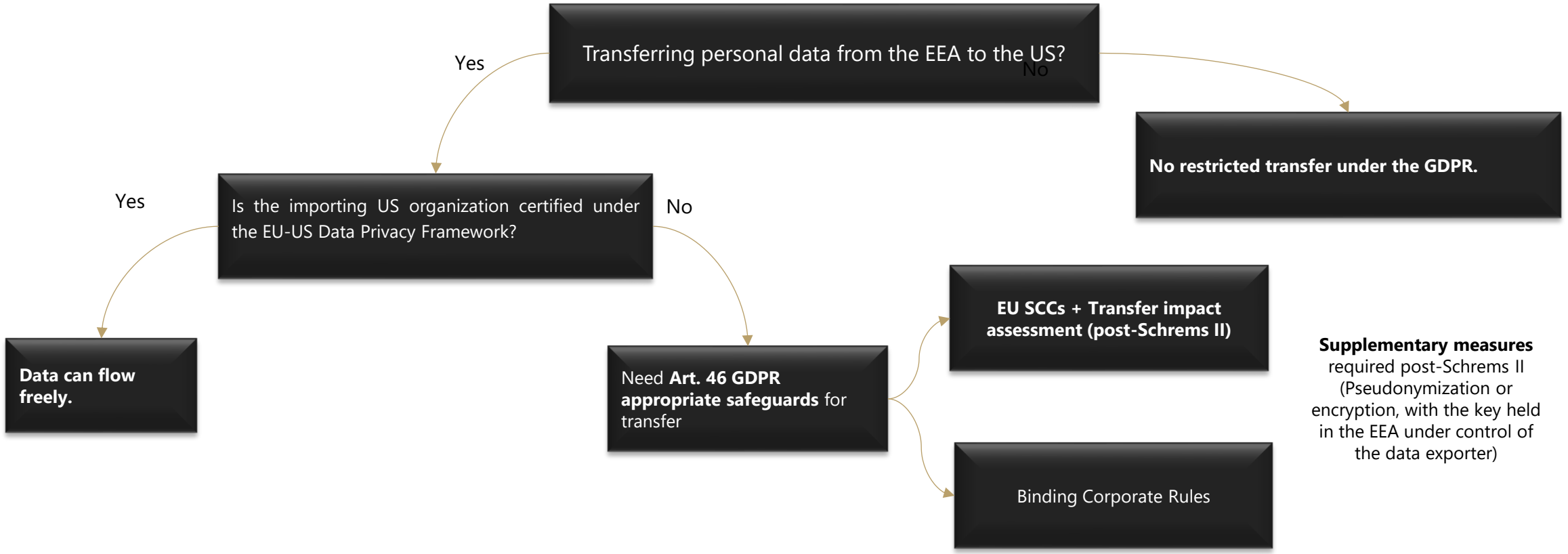
- DPF is administered by the International Trade Administration (ITA) within the U.S. Department of Commerce.
- Organizations must self-certify to the ITA via the DPF program website, https://www.dataprivacyframework.gov/.
- While it is voluntary to certify, once you do, you must comply with the DPF Principles.
- Organizations may withdraw certification, but if they do, they must: (a) cease making claims that they participate or certify under DPF; and (b) continue to comply with the DPF Principles for personal information received while participating in the program.

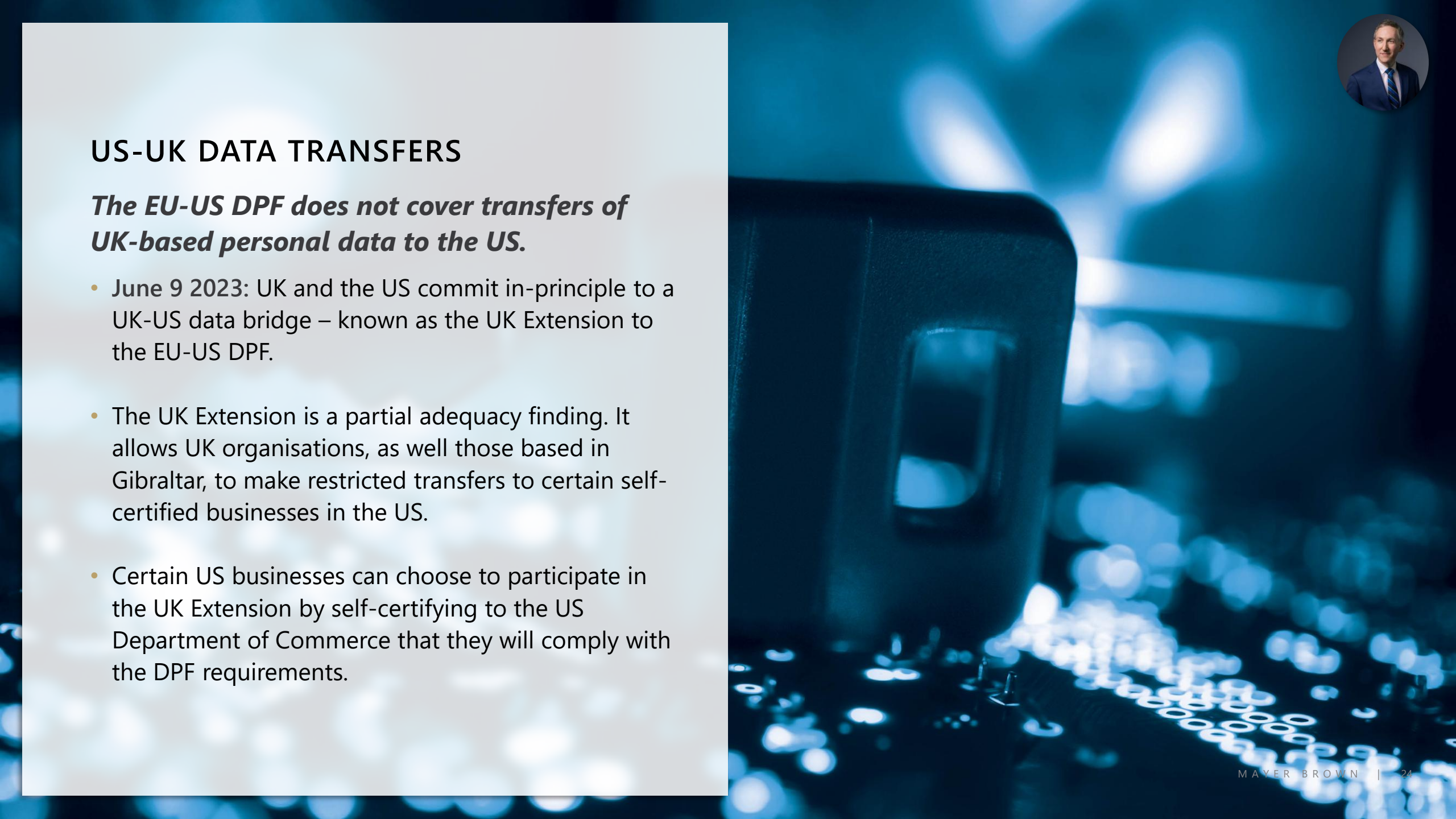
DATA PRIVACY FRAMEWORK CERTIFICATION

Step-by-Step Process

- Review the DPF Principles and confirm that your organization can comply with them.
- Prepare a DPF-compliant privacy policy statement.
- Walk through the online registration process and wait for approval.
- After submitting the certification request, organizations may get feedback for additional privacy policy statement and other updates that are necessary.

EU-US DATA TRANSFERS FLOWCHART





US-UK DATA TRANSFERS

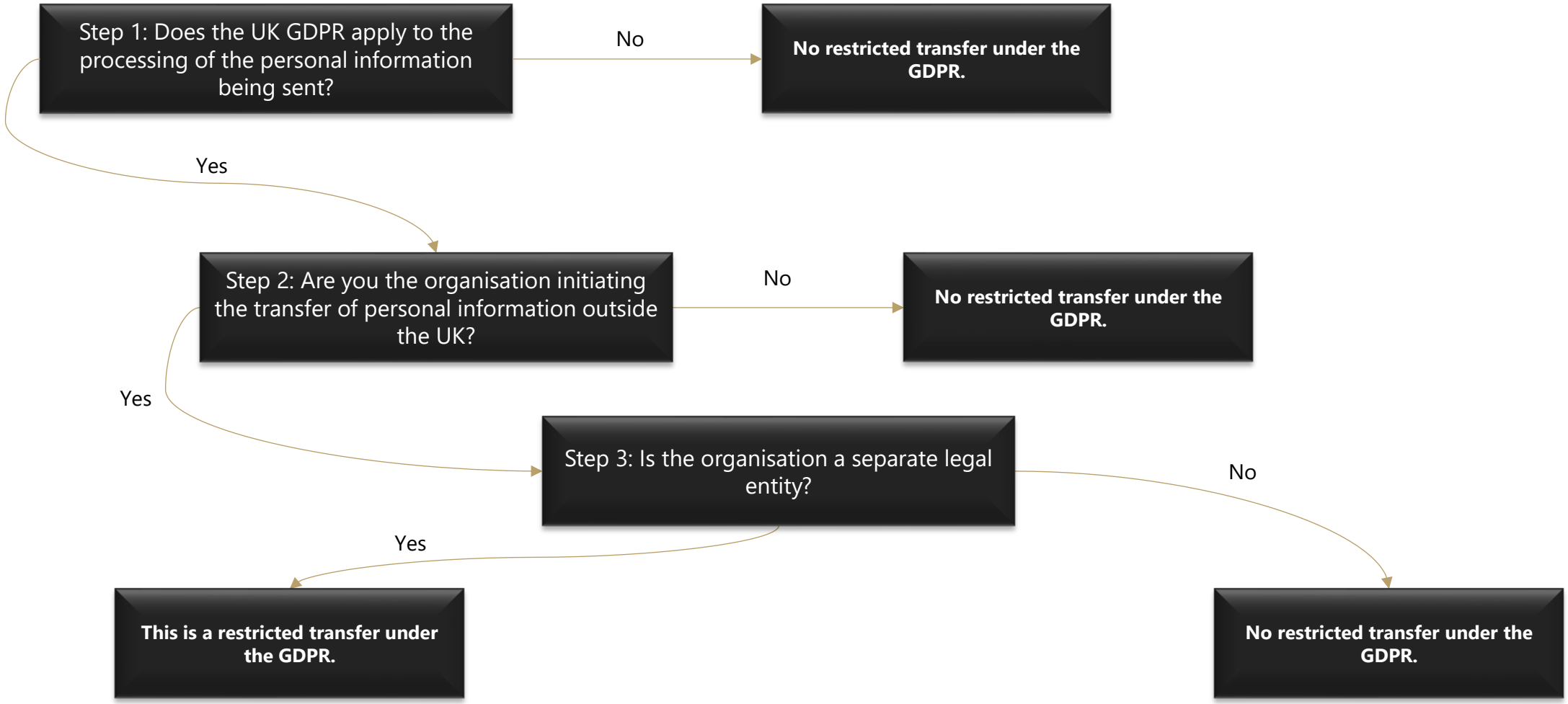
The EU-US DPF does not cover transfers of UK-based personal data to the US.

- **June 9 2023:** UK and the US commit in-principle to a UK-US data bridge – known as the UK Extension to the EU-US DPF.

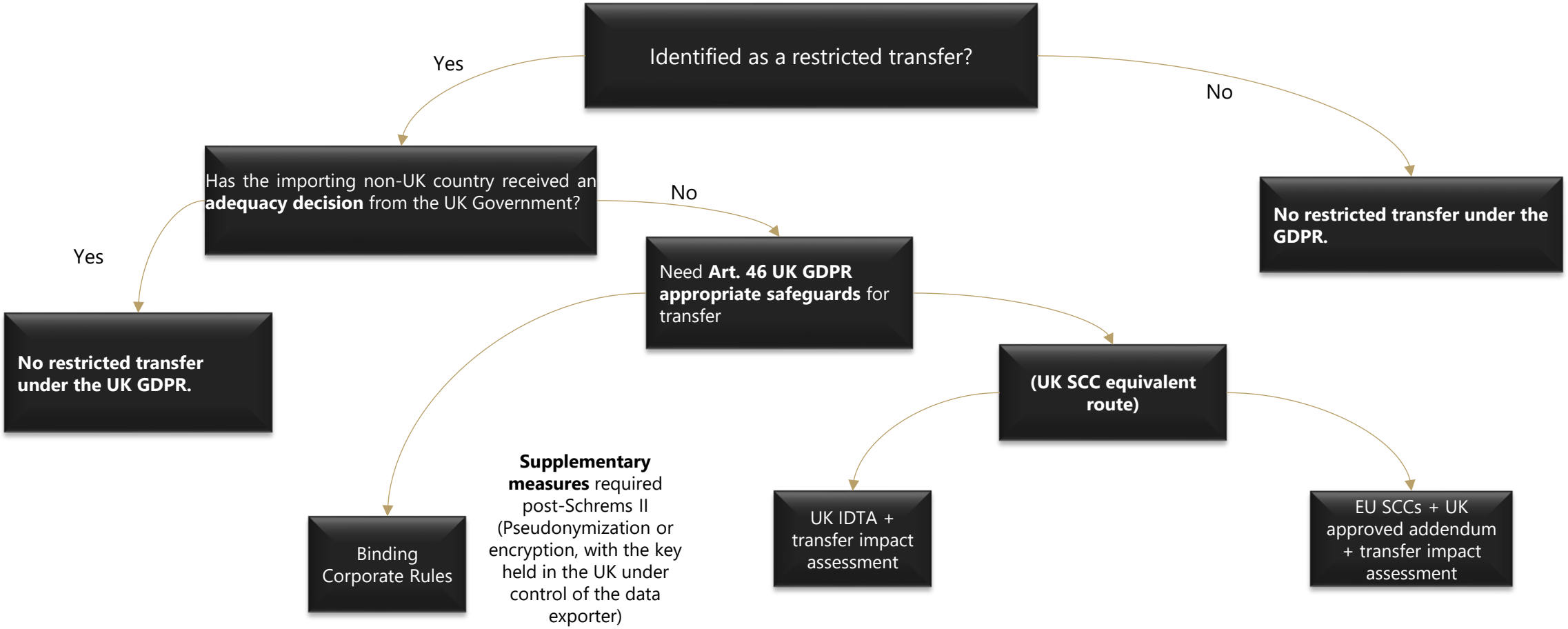
- The UK Extension is a partial adequacy finding. It allows UK organisations, as well those based in Gibraltar, to make restricted transfers to certain self-certified businesses in the US.

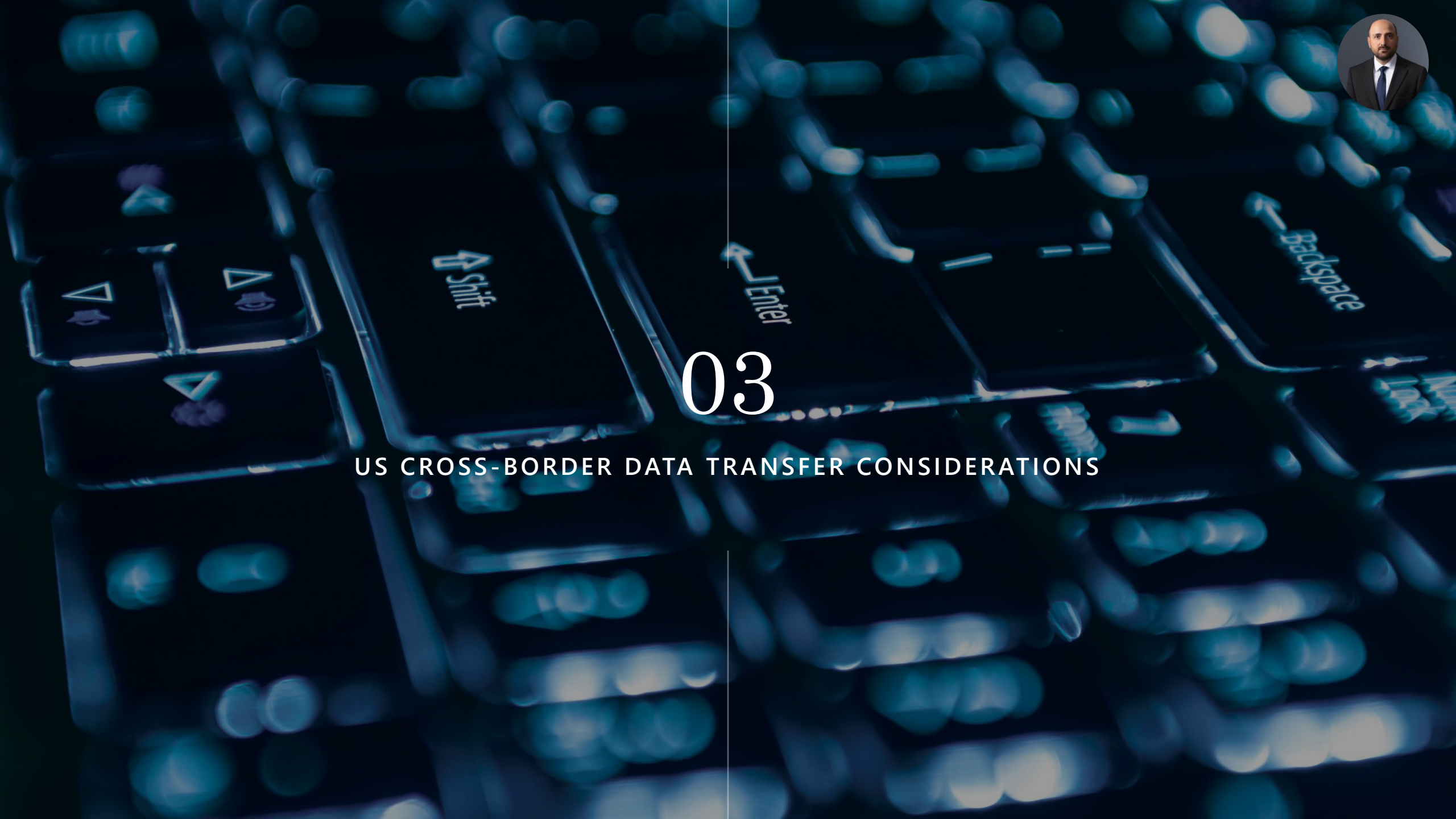
- Certain US businesses can choose to participate in the UK Extension by self-certifying to the US Department of Commerce that they will comply with the DPF requirements.

UK INTERNATIONAL DATA TRANSFERS – DETERMINING A RESTRICTED TRANSFER (ICO'S NEW THREE STEP TEST)



UK INTERNATIONAL RESTRICTED DATA TRANSFERS FLOWCHART





03

US CROSS-BORDER DATA TRANSFER CONSIDERATIONS

U.S. Department of Justice provisions pertaining to preventing access to U.S. Sensitive personal data and government-related data by countries of concern or covered persons ("DOJ rules")

Effective April 8, 2025

Government-related data or Bulk U.S. Sensitive personal data

VENDOR AGREEMENTS
(e.g., SaaS, cloud-service agreements)

EMPLOYMENT AGREEMENTS
(e.g., with a U.S. company's foreign staff located in a country of concern or with a CEO who otherwise qualifies as a covered person)

INVESTMENT AGREEMENTS
(e.g., covered person gaining majority interest in real estate or U.S. Legal entity with access to data)

DATA BROKERAGE (SALE/LICENSE) — ✕

RESTRICTED TRANSACTIONS — △

DATA BROKERAGE (SALE/LICENSE) — △

COUNTRIES OF CONCERN/ COVERED PERSONS

- Comply with CISA security requirements
- Implement data compliance program
- Audit U.S. person's compliance
- Recordkeeping

OTHER FOREIGN COUNTRIES

- Contract prohibiting onward transfer to countries of concern or covered persons
- Report known/suspect violations of contract

U.S. DEPARTMENT OF JUSTICE CROSS-BORDER RULES

Category	Type	Bulk Threshold
Bulk U.S. sensitive personal data: A collection or set of bulk* data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted. ***Bulk**: Any amount of sensitive personal data that meets or exceeds the following thresholds at any point in the preceding 12 months, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person.	**Covered personal identifiers** (e.g., SSN, DLN, account numbers, device IDs, advertising IDs, contact information)	Collected about or maintained on more than 100,000 U.S. Persons
	Precise geolocation data	Collected about or maintained on more than 1,000 U.S. devices
	Biometric identifiers	Collected about or maintained on more than 1,000 U.S. Persons
	Human 'omic data	Collected about or maintained on more than 100 U.S. Persons
	Personal health data	Collected about or maintained on more than 10,000 U.S. Persons
	Personal financial data	Collected about or maintained on more than 10,000 U.S. Persons
	Any combination thereof	If a collection of data contains more than one category of data, then the lower threshold applies
Government-related data	**Any precise geolocation data** for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government…	No volume thresholds apply to government-related data
	Any sensitive personal data that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.	

United States Person

The terms United States person and U.S. person mean any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.

Unless designated as such by the Attorney General, a U.S. person is not a covered person.

COUNTRIES OF CONCERN & COVERED PERSONS

Countries of Concern

PRC **Cuba** **DPRK** **Iran** **Russia** **Venezuela**

Covered Persons:

1. An **entity** that is a foreign person and meets one of the following criteria:
   - 50% or more owned (directly or indirectly, individually or in the aggregate) by one or more countries of concern
   - 50% or more owned (directly or indirectly, individually or in the aggregate) by one or more covered persons (including other covered entities)
   - Organized or chartered under the laws of a country of concern
   - Has its principal place of business in a country of concern
2. An **individual** who is a foreign person and meets one of the following criteria:
   - Primarily a resident in the territorial jurisdiction of a country of concern
   - Employee or contractor of a country of concern or an entity that is a covered person
3. Any **individual or entity,** wherever located, **designated by the Attorney General** as a covered person (based on certain criteria)

TAKEAWAYS

UNDERSTAND THE DATA INVOLVED IN THE TRANSACTION

- Evaluate Data Processed
- Calculate Bulk Thresholds (100-100,000 depending on data)

UNDERSTAND WHERE THE DATA FLOWS AND MAY BE ACCESSED

- Sanctioned Country
- Other Foreign Country

CONSIDER CONTRACTUAL PROVISIONS TO AVOID TRIGGERING DOJ REQUIREMENTS AND/OR ADDRESS ONWARD TRANSFERS

- Assess if Data Brokerage, Vendor, Employment or Investment Contract
- Prepare Relevant Provision

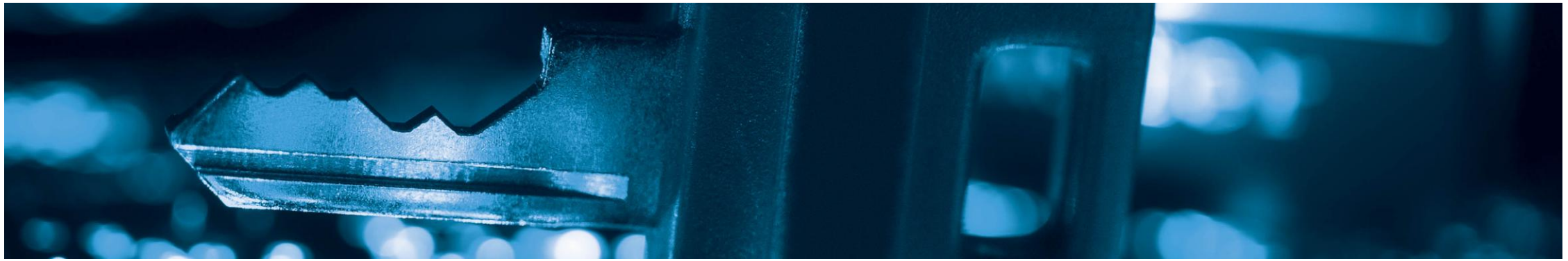
04

BRINGING IT ALL TOGETHER: UNLOCKING YOUR STRATEGY FOR ADDRESSING CROSS-BORDER TRANSFERS

UNLOCKING YOUR STRATEGY FOR ADDRESSING CROSS-BORDER TRANSFERS

Key Issues to Consider:

- The direction and types of data flows and the laws applicable to those data flows
- Where decisions about the data are taken / which teams are responsible and accountable – in one main establishment (e.g. your HQ) or across different geographies
- Any data localisation requirements / difficulties transferring data out of any specific jurisdictions that have to be addressed



Typical Strategies

- Most multinational companies typically adopt one approach (normally the most stringent, globally accepted requirements applicable to their business) and apply it as a baseline for all their international data flows, adjusting or supplementing it as needed for specific local requirements
- Organisations with large amounts of European data or customers typically adopt GDPR based standards and contracts, supplementing with additional policies and terms as may be practically needed
- Organisations with no nexus to Europe may still find that they need to put a contractual framework in place to govern data transfers, although the burden of doing so will be significantly reduced.
- Most businesses take a layered approach. E.g:
  - An organization may (if eligible) self-certify to the US-EU DPF if a substantial amount of transfers are between the US and Europe **BUT**
  - That will not negate the need for contracts to also be put in place where transfers occur between other jurisdictions.


Q&A
THANK YOU!

MAYER | BROWN