KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

September 13, 2023

Data Privacy & the Cloud: Freely Flowing Data or a Balkanized Internet

Panelists

Brian Gallagher

Associate General Counsel
Alarm.com Incorporated

Jason Gerson

Lead Counsel, Privacy & Data
Wells Fargo

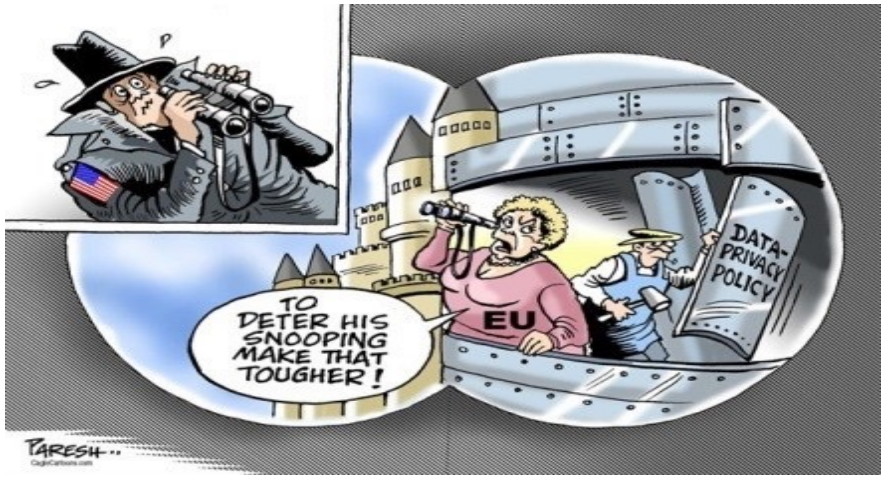
Amanda Witt

Partner
Kilpatrick Townsend

Roadmap

- Data Transfer Basics
- E.U.-U.S. Data Transfers
- US National Security Laws
- Challenges for Practitioners
- Global Data Transfers Overview
- China Data Transfers
- Data Transfers in Latin America

Cloud Challenges & the Balkanized Internet



Graphic: ST

Privacy & Security Issues in the Cloud

- Data transfer issues (EU and similar jurisdictions)
- Data location issues
- Location of users accessing data
- Movement and storage of data
- Use of subcontractors
- Lack of transparency and control
- Data breach issues
- Data destruction issues
- Ability to impose security and privacy requirements

Global data transfer contracts

By IAPP Director of Research and Insights Joe Jones

There are at least 20 draft, template or standardized contractual clauses or undertakings for international data transfers covering transfers from 71 countries.

Regions

Association of Southeast Asian Nations
Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam

Council of Europe - Draft
All European Economic Area states plus Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Moldova, Monaco, Montenegro, North Macedonia, San Marino, Turkey and the U.K.

European Economic Area
Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden

Latin American Data Protection Board (RIPD)
Andorra, Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Panama, Peru, Portugal, Spain and Uruguay

Individual jurisdictions

Abu Dhabi Global Market
Argentina
Brazil
China
Dubai International Financial Centre
Guernsey
Hong Kong
Jersey
Moldova
New Zealand
Peru
Serbia
Switzerland
Turkey
United Kingdom
Uruguay

Jurisdictions part of multiple regional contracts

Argentina†	Peru†	Spain*
Brazil†	Portugal*	Uruguay†

† Covered by their own and RIPD contracts.
* Covered by EEA and RIPD contracts.

Published April 2023.

Data Transfer Basics: Key Terminology

- **Personal Data (Art. 4(1) of the GDPR)**
  - Any information relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, **location data, an online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Processing (Art. 4(2) of the GDPR)**
  - **Any operation or set of operations which is performed on personal data** or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Transfer Basics: Key Terminology (cont'd)

- **Special Categories of Personal Data (Art. 9 of the GDPR):**
  - Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited**.
- **Exceptions:**
  - Explicit consent
  - Public interest (very rare)

Data Transfer Basics: Key Terminology (cont'd)

- **Controller (Art. 4(7) of the GDPR)**
  - The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Processor (Art. 4(8) of the GDPR)**
  - A natural or legal person, public authority, agency or other body which processes personal data **on behalf of the** controller.

Data Transfer Basics: Key Elements: Extraterritorial Reach

The GDPR applies to (Article 3):

- The processing of personal data in the context of the activities of a controller or processor **established in the EU**, regardless of whether the processing takes place in the EU or not
- The processing of personal data of data subjects who are in the EU by a controller or processor **not established in the EU**, where the processing activities are related to:
  - the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
  - the monitoring of their behavior in the EU

Data Transfer Basics: Legal Background – GDPR

- Article 46(1): "…a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided **adequate safeguards**…"
- Article 46(2)(c): "The appropriate safeguards … may be provided for, without requiring any specific authorization from a supervisory authority, by: (c) **standard data protection clauses** adopted by the Commission…"

Cloud-based Access is a Transfer

- Transfers include transmission or “making available” data to another party.
- According to the EDPB, personal data could be “made available” by creating an account, granting access rights to an existing account, “confirming”/”accepting” an effective request for remote access, embedding a hard drive or submitting a password to a file.
- Remote access from a third country (even if it takes place only by means of displaying personal data on a screen, for example in support situations, troubleshooting or for administration purposes) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer.

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

E.U.-U.S. Data Transfers

Legal Background – *Schrems II*

- What did it do?
  - Invalidated the EU-U.S. Privacy Shield framework
  - Restricted effectiveness of SCCs
- SCCs finding
  - Valid for some level of data protection, but may be insufficient
  - Additional safeguards to limit access by government authorities

International Data Transfers from the EU European Commission issued new Standard Contractual Clauses (SCCs) on June 4, 2021

- Under GDPR, cross-border transfer of personal data may not occur without an appropriate mechanism in place (adequacy decision, SCCs, Binding Corporate Rules, Derogation)
- The new SCCs reflect the evolved GDPR as well as the legal analysis from the *Schrems II* decision (which invalidated EU-US Privacy Shield and added transfer impact assessment requirements)

Important Dates

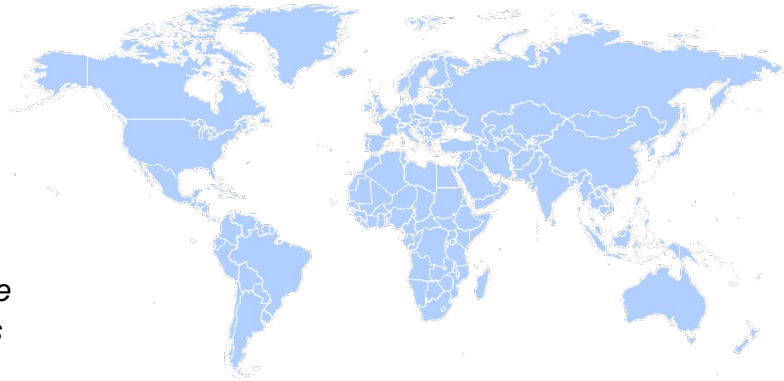
June 27, 2021
May start using the new SCCs

→

September 27, 2021
Must use the new SCCs

→

December 27, 2022
Legacy agreements must be updated with the new SCCs



When and How to use the SCCs Required for a "restricted transfer"

Test for Restricted Transfer

- Are you transferring personal data from the EEA?
- Is the recipient in a third country that does not have an adequacy decision?
- Is the intended recipient **another person or organization** (i.e., someone outside of your own company, including a subsidiary)

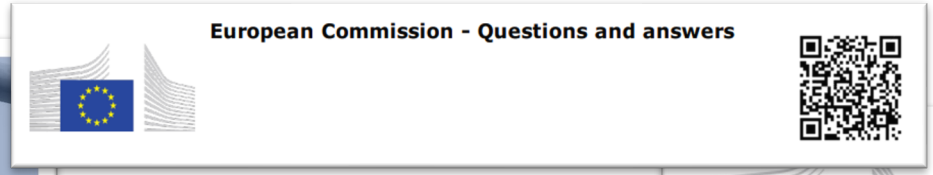
If the answer is Yes to all 3 questions, you are making a restricted transfer and need SCCs.

Then, under the *Schrems II* decision, need SCCs along with impact analysis and potentially supplementary measures if laws of recipient country do not afford appropriate privacy protections

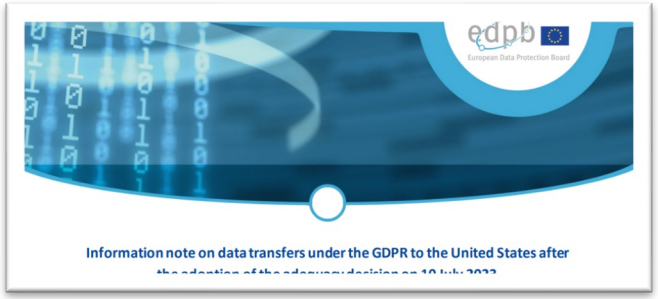
SCCs + Transfer Impact Analysis + Supplementary Measures (as applicable)

At long last…the DPF! (Or, “nobody say ‘Schrems III’”)

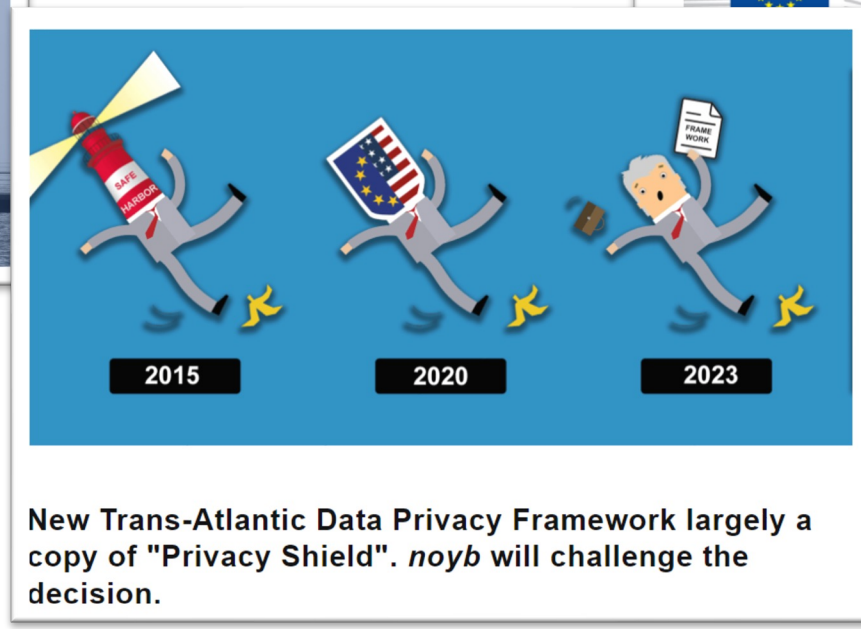
U.S. Dept. of Commerce ITA



EC FAQs



EDPB FAQs



noyb

European Commission decision

Data Privacy Framework *New Trans-Atlantic Framework (Privacy Shield 2.0)*

- On March 25, 2022, the United States and the European Commission committed to a new **Trans-Atlantic Data Privacy Framework** to replace the invalidated EU-U.S. Privacy Shield Framework
- The new Framework will ensure that:
  - Signals intelligence collection may be undertaken only where necessary to advance legitimate national security objectives
  - EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court
  - U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
- Companies will need to self-certify adherence to the Principles through the U.S. Department of Commerce.

DPF Highlights

- DPF in force July 10, 2023 – same day as EC's **adequacy decision** for EU-U.S.
- Adequacy decision based on **Executive Order** and DOJ regulations
- The US AG (DOJ NSD) designated the EU and EEA **"qualifying states"**
- **Redress:** The DPF allows Europeans to object if they suspect their data has been collected by American intelligence
  - A **Data Protection Review Court**, made up of U.S. judges, will be created to hear the claims.
- Enhanced oversight of U.S. intelligence to ensure compliance with limitations on surveillance activities
- Only **"necessary and proportionate"** data will be collected
- Organizations have three months to shift from Privacy Shield to DPF

Implementing Transatlantic Transfers

	PERSONALIZED DATA TRANSFERRED TO		
	The United States		
	A current Privacy Shield participant that is converting to the Data Privacy Framework	**A new DPF participant**	**A U.S. entity not self-certified to the DPF**
The EU, Norway, Iceland and Liechtenstein	The receiving organization must update its privacy policy no later than 10 Oct. 2023 to reflect compliance with the EU-U.S. DPF and transfer under the EU adequacy decision. It must convert from Privacy Shield to the DPF by this deadline or withdraw. The converted organization's next certification due date is listed on its record on the DPF list. Anyone may verify the U.S. organization's current participation in the DPF using these instructions.	Eligible U.S. organizations may submit applications to self-certify on the new DPF website, following all instructions closely. Only after approval by the Department of Commerce may they rely on the EU adequacy decision. The participating organization's next certification due date is 12 months after approval of its application by the Department of Commerce, with all requirements met. Anyone may verify the U.S. organization's current participation in the DPF using these instructions.	Organizations on both sides of the Atlantic may continue to rely on alternative data transfer mechanisms, e.g., standard contractual clauses. See the European Data Protection Board guidance on measures that supplement transfer tools. Transfer impact assessments can reference the EU adequacy decision and the U.S. intelligence community's implementation of Executive Order 14086 via new policies and procedures, as explained in this EDPB guidance.

Published August 2023.

Implementing Transatlantic Transfers

	PERSONALIZED DATA TRANSFERRED TO		
	The United States		
	A current Privacy Shield participant that is converting to the Data Privacy Framework	**A new DPF participant**	**A U.S. entity not self-certified to the DPF**
The U.K. and Gibraltar	Eligible U.S. receiving organizations must supplement their converted EU-U.S. Privacy Shield self-certification by applying for self-certification under the U.K. Extension to the EU-U.S. DPF. However, they may not begin relying on the U.K. Extension for transfers until after approval of the U.K.-U.S. Data Bridge. Organizations may not convert EU-U.S. Privacy Shield participation for U.K.-U.S. transfers without submitting an application. In the meantime, transfers should be effected via alternative U.K. transfer mechanisms. See guidance from the U.K. Information Commissioner's Office on transfer risk assessments.	Eligible U.S. organizations may begin applying to self-certify under the U.K. Extension to the EU-U.S. DPF. Participants must also self-certify under the EU-U.S. DPF. However, they may not begin relying on the U.K. Extension for transfers until after approval of the U.K.-U.S. Data Bridge. In the meantime, transfers should be effected via alternative U.K transfer mechanisms. See guidance from the U.K. ICO on transfer risk assessments.	Transfers must be made using alternative transfer mechanisms. See guidance from the U.K. ICO on transfer risk assessments.

Published August 2023.

Implementing Transatlantic Transfers

	PERSONALIZED DATA TRANSFERRED TO		
	The United States		
	A current Privacy Shield participant that is converting to the Data Privacy Framework	**A new DPF participant**	**A U.S. entity not self-certified to the DPF**
Switzerland	The receiving organization must update its privacy policy no later than 17 Oct. 2023 to reflect compliance with the Swiss-U.S. DPF. However, it may not begin relying on the Swiss-U.S. DPF for transfers until after the pending Swiss adequacy decision. In the meantime, transfers should be effected by alternative Swiss transfer mechanisms. See guidance from Switzerland's Federal Data Protection and Information Commissioner on data transfers.	Eligible U.S. organizations may submit applications to self-certify on the new DPF website, following all instructions closely. They may rely on the framework for transfers only after approval — and after the pending Swiss adequacy decision is finalized. In the meantime, transfers should be effected by alternative Swiss transfer mechanisms. See the FDPIC's guidance on data transfers.	Transfers must be made using alternative transfer mechanisms. See the FDPIC's guidance on data transfers.

Published August 2023.

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

U.S. National Security Laws

US Security Laws – FISA 702

§702 of the Foreign Intelligence Surveillance Act

- FISA 702 governs the collection of intelligence related to *non-U.S. Persons* reasonably believed to be located *outside* the USA.
- The U.S. government may issue "directives" to "electronic communication service providers" ("**ECSPs**") for "all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition."
- Due to a broad interpretation of ECSP, U.S. companies providing internal communications platforms (e.g., email to employees) may be subject to FISA 702.
- Checks & Balances: the U.S. Attorney General and the Director of National Intelligence jointly draft acquisition request (certificates), containing 'targeting and minimization procedures,' and submit these for approval by the Foreign Intelligence Surveillance Court (FISC), who will approve or deny these requests in 'opinions.'

FISA 702 Deep Dive

"Electronic Communications Service Provider?"

A. a telecommunications carrier, as that term is defined in section 153 of title 47

B. a provider of electronic communication service, as that term is defined in section 2510 of title 18;

C. a provider of a remote computing service, as that term is defined in section 2711 of title 18

D. any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

E. an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

Provider of "Remote Computing Service?"

- Defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications," and includes no requirement that the service be provided to the public or any other third-parties.

FISA 702 – Risks of Using an Electronic Communication Service Provider

- If an entity is not itself subject to FISA 702 but uses an electronic communication service provider to process certain data, is it possible that U.S. intelligence agencies may gain access to such data under FISA 702?
  - Yes. Insofar as the data is in the possession of the electronic communication service provider, it can be subject to collection under section 702 regardless of whether the data is "owned" or otherwise controlled by an entity other than the provider. That is to say, the question is not where the data comes from; it is whether, at the time the query is run, it is at rest or in motion through the electronic communication service provider's infrastructure.

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Challenges for Practitioners

Cloud Provider Challenges

Industry Headaches

- Myriad of data transfer laws / requirements
- DPA Negotiations
- Data Localization Requirements

DPA Negotiation Pitfalls

- Indemnity for breach of the Data Processing Agreement (DPA)/personal data breach and limitation of liability
- Audit rights
- Costs of personal data breach
- Timing for notices

Cloud-based Privacy / Cross-border Data Dynamics Within Regulated Entities

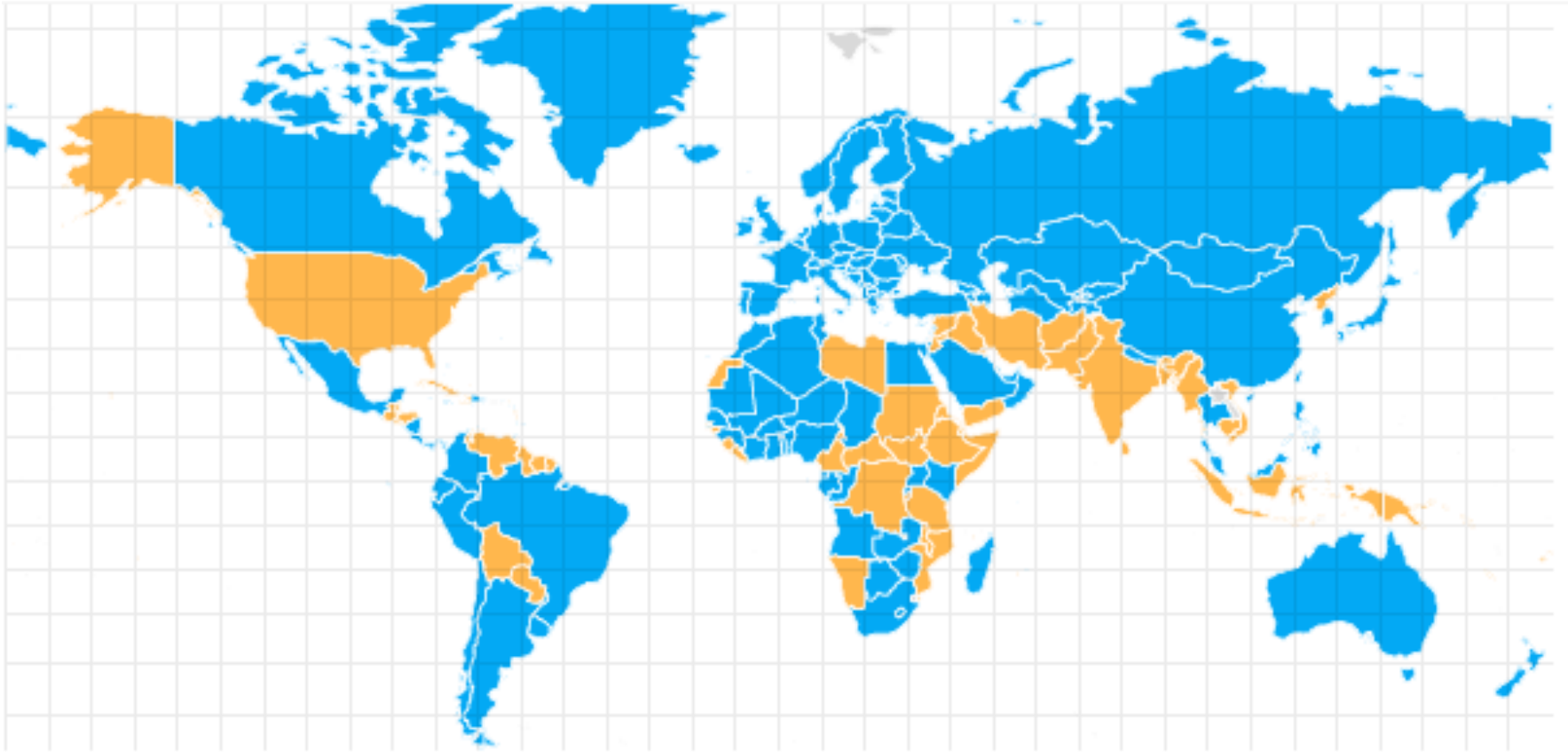
- Bifurcated functions between legal + risk + privacy ops
- Regulated entities generally are more trusted by consumers than non-regulated entities on privacy
- Regulated entities can inadvertently be swept up by legal frameworks not really written with them in mind
- Need to balance pressure to deploy PETs with pressure to ensure data integrity
- DPF is not available to certain regulated entities
  - BCRs of limited utility
- Financial institutions + SCCs
- Interplay of CPRA/CCPA + GLBA for online visitors and prospects

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Global Data Transfers Overview

Global Privacy Laws



International Data Transfers Overview

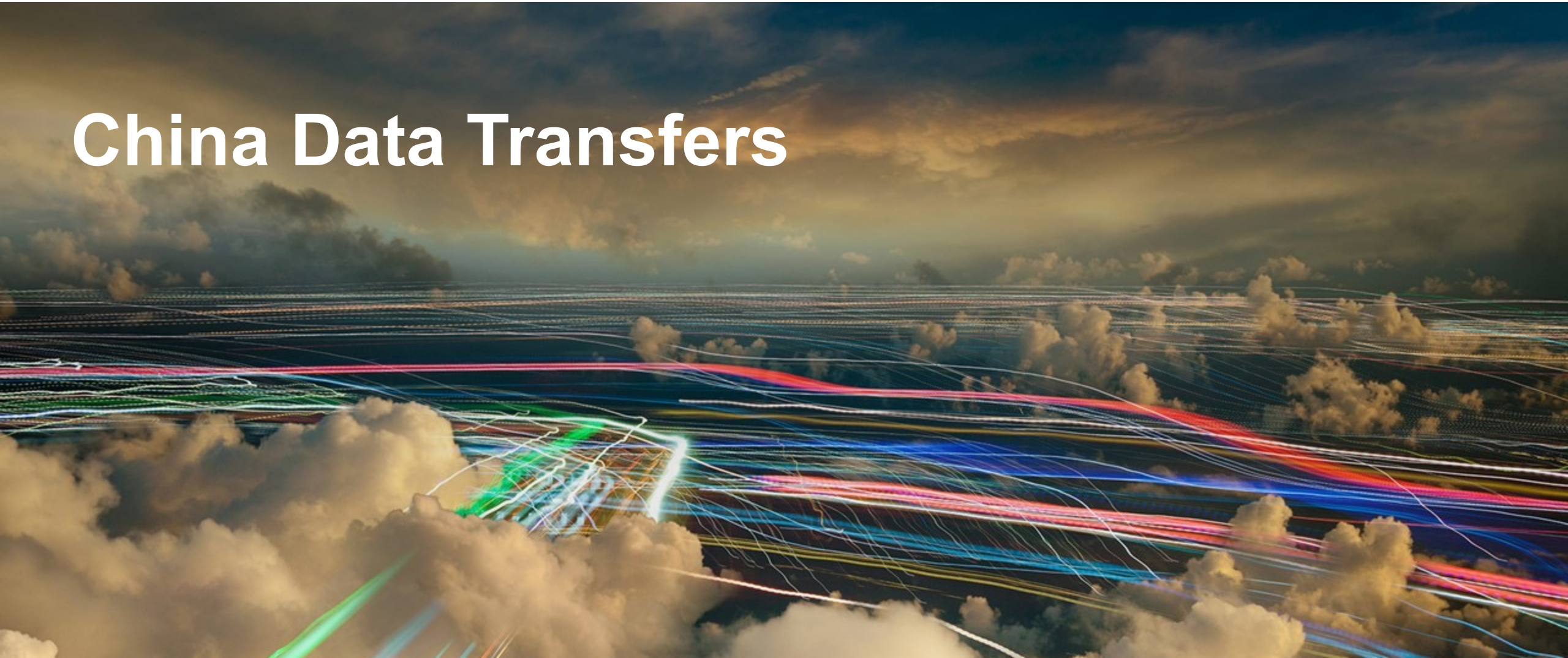
Global focus remains on protecting personal data that transfers across borders.

- **European Union & the United Kingdom:**
  - Strong distrust of the ability for companies in the United States to truly protect personal data from government surveillance continues to drive doubt.
  - Even the new EU Standard Contractual Clauses aren't enough in some regulators' view.
  - New(ish) UK IDTA
- **China:** Similar caution underlies increased data transfer protection obligations in the newly-implemented PIPL (eff. November 2021).
- **South America:**
  - Brazil's LGPD contains similar cross-border transfer requirements to the GDPR
  - Argentina has its own set of Standard Contractual Clauses and models its approach on GDPR.

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

China Data Transfers



International Data Transfers *China*

China's Personal Information Protection Law (PIPL) (effective November 2021)

- **Data localization**
  - The Cybersecurity Law (CSL) of 2017 contains data localization requirements for personal information held by Critical Information Infrastructure (CII) Operators (Art. 37). There are numerous other data localization requirements pertaining to specific sectors and types of data (e.g., banking, healthcare, internet mapping).
  - PIPL requires CII operators or entities processing a large amount of information to store the data locally, and if transfer is necessary, pass a security assessment (PIPL Art. 40).
- **International transfer restrictions**
  - Under PIPL, in general, organizations are required to provide individuals with certain information about the transfer, obtain specific consent, adopt measures to make sure the third country provides the same level of protection, and carry out a data protection impact assessment (PIPL Arts. 39, 38, 55). They must also meet one of the conditions for transfers, such as passing a security assessment (mandatory for certain organizations) or concluding a standardized contract (PIPL Art. 38)
  - Foreign entities can be added to a sanctions list whereby they may be restricted or prohibited from receiving personal information.
  - There is no similar process to the GDPR for authorities to designate countries as having adequate safeguards.

Data Transfers from China

- **China's Personal Information Protection Law (PIPL):** Applies to organizations operating in China and to organizations/businesses outside of China that process personal data to offer goods and services or analyze the behavior of Chinese natural persons, and to any (unspecified) "circumstances stipulated by laws and administrative regulations"

- **3 Data Transfer Mechanisms:**
  1. Complete a security assessment by the Cyberspace Administration of China;
  2. Complete a security certification by a certification institution designated by the Cyberspace Administration of China; or
  3. Adopt the standard contractual clauses (SCCs).

- Data exporters must file the executed standard contractual clauses along with the protection impact assessment report with the provincial Cyberspace Administration of China where they are located within 10 working days.

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Data Transfers in Latin America

International Data Transfers Latam (Brazil & Argentina)

- Brazil's LGPD (2020) mirrors GDPR cross-border transfer requirements, e.g., transfer mechanisms or adequacy; prior specific consent. (General restriction on international transfers, with exceptions.)
- Brazil's regulator (ANPD) has yet to release a list of countries with adequacy decisions. The ANPD was expected to release guidance on cross-border transfers in 2022 and announced a public hearing on a draft resolution on data transfers and SCCs on September 12, 2023.
- The ANPD will regulate the use of model DTAs, SCCs, etc. The ANPD's director indicated that she prefers a simpler approach to SCCs rather than the EU approach complicated by Schrems II.
- Hosting data in foreign countries is considered a form of international data transfer.

Data localization

- The LGPD does not specifically regulate data localization, but other laws may apply, including for the financial and public sectors.

- Argentina's Personal Data Protection Act (PDPA) was enacted in 2000.
- Main Regulations enacted in December 2001
- 2002 - recognized as adequate in Opinion 4 of 2002 by EU Commission
- Article 12 of the PDPA prevents the transfer of personal data to a country that does not provide an adequate level of protection.
- International transfers: Argentine SCCs approved 2016
- Transfers to non-adequate countries only permitted if:
  - Data subject expressly consents
  - Data is transferred pursuant to an agreement with SCCs
  - Intragroup transfers if Binding Corporate Rules have been put in place

International Data Transfers *Checklist*

- Assess and document where international data transfers are happening (internal and external).
- Determine whether data localization requirements apply.
- Prioritize transfer types, third parties, and countries for selecting appropriate transfer mechanisms that work for your client.
- Execute data protection agreements, including SCCs (where needed), to establish appropriate transfer-related obligations.
- Conduct and document transfer impact assessments.

Questions?

Locations

Counsel to innovative companies and brands around the world

We help leaders create, expand, and protect the value of their companies and most prized assets by bringing an equal balance of business acumen, technical skill, and creative thinking to the opportunities and challenges they face.

Anchorage
Atlanta
Augusta
Beijing
Charlotte
Chicago
Dallas
Denver
Houston
Los Angeles
New York
Phoenix
Raleigh
San Diego
San Francisco
Seattle
Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem