

8 November 2023

Cross-Border Data Transfer

Workshop

Speakers



Allison Brody

Chief Privacy Officer
RELX



Lee Matheson

Senior Counsel
FPF



Will Bracker

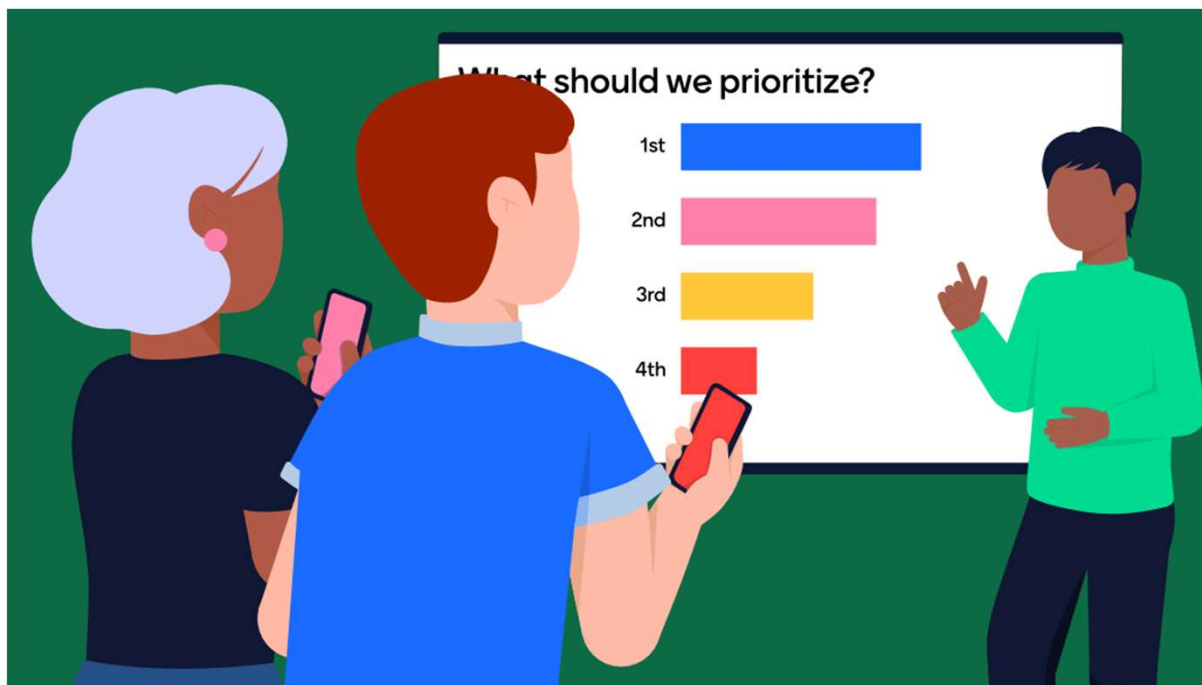
Senior Counsel
Cox Communications



Dr. Kai Westerwelle

Partner
Bird & Bird

Interactive



- ✓ We will make this **INTERACTIVE**
- ✓ We will do **POLLS**
- ✓ We will initiate **GROUP WORK**
- ✓ Please ask **QUESTIONS** (also via app)

Interactive

Go to
www.menti.com

Enter the code

8957 9389



Or use QR code

Poll

Join at menti.com use code 8957 9389

 Mentimeter

How familiar are you with cross-border data transfers?

1st | No background,
here to learn

2nd | Basic
understanding

3rd | Familiar, use day-
to-day

4th | Expert



GO TO
menti.com

ENTER THE CODE
8957 9389

 0



Poll

Join at menti.com use code 8957 9389

 Mentimeter

I would like to know more about?



Poll

Join at menti.com use code 8957 9389

 Mentimeter

The question I would most like to hear the panel address is:

I came all the way to DC to ask....



Questions



Join at menti.com use code 8957 9389

 Mentimeter

Ask me anything

No questions from the audience!

Incoming questions will show up here so that you can answer them one by one.



Tross Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Let's Play



Do the following scenarios constitute Cross-Boarder Transfer of Personal Data?

1. Consumer A in Germany purchases a T-Shirt from the US based platform "Golf US". Golf US is an English language (only) website. A pays in EURO with no VAT added.
2. Student S from France attends a virtual MBA program in Paris. Speakers include experts lecturing from the US and Singapore.
3. Canadian company C offers "EU based" cloud services. The service is run on EU based servers with first level support in Ireland. 2nd level support is provided from C's HQ in Canada.
4. Company Y (B2B only) in Spain is raising its series C. It offers customer and employee data for the due diligence of possible investors. A data room has been created by the international law firm L in Madrid. LawCloud Inc, the worldwide cloud service provider of L, has its servers in the US and Canada.

Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

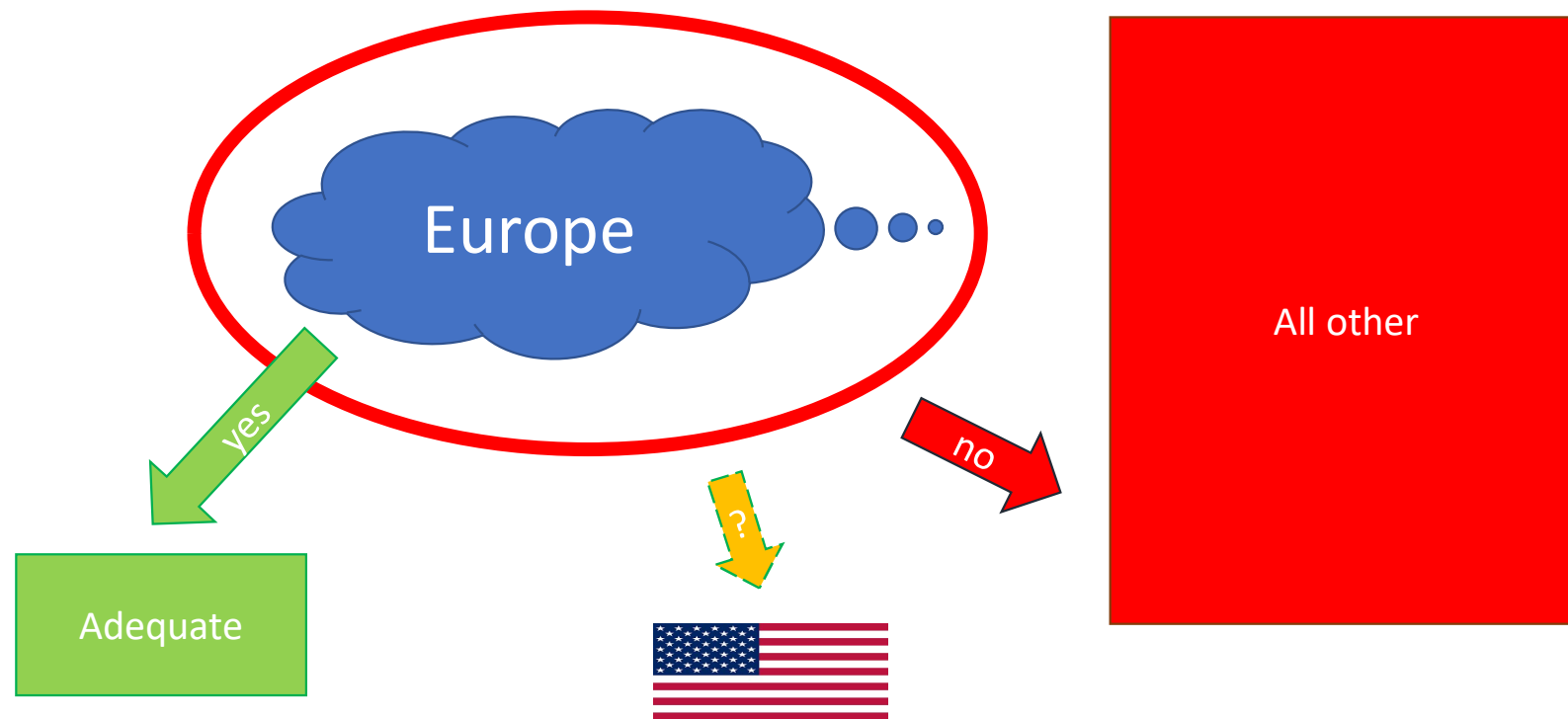
DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Data Transfers from Europe / UK



Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Consent

Standard
Contractual
Clauses

Binding
Corporate
Rules

Safe Harbor

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Consent

- By the Data Subject
 - Clear and affirmative action
 - Fully informed on data processing
 - Freely given
 - Can be withdrawn any time
- | | |
|---|--|
| <ul style="list-style-type: none">• Easy Set-up• Safe if correct• Sustainable | <ul style="list-style-type: none">• Individual Solution• Ltd use for B2B• Employment issue |
|---|--|

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

- All companies apply same standard
- Comprehensive process
- Need to be DPA approved
- Very expensive and burdensome
- Not for small to midsize companies

- Full coverage
- DPA Approved
- Sustainable

- Expensive
- Difficult set-up
- EU backlog

Binding
Corporate
Rules

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Standard Contractual Clauses

- EU Standard contract (different sets)
- Between data exporter and data importer
- Importer to comply with EU standards
- Easy, fast and cheap solution
- "The" standard for data transfer

- Easy set-up
- No DPA approval
- Worldwide

- Not negotiable
- Negative add-ons
- Liability

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

- First EU US Agreement (2000)
- US only (!)
- High importance for US companies
- Easy, fast and cheap solution
- "The" standard for data transfer to US

- Easy set-up
- No DPA approval
- No audits

- EU to US only
- Criticized
- Int. politics

Safe Harbor

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Consent

Standard
Contractual
Clauses

Binding
Corporate
Rules

~~Schrems
I
(2015)~~

Data Transfers from Europe / UK



- US Authorities can access personal data (intelligence)
- No supervision
- No legal means for EU data subjects to claim their rights in the US

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Consent

Standard
Contractual
Clauses

Binding
Corporate
Rules

~~Schrems
II
(07-16-20)~~

Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

OK

Consent

Obligation

Standard
Contractual
Clauses

Obligation

Binding
Corporate
Rules

NO

Privacy Shield

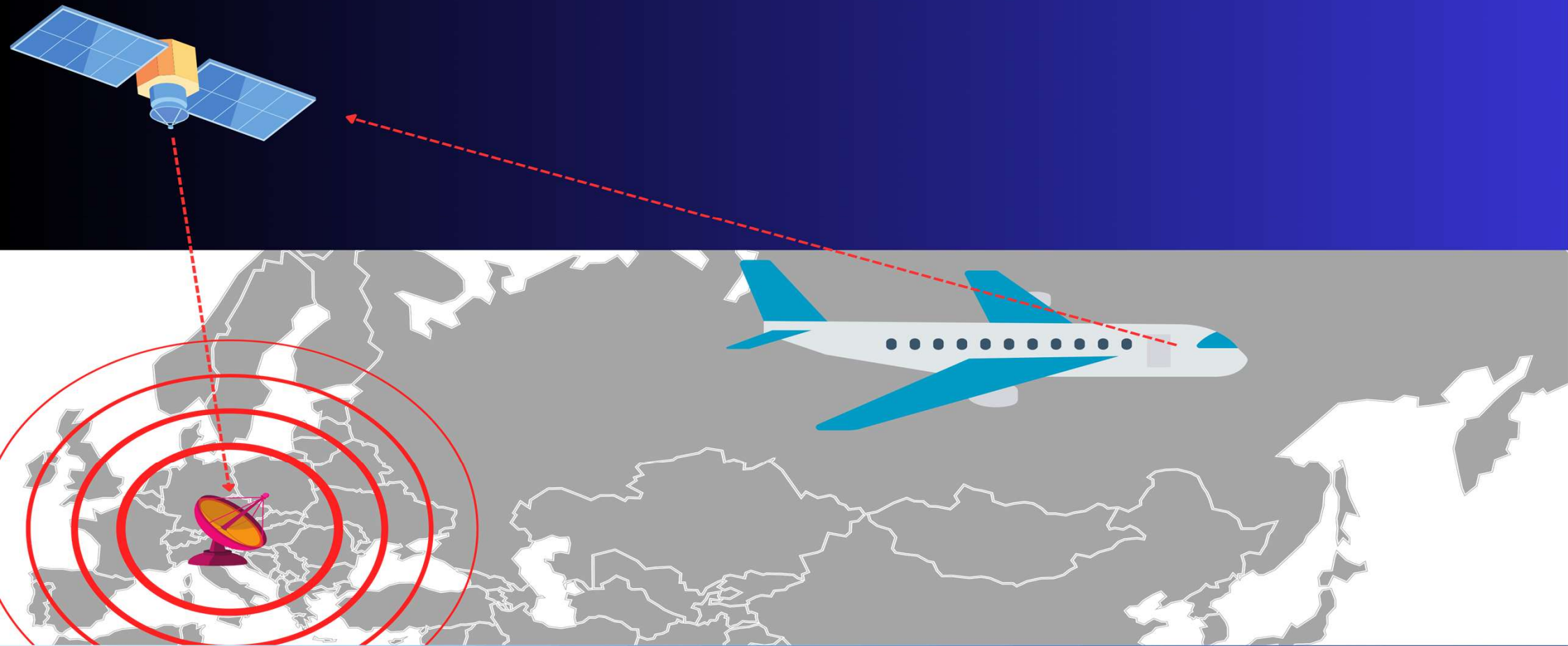
Questions



Let's Play



Group Work



Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

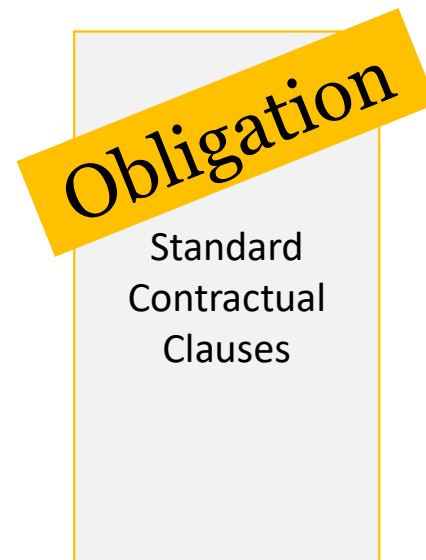
Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Standard Contractual Clauses - Deep Dive

Mechanisms for data transfer EU to the US



Standard Contractual Clauses – after Schrems II

Substantial obligations for the parties of the SCC contract !

- Ensure "appropriate protection" – SCCs are just part of this
- Consider the law of importing country (Privacy Shield standards)
- Additional safeguards (clauses or other safeguards) may be required
- Importer (US) must notify exporter if it cannot meet obligations
- If exporter still transfers data, it must send notification to DPA

EU Standard Contractual Clauses



Word Documents

EU Standard Contractual Clauses

EU Standard Contractual Clauses



Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

**on standard contractual clauses for the transfer of personal data to third countries
pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

EU Standard Contractual Clauses



STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

EU Standard Contractual Clauses



Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

EU Standard Contractual Clauses



Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

EU Standard Contractual Clauses



APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

EU Standard Contractual Clauses



ANNEX I [continued]

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

EU Standard Contractual Clauses



ANNEX I [continued]

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Nature of the processing

Purpose(s) of the data transfer and further processing

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

EU Standard Contractual Clauses



ANNEX I [continued]

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of personal data transferred

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Nature of the processing

Purpose(s) of the data transfer and further processing

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

EU Standard Contractual Clauses



ANNEX I [continued]

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

EU Standard Contractual Clauses



ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner . . .

EU Standard Contractual Clauses



ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...

EU Standard Contractual Clauses



What about Switzerland and the UK? Some companies add, for example:

ANNEX IV SUPPLEMENTARY TERMS FOR SWISS FADP TRANSFERS ONLY

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the Swiss FADP:

...

ANNEX V SUPPLEMENTARY TERMS FOR UK GDPR TRANSFERS ONLY

The following United Kingdom International Data Transfer Addendum to the European Commission Standard Contractual Clauses supplements the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the UK GDPR.

...

EU Standard Contractual Clauses



Many companies post their EU SCC with UK and Swiss supplements in jurisdiction-specific online terms, and even incorporated by reference the bulk of the substance of the EU SCC, e.g.:

To the extent that Customer transfers Personal Information from the European Economic Area (“EEA”) to Service Provider located outside the EEA, unless the Parties may rely on an alternative transfer mechanism or basis under the Data Protection Laws, the Parties will be deemed to have entered into the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 available at http://data.europa.eu/eli/dec_impl/2021/914/oj (“Clauses”) in respect of such transfer, whereby:

a. Customer is the “data exporter” and Service Provider is the “data importer”

Questions



Let's Play



Poll

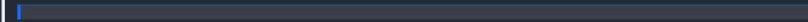
Join at menti.com use code 8957 9389

 Mentimeter

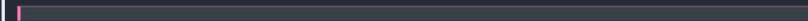
Learning check

Strongly disagree

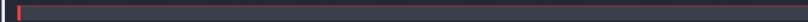
I'm understanding the concepts



I'm able to keep up with the presentation



I'm getting the right answers to the questions



Strongly agree



Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Data Privacy Framework (DPF)

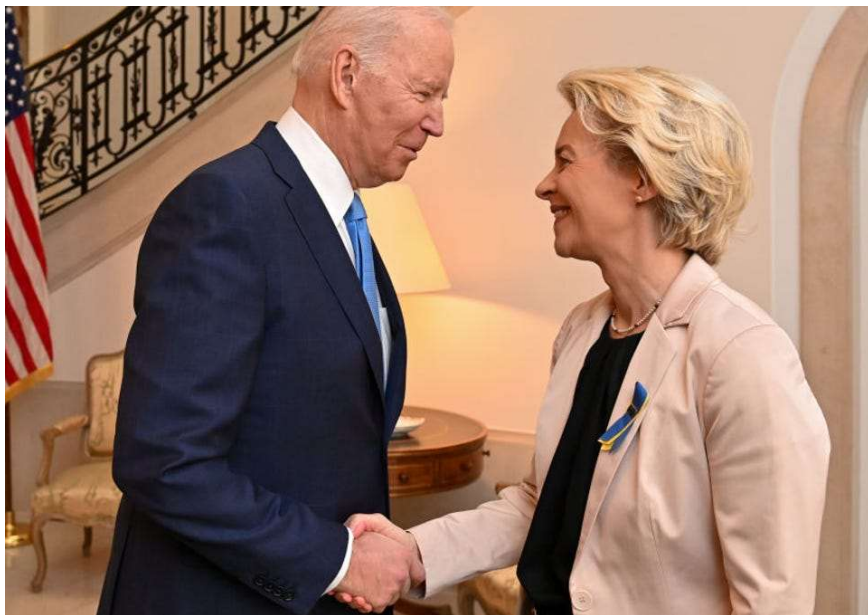
Mechanisms for data transfer EU to the US



Data Privacy Framework - Background



Data Privacy Framework – Privacy Shield II ?



- July 10, 2023 EU adopts EU-US DPF
- Principles: notice, choice, accountability for onward transfers, security, data integrity and purpose limitation, access and recourse, enforcement
- New: controls to mitigate deficiencies
- New: better rights for individuals to redress claims (Data Protection Review Court)

Data Privacy Framework - Executive Order



- ✓ Adds further safeguards for U.S. intelligence activities (i.a. Civil Liberties Protection Officer)
- ✓ Mandates handling requirements for personal information
- ✓ Creates multi-layer mechanism for individuals to redress claims (Data Protection Review Court)



SCC v DPF for transfers to US

SCC and DPF impose similar compliance requirements, for example:

- **Transparency:** Give notice of types of personal data transferred
 - DPF: 'Notice' principle
 - SCC: Clause 8.2 (Transparency) (Module 1)
- **Individual rights:** Allow requests to access, correct, amend or delete transferred data
 - DPF: 'Access' principle
 - SCC: Clause 10(a) (Data Subject Rights) (Module 1)
- **Redress/recourse:** Ensure mechanisms for handling complaints of noncompliance
 - DPF: 'Recourse, Enforcement and Liability' principle
 - SCC: Clause 11 (Redress)

SCC v DPF for transfers to US



SCC and DPF undergo different implementations, for example:

- **Means of commitment**
 - DPF: Self-certification for all transfers + annual fee payment
 - SCC: Contract for each transfer (or all transfers if SCC online) + TIA
- **Demonstration of commitment**
 - DPF: Publicly available, searchable register online at <https://www.dataprivacyframework.gov>
 - SCC: Private, unless SCC publicly available online
- **Challenges to effectiveness**
 - DPF: High-profile legal challenges to framework underway, although likely to take time
 - SCC: No high-profile challenges, although regulator order to cease transfers possible

WELCOME TO THE DATA PRIVACY FRAMEWORK (DPF) PROGRAM

The EU-U.S. DPF, UK Extension to the EU-U.S. DPF, and Swiss-U.S. DPF were respectively developed by the U.S. Department of Commerce and the European Commission, UK Government, and Swiss Federal Administration to provide U.S. organizations with reliable mechanisms for personal data transfers to the United States from the European Union, United Kingdom, and Switzerland while ensuring data protection that is consistent with EU, UK, and Swiss law.

[LEARN MORE](#)

Considerations for DPF Certification: Pros



- 1) **Convenient.** Convenient, cost-effective transfer mechanism that reduces paperwork burden (SCC, TIA), negotiation time and effort, and alternative commercial proposals with customers
- 2) **Strong.** Despite criticism, DPF is stronger and may be perceived as a kind of ‘privacy seal’ that provides a competitive advantage or serves as a prerequisite for doing business in EU/EEA/UK/CH
- 3) **Straightforward.** For Privacy Shield-certified organizations: Changes present little significant operational impact
- 4) **Manageable.** For “B2B” organizations: Keeping scope of certification limited to personal data received from your EU/EEA/UK/CH business customers limits scope of verification assessments and supplier contracts involved in “Onward Transfer”; and processing solely as “processor” (i.e., only on instructions from “controller”) limits scope too

Considerations for DPF Certification: Cons



- 1) **Scrutinized.** Subject to public ‘look up’ and scrutiny and wider array of enforcement authorities and avenues of redress (IDR, FTC)
- 2) **Susceptible.** Legal challenges to DPF have commenced, which may cause unease with customers, which may insist on alternatives anyway
- 3) **Redundant.** Most organizations already migrated to or rely on SCC anyway
- 4) **Costly.** Costs (outside counsel, consultants, internal resources’ time and effort) to conduct due diligence and assess language in certification, external notice, internal policies, customer contracts and supplier (“agent”) contracts satisfies requirements and any applicable exemptions

See also *Why should my company join the EU-US Data Privacy Framework?* (IAPP Privacy Perspectives, Oct. 17, 2023) <https://iapp.org/news/a/why-should-my-company-join-the-eu-u-s-data-privacy-framework/>

A grayscale photograph of a dense city skyline, likely New York City, with numerous skyscrapers and buildings. The Empire State Building is prominent on the right side.

U.S. BUSINESSES

This website provides information to help U.S. businesses understand the benefits and requirements of participation in the Data Privacy Framework (DPF) program.

<https://www.dataprivacyframework.gov/s/us-businesses>

How to join the DPF program



Pre-certification logistics

Identify:

- ✓ Which organization(s) to certify
 - Determine the entities that “receive” personal data either directly or indirectly from EEA/UK/CH
 - Narrowly specify divisions or businesses based on product/service, if appropriate

- ✓ Which personal data to certify
 - Determine which kinds of personal data to include in scope
 - Non-HR data (customer data, client data, visitor data, clinical trial data, etc.)
 - HR data (personal data about employees, past and present)

<https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-1-dpf>

How to join the DPF program



Pre-certification logistics

Identify who will:

- ✓ Serve as internal point of contact in each business/group to validate data flows
- ✓ Handle access requests, questions, complaints and any other Privacy Shield issues
- ✓ Conduct staff training
- ✓ Handle certification renewals and updates
- ✓ Serve as independent recourse mechanism (a/k/a ADR provider)
- ✓ Verify compliance via in-house self-assessment *or* outside/third-party compliance review
- ✓ Certify compliance via in-house executive *or* outside/third-party letter of attestation

<https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-2-dpf>

How to join the DPF program



Pre-certification logistics

Develop a DPF-Compliant Privacy Policy:

- ✓ Ensure Privacy Policy Conforms to the DPF Principles: [Notice Principle](#) essentially provides a checklist
- ✓ Specify Compliance with the DPF Principles: Explicitly state adherence to the relevant DPF Principles and link to <https://www.dataprivacyframework.gov>
- ✓ Identify Independent Recourse Mechanism: Link to the relevant website or complaint submission form of the mechanism available to investigate unresolved complaints
- ✓ Make Privacy Policy Publicly Available: Provide the web address (except if HR only, corporate intranet OK)

See [Privacy Policy FAQs](#)

How to join the DPF program



Pre-certification logistics

Draft/update and verify:

- ✓ Internal compliance policies and procedures
 - Explain how DPF Principles are implemented, including:
 - Data integrity and retention policy and procedures
 - Access and correction policy and procedures
 - Complaint handling and escalation policy and procedures
 - Security policies, standards and controls (cross-reference existing ones)
- ✓ Internal compliance training
 - Explain requirements and operating procedures to relevant staff
 - Stand-alone deck, computer-based training (CBT), or add-on, supplemental training module to existing CBT

How to join the DPF program



Self-Certification

Submit:


- ✓ Organization name, mailing address, contact and corporate officer, email addresses
- ✓ Organization's annual revenue (to determine fee)
- ✓ Organization's number of employees (range), industry, industry sector [optional]
- ✓ Organization's affiliates also adhering to DPF ("covered entities")
- ✓ Description of personal data received, including purposes of processing and third-party recipients
- ✓ Verification method (self-assessment or outside compliance review)
- ✓ Details about organization's DPF Privacy Policy, including URL and effective date
- ✓ Independent recourse mechanism
- ✓ Payment <https://www.dataprivacyframework.gov/s/article/Self-Certification-Information-dpf>

How to verify participation



Participant Search

https://www.dataprivacyframework.gov/s/participant-search



**DATA PRIVACY
FRAMEWORK
PROGRAM**

Search

Log in

Home Self-Certify Data Privacy Framework List Audiences ▾ About ▾

ACTIVE INACTIVE

Search

Advanced Search

Post-certification



Annual renewal and updates

- ✓ Docket the annual renewal deadline
 - Email reminders will be sent from the DPF team but keep that email address up to date!
- ✓ Keep registrations, notices, policies, trainings, etc. up to date
 - 1) add new or acquired entities
 - 2) withdraw divested or merged entities
 - 3) update names of entities from reorgs and acquisitions
 - 4) update names/titles of contacts from job changes
- ✓ Ensure complaint mechanisms/inboxes are monitored
- ✓ Optional: Engage an IRM to help with compliance support
- ✓ Remember your DPF/ITA website username and password!

A screenshot of the login page for the Department of Commerce International Trade Administration. The page features the department's seal and logo at the top. Below the header, there are two input fields: "Username" with a person icon and "Password" with a lock icon. A dark blue "Log in" button is positioned below the password field. At the bottom, there are two links: "Forgot Password?" and "Sign Up".

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

INTERNATIONAL
TRADE
ADMINISTRATION

Username

Password

Log in

[Forgot Password?](#) [Sign Up](#)

Questions



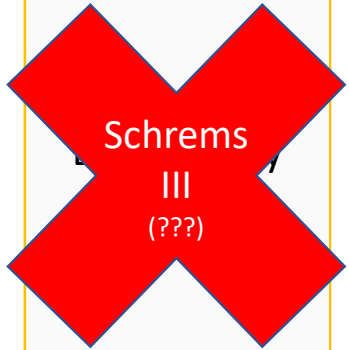
Data Transfers from Europe / UK

Mechanisms for data transfer EU to the US

Consent

Standard
Contractual
Clauses

Binding
Corporate
Rules

Schrems
III
(???)

BRIEFING



Reaching the EU-US Data Privacy Framework: First reactions to Executive Order 14086

... "Moreover, the interplay between the executive order and the Cloud Act remains uncertain. Furthermore, the Baden-Württemberg DPA pinpoints discrepancies between EU and US interpretations of 'proportionality', pointing out that the permission of bulk surveillance does not meet CJEU standards. Finally, it criticises that lodging a complaint with the CLPO is subject to the fulfilment of substantial requirements, which may present a means of preventing 'unwelcome' complaints; that the order envisages the DPRC as being part of the executive branch, which runs contrary to judicial independence; and that the neither-confirm nor-deny principle hampers effective redress. ..."

Data Privacy Framework – Schrems III

- November 2022 (IAPP EU DP Congress): going to CJEU re DPF
 - DPF still allows for data collection by US intelligence agencies, and what constitutes as “necessary and proportionate” is open to interpretation
 - The Data Protection Review Court (DPRC) may not meet the standards of independence, transparency, and impartiality required under EU law
 - The DPF doesn’t address onward transfers of data from the US to third countries, which may pose additional risks to EU individuals’ data
- noyb (none of your business) already on it



Data Privacy Framework – Latombe I



POLITICO

Enter keyword



EXPLORE ▾

NEWSLETTERS & PODCASTS ▾

POLITICO PRO

French lawmaker challenges transatlantic data deal before EU court

MP Philippe Latombe launches the latest round of legal fighting.



Latombe filed two challenges, he told POLITICO: one to suspend the agreement immediately and another on the text's content | Joel Saget/AFP via Getty Images

- September 7th 2023
- Challenging the DPF at the CJEU:

"The text resulting from these negotiations violates the Union's Charter of Fundamental Rights, due to insufficient guarantees of respect for private and family life with regard to bulk collection of personal data, and the General Data Protection Regulation ([GDPR](#)),"

- October 12, 2023 - CJEU denies Interim Measures

Data Privacy Framework – The Germans ...

AAA Kontakt Impressum Drucken

TLfDI
Thüringer Landesbeauftragter
für den Datenschutz
und die Informationsfreiheit

Animation einschalten

- Videoüberwachung
- Gesundheit
- Technik
- \$\$\$
- Soziales
- Aktenlager Immelborn
- Bildungswesen

Datenschutzerklärung

WIR ÜBER UNS ► DATENSCHUTZ ► INFORMATIONSFREIHEIT / TRANSPARENZGESETZ ► EUROPA ► PRESSE ► INFOTHEK ►

TLfDI UNTERNEHMEN
Datenschutz in Unternehmen
► zum Datenschutz in Unternehmen

TLfDI TRANSPARENZ
Sie suchen Informationen von Thüringer Behörden?
► Hier geht es zum Thüringer Transparenzportal

TLfDI
Datenschutz in Kommunen

TLfDI
Quellensammlung für

10 Jahre Informationsfreiheit - Talkrunde in Kooperation mit der TLM
► hier geht's zum Video der Talkrunde

YoungData
► Jugendportal der Datenschutzbehörden

Landesbeauftragter Dr. Lutz Hasse

„Unternehmen etwa sollten vor diesem Hintergrund abwägen, ob sie sensible Daten – auch Kundendaten – in die USA transferieren oder bis zur Entscheidung des EuGH vorsorglich nicht. Denn die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, ist danach recht hoch.

Let's Play



Poll



How long will the Data Privacy Framework last?

1. Less than 2 years
2. 2 – 3 years
3. 3 – 5 years
4. Forever

Poll



Given the uncertainty, will you advocate the self-certification under the DPF in your company?

1. We are already in the process of self-certifying under the DPF.
2. I will not advocate the self-certification of my company.
3. I will advocate the self-certification of my company.
4. I am not sure / still evaluating.

Group Work



Would anyone share the reasons for their answer with the group?

Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Other Regions - APAC



APAC Countries with Recent Developments

China – Personal Information Protection Law (PIPL), adopted 2021.

India – Digital Personal Data Protection Act (DPDP), adopted 2023.

Indonesia -- Personal Data Protection Bill (PDP), adopted 2022.

Japan, -- Act on Protection of Personal Information (APPI), amended 2022.

South Korea – Personal Information Protection Act (PIPA), amended 2023

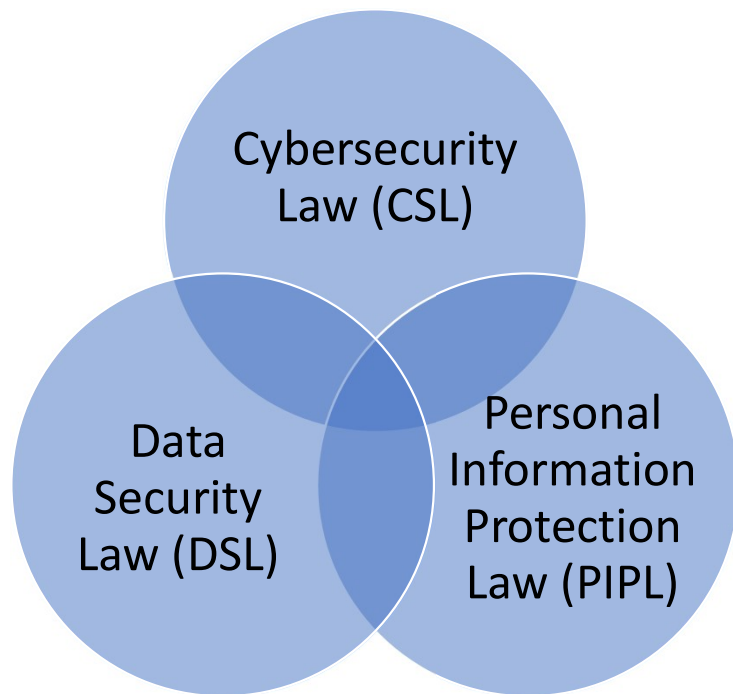
Thailand -- Personal Data Protection Act (PDPA), adopted 2019.

Vietnam – Decree of Personal Data Protection (DPDP), promulgated 2023.

Common Features in APAC Data Protection Laws

- Assessment of the level of personal data protection in the destination jurisdiction (also known as “adequacy”);
- Adoption of safeguards, such as legally binding agreements or certifications or rules approved by a regulator;
- Consent from data subjects; and/or
- Necessity for various, specifically defined purposes.

Other Regions - China



CSL – general “security assessment” required for “critical infrastructure operators” and the transfer of PI or “important data” out of the PRC.

PIPL – Article 38 provides four lawful bases for transferring data out of the PRC:

1. Passing a CAC Security Assessment
2. Undergoing certification by a body approved by the CAC
3. Using the standard contract provided by the CAC
4. Complying with conditions provided in other law or regulation, or as required by the CAC.

Other Regions - China

Other Key Features of the PIPL:

- ❖ There is no adequacy/whitelist process
- ❖ Consent is not an independent legal basis for transfers out of China (though may still be relevant if it is the Article 13 basis for general processing)

Recent Developments:

CAC Draft Provisions on Regulating and Promoting Cross-Border Data published September 2023 ease the basis requirement for specific types of transfer, for example:

- Transfers of employee data for HR purposes;
- Transfers necessary for a contract with the data subject
- Transfers of PI collected outside of China and stored in China;
- Transfers of fewer than 10,000 individuals' information in 1 year;
- Transfers of between 10,000 and 1,000,000 individuals' data may not need a security assessment.

China's Standard Contract

Published by the CAC in February, 2023, the Standard Contract Measures are one of the bases for transfer under the PIPL. Key SCM requirements include:

- ☐ A template risk assessment that any transferor must use, documenting various features of the transfer.
- ☐ Filing the executed SCM with the CAC within 10 days of its effective date

Notably, the Standard Contract does NOT distinguish between controller-controller and controller-processor transfers. There is a single form that must be signed, unaltered, by both parties.

Other Regions – Brazil



Chapter V of the LGPD:

- ❖ Brazil's law is structured similarly to the GDPR -- it contains a number of lawful bases for the transfer of personal data, including:
 - ❖ Adequacy
 - ❖ The use of standard contract clauses
 - ❖ Binding corporate rules
 - ❖ Authorized stamps, certificates, or codes of conduct
 - ❖ Necessity, either for a variety of government purposes, or to protect the life or physical safety of the data subject
 - ❖ When the data subject has provided specific, highlighted consent to the transfer, distinct from other purposes.

Brazil's Standard Contract Clauses

- ❖ The ANPD published draft regulations on international data transfers and a draft contract on August 15, 2023.
 - ❖ Brazil's SCCs have only one model, similar to the PIPL's Standard Contract.
 - ❖ If both the exporter and importer are processors, the contracts require the "third party controller" to sign as well.
 - ❖ Brazil's current draft does not include any provisions related to automated decisions or AI

Other Cross-Border Transfer Tools



ASEAN MCCs

- Created in context of ASEAN Framework on Digital Data Governance and ASEAN Framework on Personal Data Protection
- A voluntary tool to help ensure personal data transferred among and beyond the ASEAN Member States continues to benefit from a high level of data protection
- Designed as a “baseline” set of clauses for use in all AMS, whether or not a national data privacy law is extant
- Cover two types of data transfer:
 - Controller-to-controller
 - Controller-to-processor

RIPD MTA

- Created by the Ibero-American Data Protection Network
- A voluntary tool for use by the member nations of the RIPD, finalized in March 2023.
- Contain similar elements and principles to the EU SCCs, but are not a word for word reproduction of those clauses
- Cover two types of data transfer:
 - Controller-to-controller
 - Controller-to-processor

Other Regions – APAC / India

Also...

- South Korea, Japan, Singapore, and Indonesia all broadly impose an “adequacy” standard.
- India’s DPDP, while generally permissive of cross-border data transfers, empowers the Government to later “blacklist” specific jurisdictions as impermissible.



Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

The CBPR System: Overview

The Cross-Border Privacy Rules (CBPR) and Privacy Rules for Processors (PRP) systems are government-backed data privacy certifications that companies can join to demonstrate compliance with internationally-recognized data privacy protections.

- The framework originally began as an initiative of the Asia-Pacific Economic Cooperation (APEC) organization; on April 21, 2022, the APEC CBPR Member Economies announced the establishment of a “Global CBPR Forum” to expand the APEC CBPR outside of APEC.
- The system has requirements for member economies as well as potential recipients of CBPR Certification; fundamentally, it functions as a certification awarded to participating companies who pass a third-party audit of their privacy practices, permitting certified companies to carry out transfers among member economies without additional legal or administrative compliance requirements.
- Operationally, the system requires a recognized “accountability agent” to analyze an applicant’s compliance with 50 program requirements designed to facilitate 9 core principles.

The CBPR System: Overview

Member Countries:

Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States of America

- In July 2023, the UK joined as an “associate member.”

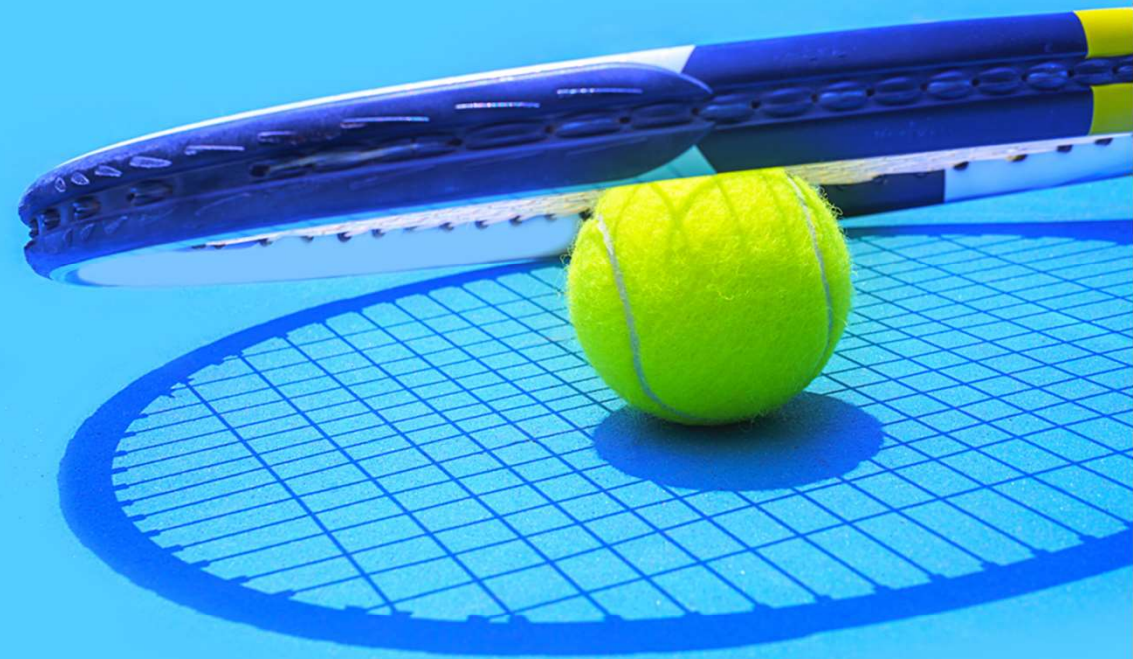
Example CBPR Requirements:

- Clear and easily accessible statements about privacy practices and policies.
- Disclosure of mechanism for filing complaints, access and correction requests.
- Notice of disclosure of collected information to third parties.
- Implementation of an information security policy (physical, technical, and administrative safeguards).
- Use of risk assessments and/or third party certifications.

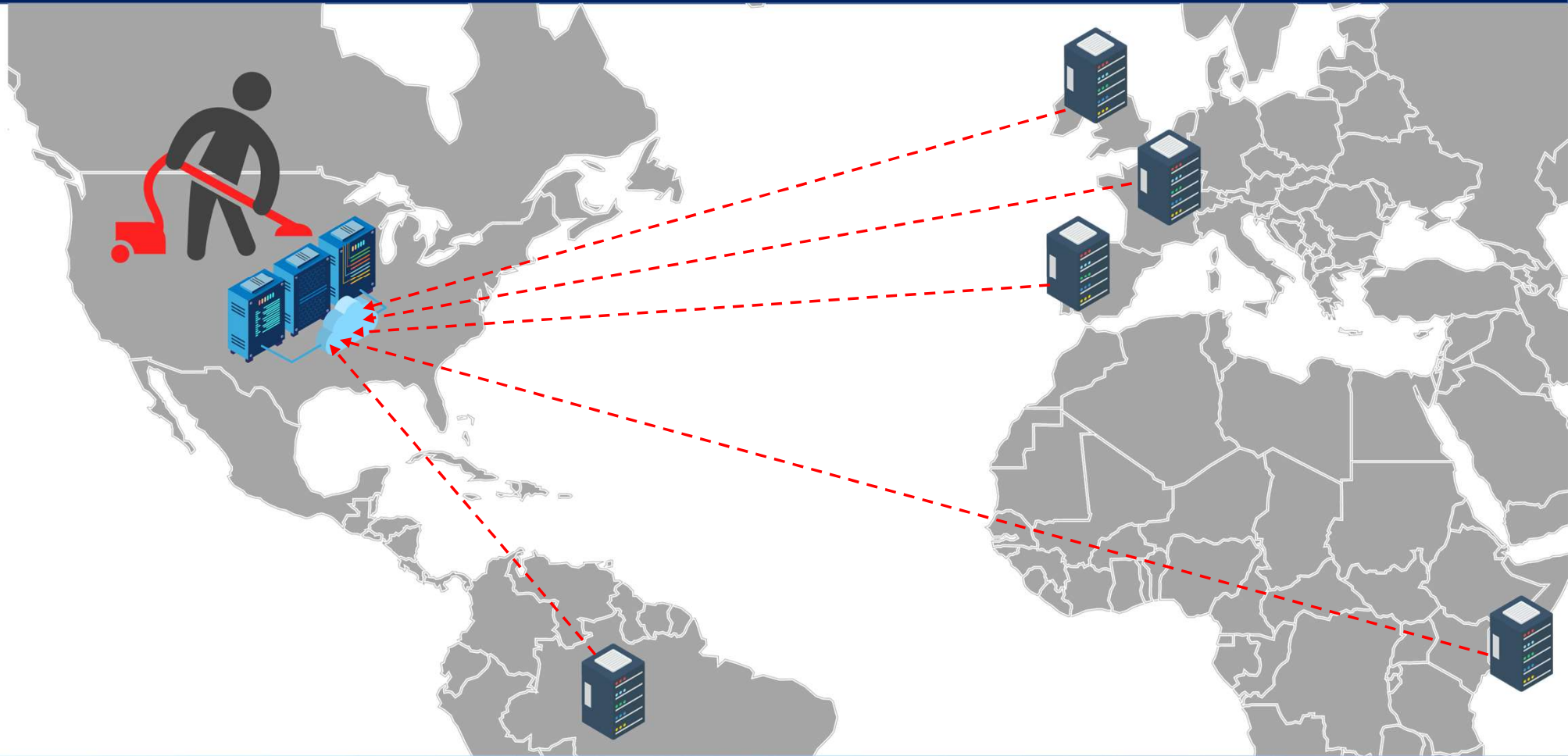
The CBPR System Process for Companies



Let's Play



Group Work



Cross-Border Data Transfer

Data Transfers from Europe / UK

Overview on SSCs

DPF and how to use it

Data Transfer Rules in other Regions

The CBPR System

Increasing Localization Requirements

Localization Requirements - XYZ

Source: <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/>

Learn more about countries
with data residency regulations

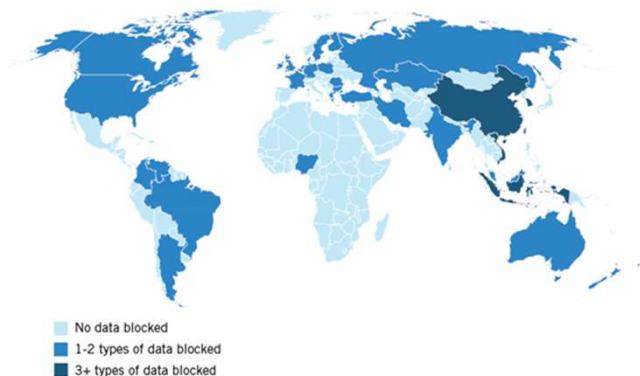
Health data regulations

- HEAVILY REGULATED
- REGULATED
- LIGHTLY REGULATED
- PENDING

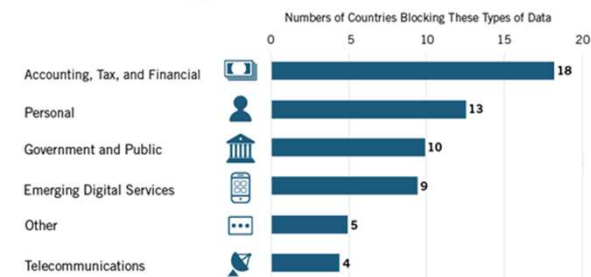
<https://incountry.com/blog/data-residency-laws-by-country-overview/>

Blocking the Global Flow of Data

Which Countries Block Data Flows?*



What Types of Data Are Blocked?*



*ITIF analysis of formal laws or regulations publicly reported as of April 2017.

Learn more at itif.org/databarriers

Localization Requirements - Variations

Universal Data Sovereignty

- Personal Data to be stored in the country

Partial Data Sovereignty

- Some Personal Data stored in the country (category, industry)

Data Replication

- Copy of Personal Data to be stored in the country

Controlled Localization

- Restrictions apply (mainly privacy)

Sprint to the Finish Line – Key Take Aways



See you !



Contacts



Allison Brody

Chief Privacy Officer
RELX

Allison.brody@relx.com



Lee Matheson

Senior Counsel
FPF

L.Matheson@fpf.org



Will Bracker

Senior Counsel
Cox Communications

Will.Bracker@cox.com

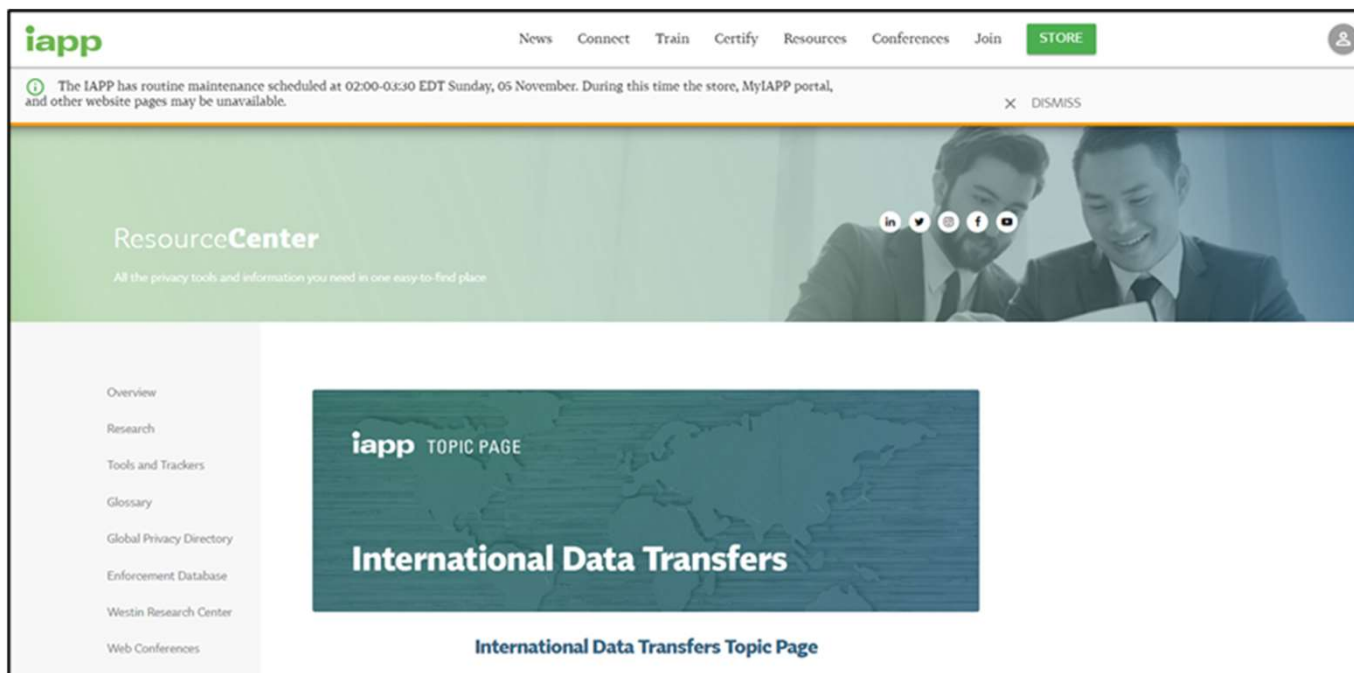


Kai Westerwelle

Partner
Bird & Bird

Kai.Westerwelle@twobirds.com

Resources – Further information



The screenshot shows the iapp ResourceCenter website. At the top, the iapp logo is on the left, and navigation links (News, Connect, Train, Certify, Resources, Conferences, Join) and a green STORE button are on the right. A maintenance notice banner is below the navigation. The main header features the text "ResourceCenter" and a sub-header "All the privacy tools and information you need in one easy-to-find place" over a background image of two men. A sidebar on the left lists various resources. The main content area displays a "TOPIC PAGE" for "International Data Transfers" with a world map background.

iapp

News Connect Train Certify Resources Conferences Join **STORE**

The IAPP has routine maintenance scheduled at 02:00-03:30 EDT Sunday, 05 November. During this time the store, MyIAPP portal, and other website pages may be unavailable. ✕ DISMISS

ResourceCenter

All the privacy tools and information you need in one easy-to-find place

- Overview
- Research
- Tools and Trackers
- Glossary
- Global Privacy Directory
- Enforcement Database
- Westin Research Center
- Web Conferences

iapp TOPIC PAGE

International Data Transfers

International Data Transfers Topic Page

Data Transfers from Europe / UK



GDPR – CHAPTER V: Transfers of personal data to third countries or international organizations

- Article 44: General principle for transfers
- Article 45: Transfers on the basis of an adequacy decision
- Article 46: Transfers subject to appropriate safeguards
- Article 47: Binding corporate rules
- Article 48: Transfers or disclosures not authorized by Union law
- Article 49: Derogations for specific situations
- Article 50: International cooperation for the protection of personal data

Article 44: General principle for transfers

“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. **All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.**”

Article 45: Transfers on the basis of adequacy



Recital 104: “ (...) The third country should offer guarantees ensuring an adequate level of protection **essentially equivalent to that ensured within the Union**, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States’ data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.”

Nations with adequacy:

Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, UK, Uruguay, and the United States (for members of the Data Privacy Framework).

Article 46: Appropriate Safeguards

To transfer data to a non-adequate country, **without DPA approval**, a transferor must rely on one of:

- a) legally binding and enforceable instrument between public authorities or bodies;
- b) Binding Corporate Rules (BCRs) adopted by the European Commission
- d) Standard Contract Clauses (SCCs) adopted by the EU Commission
- c) SCCs adopted by a DPA and approved by EU Commission
- e) A Code of Conduct recognized by the EU Commission
- f) A certification mechanism recognized by the EU Commission

Appropriate safeguards with prior authorization by a DPA:

- a) ad-hoc clauses
- b) administrative arrangements between public authorities

Article 49: Derogations for Specific Situations

Alternatively, **without adequacy OR one of the Article 46 methods**, a controller may still transfer data if:

- a) The controller has explicit consent, after data subject is informed of risks
- b) The transfer is necessary for the performance of a contract (data subject – controller)
- c) The transfer is necessary for the performance of a contract (controller – third party, but in the benefit of the data subject)
- d) The transfer serves important reasons of public interest
- e) The transfer is for establishment, exercise and defense of legal claims
- f) The transfer is for the vital interests if the data subject