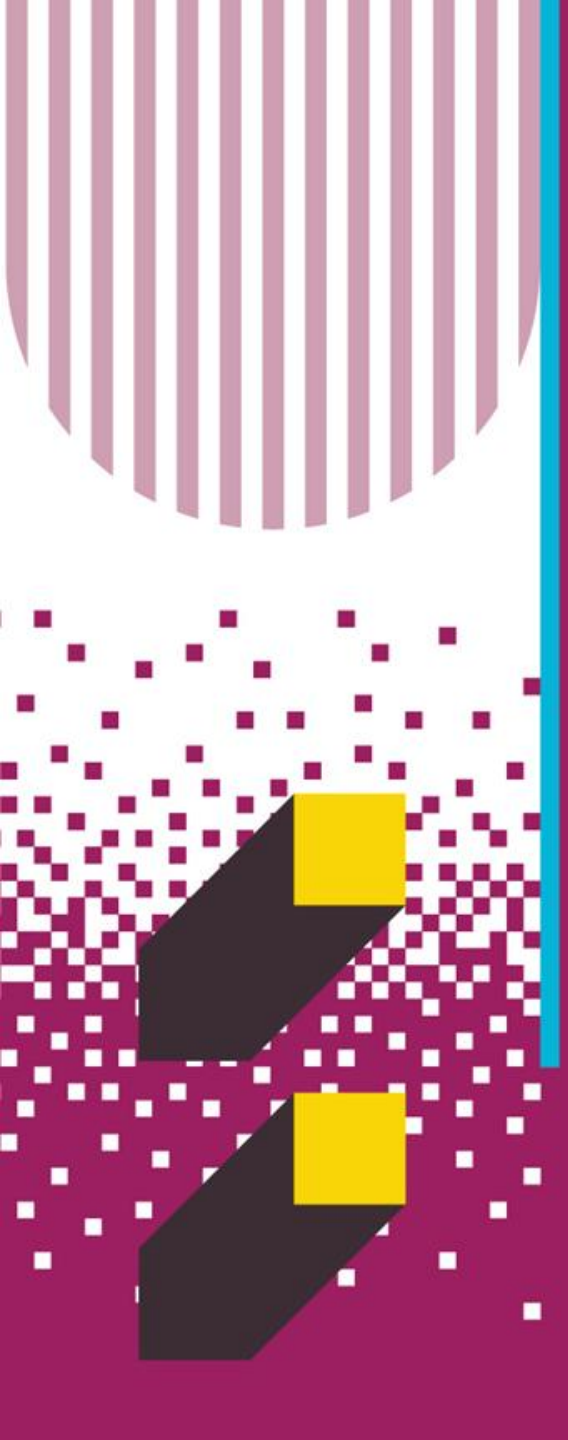

IAPP Canada Symposium 2026

Privacy | AI governance | Cybersecurity law

Conference 4-5 May
Workshops 6 May
Training 6-7 May
TORONTO

#IAPPSymposium26

How Does Privacy Facilitate Trade?

Global Cross-Border Transfers and AI

WELCOME AND INTRODUCTIONS

Helene Ammar
VP Enterprise Risk &
Global Privacy Officer

Zafin Labs

Laura Crestohl
Manager, Policy &
Research

Office of the Privacy
Commissioner of Canada

Constantine Karabliotis
Counsel

nNovation

Maciej Piszcz
Director, Privacy & AI
Governance

TrustArc

Canada's Moment: Privacy, Trade, and the Global Stage

Why This? Why Now?

Data flows are trade flows shifting trade relationships,

Privacy professionals are officially at the table

Context

Impacts of Proposed Regulations

Global CBPR
PIPEDA vs CBPR mapping
Role of he OPC

Frameworks

EU Adequacy & the AI Act

Adequacy opens the door

The AI Act raises the bar

EU Lens

The Playbook

The Hard Lessons
Making it work with
Actionable takeaways

Strategies

What is Global CBPR?

- Introduction
- Why is it important?
- Accountability-based certification mechanism
- Evolution
- Scalability

- 9 Principles
- 50 Program Requirements
- Updates effective April 1, 2027
- Member jurisdictions include: Canada, Mexico, U.S., South Korea, Singapore, Japan, Australia
- Associate members - the UK, Nigeria, Bermuda, Mauritius

Case for the Global CBPR

- Requirements negotiated by **multiple jurisdictions**.
- **Pragmatic** solution that builds on the existing laws.
- **Scalable framework** with universal requirements and scalable implementation
- **Annual review** by an Accountability Agent
- **Recognized** by several jurisdictions in their privacy laws
- **Facilitates** access to new markets
- Sends a **strong signal** to customers and business partners

Case for the Global CBPR

- Overlap
- OECD Principles
- PIPEDA
- Mapping

CBPR Principle	Corresponding PIPEDA Principle	PIPEDA Reference (Schedule 1)
Notice	Principle 8 – Openness	4.8
Collection Limitation	Principle 4 – Limiting Collection	4.4
Use of Personal Information	Principle 5 – Limiting Use, Disclosure, and Retention	4.5
Choice (Consent)	Principle 3 – Consent	4.3
Integrity of Personal Info	Principle 6 – Accuracy	4.6
Security Safeguards	Principle 7 – Safeguards	4.7
Access and Correction	Principle 9 – Individual Access	4.9
Accountability	Principle 1 – Accountability	4.1

The Role of the OPC

- Participating jurisdictions need a designated ***Privacy Enforcement Authority*** (PEA)
- PEAs can take enforcement actions against a certified organization for violations of the Global Systems
- ***Global CAPE*** facilitates enforcement cooperation amongst participating PEAs

Signatories to the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE) in Washington, April 2, 2024.

EU: Adequacy decision. What does it mean for companies? Other important laws?

- What is it?
  - Our privacy laws (PIPEDA) are deemed sufficient for data transfers
  - Renewed in January 2024
  - A significant advantage over countries like the U.S. in simplifying compliance
- How to leverage the adequacy decision?
  - Understanding controller versus processor
  - Documentation requirements
  - Contractual elements
- Why is it important for Canadian companies

What adequacy with the EU does NOT mean:

- It does **NOT** mean automatic GDPR compliance
- It **ONLY** refers to a mechanism for transferring personal data from EU to Canada
- It does **NOT** eliminate the need for a Data Protection Addendum (DPA)
- It **ONLY** applies to commercial activities under federal jurisdiction

EU AI Act: What does it mean for Canadian companies?

- What is it?
- How companies can build their governance framework around the Act
- Why is it important for Canadian companies (Vendor AI usage vs internal AI
- Continuous data flows
- Explainability expectations

- Introduced in 2024
- Sets out a risk-based rules for AI developers and deployers
- Imposes significant penalties
- Includes rules for the General Purpose AI-Models

OPC Perspective

Recognizing that cross-border data flows are critical in an increasingly globalized world, the OPC has:

- **Released guidelines for processing personal information across borders** that sets out accountability and transparency requirements and best practices for companies
- **Recommended that PIPEDA be amended** to explicitly address cross-border data flows
- **Sought opportunities for interoperability with international counterparts** through participation in international fora and examination of data transfer mechanisms

Why Cross Border Programs Fail in Practice

You can't see it

Risk lives in the subprocessor chain, not the vendors you've documented

You can't rely on it

Transfer mechanisms are fragile
Stability is an assumption, not a guarantee

You can't defend it

Compliance on paper is not enough A signed SCC without a real TIA is difficult to defend.

Canadian organizations face pressure from every direction:

- EU adequacy
- US executive orders
- Localization mandates
- Shifting obligations under PIPEDA and Quebec's Law 25.

Can your program adapt?

Assumptions that Break Programs

Our SCCs are signed, we're covered

Without a TIA, a signed SCC is not a complete safeguard

The DPF is stable enough to build on

An active legal challenge is pending. Few organizations have fallbacks ready to deploy

We know where our data goes

The exposure lives in the subprocessor chain, not the vendors we've documented

Localization solves the problem

Geography doesn't solve access.
Data can be compelled regardless of where it's stored

If you had to defend your transfer decisions tomorrow, would your assumptions hold up?

Compliance to Resilience Strategies

Design for Transfers Early

Address transfer risk at the design, architecture, and procurement levels

Not at contract signing

Build Layered Mechanisms

Don’t rely on a single transfer mechanism

Combine SCCs, contractual controls, and governance with fallbacks that are pre-approved and ready

Vendor Oversight is Intelligence

Your greatest exposure is often your vendor’s architecture

Assess sub-processors

Not just direct vendors

Strategies for navigating cross-border data transfers

- Design for transfers early
- Build layered transfer mechanisms (resilience) + Importance of the Global CBPR in the transfer strategy
- Treat TIAs as a risk exercise, not just a legal one
- Vendor ecosystem governance
- Stress-test the transfer architecture (e.g. vendor exit, regulatory shift, framework invalidation)

For Canadian business, implementation typically requires:

- Gap analysis between current practices and GDPR requirements
- Documentation of policies and processes
- Individual rights procedures (including "right to be forgotten")
- Breach response protocols (72-hour notification timeline)
- Vendor management program
- Onward transfer protections

“Gotchas”

- Sign and forget SCC Trap (can we defend assumptions behind the TIA)
- Over reliance on “stable” mechanisms (DPF / adequacy)
- Data mapping illusion (3rd 4th party blind spots)
- Thinking localization solves the problem (even when data is localized, access isn’t)Not stress testing transfer architecture (contingency for DPF invalidation, vendor changes, etc.)

- **For Canadian business, implementation typically requires:**
  - Gap analysis between current practices and GDPR requirements
  - Documentation of policies and processes
  - Individual rights procedures (including "right to be forgotten")
  - Breach response protocols (72-hour notification timeline)
  - Vendor management program
  - Onward transfer protections

Privacy as a Trade Facilitator

Privacy Enables Global Trade

- Reduces friction in sales and vendor onboarding
- Builds trust in entering new markets Across geographies and industries
- Enables scalable cross-border operations

From Compliance To Continuity

- Cross-border readiness prevents operational disruption
- Supports resilience in changing regulatory environments
- Enables defensible decision-making under pressure

How do privacy professionals facilitate trade?

- Business continuity
- Navigating laws and enabling trade
- Vendor management
- Data localization, trade barriers, and other considerations

Proactive demonstration of compliance:

- Builds trust with EU/CBPR partners
- Reduces legal due diligence burden
- Shortens contract negotiation time
- Differentiates from competitors
- Reduces time to closing the deal

Call to Action!

- Get a handle on data governance:
  - Conduct a baseline assessment of your current privacy practices
  - Identify your trade opportunities and data flows
  - Develop a structured implementation roadmap
  - Prepare documentation to demonstrate compliance
  - Identify your technical, organizational and administrative controls over data
  - Proactively address privacy with clients in your business development processes

- This is a call to action, to invoke action – instigate new opportunities for ourselves, our organizations and our country

RESOURCE LIST

- OPC *Guidelines for processing personal data across borders*

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Symposium 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!