Skadden

The Next Digital Trade Framework: What an EU-CPTPP Agreement Signals for Data, Cyber and AI Governance

June 15, 2026

Skadden Publication
Brooks E. Allen David A. Simon Michael Albrecht vom Kolke Nicola Kerr-Shaw Cynthia C. Galvez Michael Tian

Executive Summary

- **What's new:** The EU and CPTPP countries have agreed to accelerate work toward a digital trade agreement covering e-commerce, cross-border data flows and data localization for a combined economy of $35 trillion and 1.6 billion people.
- **Why it matters:** For multinationals operating across the EU and Asia Pacific markets, the initiative signals a shift toward a multibloc digital governance environment, with implications for data transfer architectures, cloud strategies, AI deployment and cybersecurity compliance.
- **What to do next:** Companies should consider monitoring developments and prepare for a potential shift in the regulatory architecture governing cross-border data, AI and cybersecurity, including by mapping data transfer mechanisms, assessing cloud strategies and elevating digital trade risk to board level.

Key Points

- On March 27, 2026, at the 14th WTO Ministerial Conference in Yaoundé, Cameroon, the EU and CPTPP countries agreed to accelerate work toward a digital trade agreement covering e-commerce, cross-border data flows and data localization for a combined economy of $35 trillion and 1.6 billion people.
- The EU has already concluded digital trade deals with several CPTPP members, including Chile, Japan, New Zealand, Singapore and the U.K., providing a road map for a broader agreement.
- Key differences between the two parties' existing approaches to digital trade will be central to negotiations, including the treatment of personal data as a "policy objective" in the CPTPP versus a "fundamental right" in the EU, the breadth of security exceptions, and the scope of financial services data rules.
- For multinationals operating across the EU and the Asia Pacific markets, the recent initiative signals a shift toward a multibloc digital governance environment, with implications for data transfer architectures, cloud strategies, AI deployment and cybersecurity compliance.

What Has Been Agreed (and What Is to Come)

On March 27, 2026, ministers and representatives of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the European Union released a Joint Ministerial Statement (the Joint Statement) on the sidelines of the 14th World Trade Organization (WTO) Ministerial Conference (MC14) in Yaoundé, Cameroon. The parties committed to cooperating on trade diversification, supply chain resilience, digital trade and the global trading environment, and instructed senior officials to develop work plans.

The Joint Statement is a commitment at the level of a memorandum of understanding (MOU) and does not contain any binding language. Nevertheless, the statement signals the parties' intent to establish an EU-CPTPP digital trade agreement that would set common rules on e-commerce, data flows, and data storage. Canada's minister of international trade characterized the prospective agreement as potentially "the largest trading agreement in civilization."

The broader context makes the timing notable. MC14 ran nearly two days past its scheduled close, failing to finalize key texts on WTO reform and fisheries subsidies. Most significantly, WTO members failed to renew the Moratorium on Customs Duties on Electronic Transmissions, a longstanding agreement first adopted in 1998 that bans customs duties on digital downloads, streaming and other electronic transmissions. Sixty-six WTO members subsequently agreed to put the moratorium into effect on an interim basis outside the WTO framework, reflecting a shift

toward coalition-based rulemaking when multilateral consensus proves elusive. Against this backdrop, the EU-CPTPP initiative represents a broader exercise in coalition-building aimed at preserving rules-based trade amid a fragmented WTO.

Likely Scope: Data Flows, Localization, Source Code and AI

The existing treaty texts of the CPTPP and the EU's five trade agreements that contain digital trade provisions — the EU-Singapore Digital Trade Agreement (EU-Singapore DTA), EU-Japan Economic Partnership Agreement (EU-Japan EPA), EU-New Zealand Free Trade Agreement (EU-New Zealand FTA), EU-Chile Advanced Framework Agreement (EU-Chile AFA) and EU-UK Trade and Cooperation Agreement (EU-UK TCA) — provide a picture of the likely contours of a combined framework.

Cross-Border Data Flows and Localization Bans

The CPTPP and the EU bilateral instruments start from the same premise: Digital trade rules should limit parties from using data localization requirements as a condition of doing business.

The CPTPP does this through two principal commitments in Chapter 14 (Electronic Commerce). Article 14.11 requires parties to allow cross-border transfers of information, including personal information, by electronic means when the activity is for the conduct of a covered person's business, and Article 14.13 separately prohibits a party from requiring a covered person to use or locate computing facilities (such as servers, data centers and related network elements) in its territory as a condition for conducting business.

Parties are permitted to derogate from these obligations for legitimate public policy reasons, provided the measure is not applied in an arbitrary or discriminatory way, is not a disguised restriction on trade and is not more restrictive than necessary. As discussed below, these obligations are also subject to an "essential security" exception and other general exceptions. Importantly, both obligations apply only to "covered persons," a category defined in Article 14.1 that does not include "financial institutions" as defined in the CPTPP's separate Chapter 11 (Financial Services). The CPTPP therefore does not categorically prohibit cross-border data flow restrictions or localization measures applied to financial institutions through Chapter 14; data-related obligations for financial institutions are instead addressed through Chapter 11, which is discussed below.

By contrast, the EU bilateral agreements are more specific about the forms of localization, and the forms of cross-border data transfer restrictions, that they prohibit. For example, the EU-UK TCA, EU-New Zealand FTA and EU-Chile AFA each prohibit four specific categories of restrictions on covered cross-border data flows — *i.e.*, measures that:

- Require the use of local computing facilities or network elements (such as in-territory servers, data centers or similar infrastructure) for data processing.
- Require the localization of data (*i.e.*, requirements that data be stored or processed within the party's territory).
- Prohibit the storage or processing of data in the other party's territory.
- Make the cross-border transfer of data contingent on the use of local computing facilities or compliance with data localization requirements.

The protocol amending the EU-Japan EPA (the Protocol) extends that list by also prohibiting measures that block transfers of information into a party's territory or require a party's prior approval for cross-border transfers of information.

The EU instruments preserve regulatory space somewhat differently from the CPTPP framework. The EU-UK TCA preserves data protection transfer mechanisms of general application; the EU-New Zealand FTA preserves personal data and privacy protections and includes agreement-specific scope exclusions, including for information held or processed by or on behalf of a party and specified Māori-related measures; and the EU-Chile AFA incorporates general, security and prudential exceptions into the digital trade chapter. The EU-Japan Protocol (Protocol) adds an objectively interpreted legitimate public policy exception, preserves personal data transfer instruments of general application and excludes information held or processed by or on behalf of a party.

Financial Services Data

Under the CPTPP, "financial institutions" is a separately defined term that is excluded from the "covered person" definition in Article 14.1, so the digital trade chapter's cross-border data transfer and localization commitments (Articles 14.11 and 14.13) do not apply to them as such. Data-related obligations for financial institutions are instead governed by the CPTPP's separate financial services chapter (Chapter 11), which is structured around prudential supervision and contains its own, more limited data-transfer disciplines. As a result, CPTPP parties retain broader latitude to impose data localization or transfer requirements on financial institutions for prudential or supervisory reasons than they do for nonfinancial covered persons under Chapter

14. The scope of any combined EU-CPTPP framework with respect to noninstitution financial-services suppliers will be an important point to monitor.

The EU agreements include a mixture of cross-sectoral and financial-services-specific rules:

- The EU-Singapore Free Trade Agreement (EU-Singapore FTA), which provides the foundation for the EU-Singapore DTA, contains a financial-services-specific rule requiring each party, subject to privacy and confidentiality safeguards, to permit a financial service supplier of the other party to transfer information into and out of its territory for data processing where required in the ordinary course of business.
- The EU-Japan EPA originally included a similar financial-services-specific transfer rule, but the Protocol deletes that provision and instead applies a horizontal cross-border transfer rule to financial-services suppliers, while preserving prudential, privacy and other exceptions.
- The EU-Chile AFA takes a hybrid approach: It brings the provision and transfer of financial information, and financial data processing and related software, within the scope of its cross-border supply of financial services discipline, thereby prohibiting market access and national treatment restrictions on those activities subject to the agreement's prudential carve-out and confidentiality protections.

Negotiations in this area are likely to focus on whether the digital trade chapter of any combined EU-CPTPP framework will apply to financial services at all (as the EU agreements generally do, in varying ways) or carve them out (as the CPTPP does for "financial institutions"). If the digital trade chapter does apply to financial services, will the resulting rules be the cross-sectoral cross-border data flow and data localization disciplines (subject to prudential and confidentiality safeguards) or a separate set of financial-services-specific transfer provisions? The final landing zone could have significant practical consequences for banks, insurers, asset managers and fintech firms operating across the two blocs.

Source Code and Algorithm Protection

Both the CPTPP and EU agreements prohibit governments from requiring the transfer of, or access to, software source code as a condition for market entry. The CPTPP's protection covers mass-market software but excludes critical infrastructure. The EU-Japan EPA, EU-New Zealand FTA, EU-Chile AFA and EU-U.K. TCA each include comparable prohibitions, although with varying exceptions for court orders, competition law, intellectual property enforcement and public procurement.

Notably, the EU-Singapore DTA goes the furthest, extending source code protections to algorithms and machine-learning models. The DTA provides certain exceptions to these protections to preserve access or disclosure authority for specified functions — such as investigations, inspections, enforcement actions, judicial proceedings, competition-law remedies, intellectual property enforcement and public procurement — generally subject to safeguards against unauthorized disclosure. As AI-driven business models proliferate, the question of whether forced disclosure requirements extend to algorithms, training data and model weights becomes increasingly consequential. The EU-Singapore approach may serve as a useful template for any combined framework.

Customs Duties on Electronic Transmissions

Both the CPTPP and all five EU bilateral agreements permanently ban customs duties on electronic transmissions. This is the strongest area of convergence, and its significance has been amplified by the lapse of the WTO e-commerce moratorium at MC14. Embedding a permanent ban in an EU-CPTPP agreement would provide a stable floor for digital commerce as the multilateral consensus frays.

Points of Divergence: Privacy, Security Exceptions and Regulatory Frameworks

While there is substantial convergence on digital trade prohibitions and protections, the two models diverge on the conditions under which parties can restrict data flows and on the hierarchy of values that governs derogation. Resolving these differences will be important for any future EU-CPTPP agreement.

Privacy: ‘Policy Objective’ vs. ‘Fundamental Right’

The CPTPP requires parties to maintain a legal framework for the protection of personal information but accords the parties considerable flexibility in how they do so. For instance, CPTPP parties may satisfy the requirement through comprehensive national laws, sector-specific laws or even voluntary enterprise undertakings. When invoked to justify restrictions on data flows, privacy is treated as a “legitimate public policy objective” that must pass a trade-law necessity test. This means that the measure must not be arbitrary, must not be a disguised restriction on trade and must not be more restrictive than necessary.

The EU's bilateral agreements take a different approach. The EU-New Zealand FTA, EU-U.K. TCA, EU-Chile AFA and EU-Singapore DTA each recognize the protection of personal data and privacy as a "fundamental right." The EU-Singapore DTA expressly preserves each party's right to adopt measures for the cross-border transfer of personal data, provided its law includes instruments enabling transfers under conditions of general application. This effectively carves out General Data Protection Regulation (GDPR) adequacy decisions, standard contractual clauses and similar mechanisms. By elevating privacy to the status of a fundamental right, these agreements aim to place privacy measures beyond the reach of trade proportionality tests, a qualitative difference from the CPTPP model.

The EU-Japan Protocol, which is an amendment to the EU-Japan EPA, represents the most pragmatic attempt to bridge this divide. The Protocol recognizes each party's right to determine the appropriate level of protection for personal data and privacy; encourages adoption of high standards, including those outlined by the Organisation for Economic Co-operation and Development (OECD); and preserves each party's right to maintain its own cross-border transfer instruments. This concept, sometimes described as "Data Free Flow With Trust" (DFFT), accepts CPTPP-style localization bans while carving out space for EU-style data protection instruments such as adequacy decisions and standard contractual clauses. It may represent the most likely template for a combined framework.

Existing cross-border enforcement infrastructure could also play a role. The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Enforcement Arrangement (CPEA), a voluntary cooperation framework among privacy enforcement authorities across APEC economies, facilitates information sharing and enforcement referrals among several CPTPP members. While the CPEA does not create binding obligations, its operational infrastructure could also provide a practical foundation for interoperability between APEC and EU privacy enforcement mechanisms.

The Security Exception

The CPTPP's digital trade obligations are subject to the general and security exceptions set out in Chapter 29. This chapter provides an "essential security" exception that allows a party to take any measures that "it considers necessary" for the protection of its essential security interests. This language could be construed as self-judging, in which case the invoking party itself would determine whether the exception applies.

By contrast, the EU's bilateral agreements include security exceptions, but they are framed in language that echoes Article XXI of the General Agreement on Tariffs and Trade (GATT). GATT

Article XXI uses the “it considers necessary” formulation but ties it to enumerated categories: fissionable materials, arms and military supply, measures taken in time of war or other emergency in international relations, and actions under the United Nations Charter. The EU-Japan EPA, EU-Singapore FTA and EU-Chile AFA largely follow this architecture: The self-judging phrase is present but is tethered to defined security categories.

WTO panels have been willing to review the applicability of certain aspects of Article XXI to specific facts. For instance, panels have in some cases been willing to assess whether the challenged measure falls within the treaty’s listed categories and whether it has been invoked in good faith, rejecting the U.S. position that Article XXI is entirely self-judging.[1] Indeed, in recent disputes, panels have declined to accept the invocation of Article XXI where these elements were not satisfied.[2] Thus, for purposes of an EU treaty, the invocation of a security exception may be difficult to overcome, but it is not entirely immune from scrutiny by a dispute settlement panel.

Given recent WTO panel disputes and wider disagreements with the U.S. over the use (and perceived abuse) of security exceptions to depart from trade commitments, EU negotiators may be reluctant to adopt the CPTPP’s broader self-judging exception. Indeed, although the U.S. ultimately withdrew from what was originally labeled the Trans-Pacific Partnership (TPP), it drove much of the negotiations and provisions that carried into the CPTPP, such as the essential security clause, reflect U.S. drafting preferences. With the U.S. no longer a party to the agreement, there may be greater openness among the remaining CPTPP members to adopt the EU’s narrower approach.

Binding Commitments vs. Aspirational Norms

A further open question is whether an agreement would translate into binding changes in domestic laws and regulations or remain a set of principles and norms. Whether there is appetite for that level of commitment, backed by dispute settlement provisions, or whether the agreement will be more aspirational are some of the most important strategic questions for a possible EU-CPTPP agreement.

Cybersecurity

The CPTPP takes a cooperative approach to cybersecurity, recognizing the importance of building national incident response capabilities and cooperating on malicious intrusions. These are best-efforts commitments, not prescriptive requirements.

In contrast, the EU's approach is more concrete. Specifically, the EU-Singapore DTA commits the parties to risk-based cybersecurity approaches and consensus-based standards, and the accompanying EU-Singapore Digital Partnership commits to mutual recognition arrangements for cybersecurity certifications where compatible approaches exist on both sides. The EU's domestic regime, including the Network and Information Security Directive (NIS2) and the Cybersecurity Act, imposes incident reporting and operational resilience standards that go beyond the CPTPP's cooperative model.

A potential path is mutual recognition rather than harmonization. The EU-Singapore model proceeds in three steps:

- First, it sets a common baseline through digital trade commitments.
- Second, it preserves each side's domestic regulatory autonomy.
- Third, it uses the Digital Partnership to pursue mutual recognition of compatible standards, including cybersecurity certifications, through future workstreams..

What Companies Should Consider Now

For multinationals with operations spanning the EU and the Asia Pacific regions, the recently announced initiative is a signal to begin monitoring developments and preparing for a potential shift in the regulatory architecture governing cross-border data, AI and cybersecurity. Companies should consider taking the following steps:

- **Map cross-border data transfer mechanisms.** Companies will want to assess whether their current data transfer architectures are positioned to operate under both CPTPP and EU frameworks, or if a combined framework might create new interoperability challenges.
- **Assess cloud and data center strategies.** Companies will want to evaluate whether existing cloud architectures can take advantage of any broader harmonization of localization bans and note existing sectoral differences between the CPTPP and the EU agreements. In the financial sector, banks, insurers and fintech companies should therefore track whether any combined framework brings financial data under the localization ban by default or leaves it governed primarily by financial-services exceptions.
- **Integrate AI governance with trade restrictions.** Emerging protections for algorithms and machine-learning models in the EU agreements signal that AI deployment strategies will increasingly be shaped by trade rules, not just domestic regulation. Companies developing or

deploying AI across jurisdictions should monitor whether source code protections extend to training data, model weights or other components of the AI stack.

- **Evaluate cybersecurity posture.** Companies will want to assess their incident reporting posture against the standards emerging from both frameworks, given the EU's NIS2 requirements and the possibility of mutual recognition of cybersecurity certifications.
- **Elevate "digital trade risk" to the board level.** As digital trade frameworks evolve, the strategic implications for market access, data infrastructure investments and regulatory compliance merit attention at the board level, not just within compliance functions.

What We're Watching

The EU-CPTPP Joint Ministerial Statement instructed senior officials to develop work plans and prepare a progress report for their next meeting. Several developments will shape whether this initiative gains momentum.

- **Timeline and form.** A critical question is whether the parties will pursue a binding agreement backed by dispute settlement provisions, or a softer framework of principles and norms.
- **WTO e-commerce moratorium.** The 66-member interim arrangement preserving the moratorium on customs duties is a stopgap. If it cannot be restored through the WTO, embedding a permanent ban in an EU-CPTPP agreement could become even more strategically significant.
- **U.S. position.** The U.S. is not a CPTPP member, having withdrawn from the original TPP in 2017. Even so, an EU-CPTPP agreement could affect U.S. companies because it may set the operating baseline for data transfers, localization, AI-related disclosures and cybersecurity across markets where many U.S. multinationals sell, host data or rely on regional supply chains. If those standards diverge from U.S. policy, companies may need to build compliance programs around an EU-CPTPP rule set even without U.S. participation.
- **Broader geopolitical dynamics.** The EU-CPTPP initiative is part of a wider pattern in which trade partners are using regional and bilateral frameworks to fill gaps left by WTO gridlock. For the EU, recent efforts to conclude or advance major trade agreements with Australia, India, Indonesia and Mercosur point in the same direction: building issue-specific coalitions that can set practical rules for market access, resilience and digital governance even when multilateral rules lag.

As the preceding reflects, digital trade governance is no longer a single-jurisdiction compliance exercise. It is a multibloc strategic challenge that touches on data infrastructure, AI governance, cybersecurity and enterprise risk. Companies should continue to monitor developments in this space, including with respect to the EU-CPTPP dialogue, and ensure that they are able to adapt to this rapidly changing environment.

---

1 See, *e.g.*, Panel Report, United States – Origin Marking Requirement, WT/DS597/10 (Dec. 21, 2022); Panel Report, United States – Certain Measures on Steel and Aluminum, WT/DS544/14 (Dec. 9, 2022); Products, Press Release, U.S. Trade Representative [USTR], Statement from USTR spokesperson Adam Hodge (Dec. 21, 2022) ("The United States has held the clear and unequivocal position, for over 70 years, that issues of national security cannot be reviewed in WTO dispute settlement, and the WTO has no authority to second-guess the ability of a WTO Member to respond to what it considers a threat to its security.")

2 See, *e.g.*, Panel Report, Russia – Measures Concerning Traffic in Transit, WT/DS512/R (April 5, 2019).

Related Capabilities

Artificial Intelligence // Asia Pacific // Corporate Governance // Cybersecurity and Data Privacy // Europe // Intellectual Property and Technology // International Trade // National Security