Centre for Information Policy Leadership
HUNTON

GLOBAL CBPR & GLOBAL PRP SYSTEMS

PLAYBOOK

An Actionable Guide for Participation in the

Global Cross-Border Privacy Rules and the

Global Privacy Recognition for Processors

June 2026 | Version 2.0

Contents

EXECUTIVE SUMMARY

Cross-border data flows drive today's global economy, yet companies seeking to transfer data across borders are faced with varying and complex requirements from different jurisdictions. The **Global Cross-Border Privacy Rules (Global CBPR)** provide private-sector data controllers with a streamlined, yet flexible, accountability-based solution that satisfies the requirements of participating jurisdictions. It is based on formal third-party assessments affirming that certified organizations adhere to a common set of approved standards. The **Global Privacy Recognition for Processors (Global PRP)** provide analogous certifications for private sector organizations operating as data processors.

Significantly, the Global CBPR and Global PRP are not self-regulatory best practices—they are **certified compliance programs** enforceable by the participating jurisdictions' relevant enforcement authorities. Global CBPR and Global PRP certifications ensure that organizations have implemented practical measures, called "Program Requirements," that fulfill overarching data protection and privacy principles.

The Global CBPR and Global PRP are purely **voluntary** and are able to **co-exist alongside other transfer and due diligence mechanisms**. Organizations thus continue to have the option to rely on adequacy decisions, standard contractual clauses, binding corporate rules, and other transfer mechanisms as needed.

If an organization chooses to seek certification under the Global CBPR or Global PRP, it starts with a self-assessment of its data protection and privacy policies and practices against the applicable Program Requirements. The organization then presents that assessment to an approved third-party certification body, known as an **Accountability Agent**, that independently assesses whether the organization satisfies the Program Requirements and, where necessary, assists the organization in meeting those requirements.

However, before an organization can seek certification, the jurisdiction in which the organization is principally located must become a Member of the **Global CBPR Forum**—a group of jurisdictions that have agreed to operationalize the Global CBPR and Global PRP Systems. Jurisdictions not yet ready to operationalize the Systems may participate in the Forum as "Associates," allowing them to learn more about the Global CBPR and Global PRP Systems and receive assistance as they prepare for full membership.

Participation in the Global CBPR and Global PRP Systems conveys benefits not only for jurisdictions, privacy enforcement authorities, and businesses, but also for the individuals whose personal data is protected.

For jurisdictions, participation **enables trusted data flows with other jurisdictions**, thereby boosting the economy, enabling data-driven innovation, and attracting business for local industry, particularly in the data processing context. Moreover, the Global CBPR and Global PRP Systems enable more streamlined and efficient data protection and privacy investigations and enforcement actions, providing added benefits to local and/or national enforcement authorities.

For businesses, Global CBPR and Global PRP certifications **help facilitate compliance** with data protection and privacy laws in participating jurisdictions and can serve as a trustmark for the transfer of personal data. The process of certification can be particularly helpful for SMEs that may lack the expertise, staff, or resources to devise their own comprehensive data protection and privacy

programs. They can also serve as due diligence and risk management tools for companies seeking qualified third-party vendors, processors, and business partners.

For individual consumers, the Global CBPR and Global PRP Systems ensure that companies have effective—i.e., stronger—data protection and privacy programs in place, providing **more robust and reliable privacy protections for consumers**. Moreover, the Global CBPR and Global PRP Systems provide complaint and dispute resolution mechanisms for consumers that might otherwise not be available.

Participation by jurisdictions forms the foundation of the Global CBPR and Global PRP Systems. Their participation demonstrates that their data protection and privacy frameworks are aligned with the Program Requirements of the Global CBPR and Global PRP Systems, facilitating interoperability. This gives businesses the assurance that their Global CBPR or Global PRP certifications will facilitate seamless transfer of personal data across participating jurisdictions.

Jurisdictions and organizations interested in learning more may review this Playbook and consult the **Global CBPR Forum website** (https://www.globalcbpr.org/) for additional information.

GLOBAL CBPR & GLOBAL PRP SYSTEMS AT A GLANCE

The **GLOBAL CBPR AND GLOBAL PRP SYSTEMS** are **certified compliance programs** that facilitate trusted personal information flows from and between participating **jurisdictions** and **organizations**.

Certifications ensure that organizations have implemented practical measures — called **PROGRAM REQUIREMENTS** — that fulfill overarching data protection and privacy principles.

The **GLOBAL CBPR FORUM** is a group of **jurisdictions** with administrative, operational, and oversight functions with respect to the **Global CBPR and Global PRP Systems**.

Participation by JURISDICTIONS forms the foundation of the Global CBPR and Global PRP Systems. Jurisdictions may apply for Forum membership by accepting the principles and objectives of the **Global CBPR Declaration and Framework** and demonstrating how their domestic legal system enables enforcement of the **Program Requirements** or recognize the Systems under their domestic legal system.

Domestic laws and regulations provide participating jurisdictions with the **legal basis for enforcing** the Systems. A participating jurisdiction must have at least one **PRIVACY ENFORCEMENT AUTHORITY** (PEA), a public body responsible for enforcing the data protection and privacy laws of that jurisdiction. The PEA, in turn, joins the Global Cooperation Arrangement for Privacy Enforcement (**Global CAPE**), which facilitates enforcement cooperation among PEAs.

A participating jurisdiction must identify, and the Forum must recognize, a **third-party certification body** — known as an **ACCOUNTABILITY AGENT** — which assesses whether an applicant organization may be certified as satisfying the **Program Requirements** of the Global CBPR or Global PRP Systems.

An **ORGANIZATION** "primarily located" in a participating jurisdiction may seek certification from an **Accountability Agent** recognized in that jurisdiction, starting with a **self-assessment** of its policies and practices against the applicable **Program Requirements**. The Accountability Agent evaluates the self-assessment and assists the company to come into compliance. Certifications are subject to annual attestation and re-certification.

The Global CBPR and Global PRP Systems provide **complaint and dispute resolution** mechanisms for **CONSUMERS** that might otherwise not be available.

I. THE NEED FOR A MULTILATERAL DATA TRANSFER SOLUTION

A. Data Flows are Essential to the Global Marketplace

Cross-border data flows drive today's global economy and facilitate business growth. The free flow of data allows companies to access the best technology and the best services at the best prices, irrespective of where they are located. Transformative technologies demand vast amounts of electronic data to flow seamlessly across jurisdictions. The ability to use, share, and access information across borders stimulates innovation, enables data-driven products and services, and fuels economic growth and ideas. It fosters competition by allowing new entrants access not only to data, but also to new markets and customers. It benefits individuals by enabling their access to services and products across the globe. Indeed, the explosive growth of generative AI has put in sharp focus the need for trusted data flows, as data powers the development and deployment of AI technologies.

WHY GLOBAL CBPR & GLOBAL PRP?

- ⇨ To create a multilateral solution for data transfers
- ⇨ To build a trusted network of participating jurisdictions and businesses
- ⇨ To supplement existing data transfer mechanisms

B. Data Flows Have Become Globally Complex

Data protection and privacy laws continue to proliferate around the globe, often with different and sometimes conflicting standards, leading to a range of data transfer mechanisms authorized by different laws. This has resulted in increasing complexity and substantial compliance challenges for organizations with multinational or global business operations.

The types of transfer mechanisms include (1) standard and model contractual clauses; (2) certifications; (3) codes of conduct; (4) binding corporate rules; (5) adequacy decisions; (6) bilateral frameworks; (7) regional agreements; and (8) derogations. Each method has its own advantages and shortcomings, but significantly, each differs in scope and application from jurisdiction to jurisdiction. Legal challenges and conflicting interpretations of various methods have added unpredictability and legal uncertainty to the mix. Given these variables, companies seeking to transfer data across borders must assess each option's requirements, jurisdictional nuances, and likely robustness before deciding which mechanism may be most appropriate for a given transfer. Additionally, some jurisdictions require organizations to conduct country-specific transfer risk assessments, adding another layer of complexity and administrative burden on organizations. With so many considerations at play, the decision-making process is oftentimes done on a transaction-by-transaction and jurisdiction-by-jurisdiction basis, which can consume a great deal of time and human resources for organizations.

C. Global CBPR & Global PRP Provide a Multilateral Solution

A streamlined, yet flexible, accountability-based solution that applies across jurisdictions is sorely needed.

That's where Global Cross-Border Privacy Rules (Global CBPR) and the Global Privacy Recognition for Processors (Global PRP) come in. The Global CBPR help data controllers implement data protection and privacy practices aligned with a set of standards, called "**Program Requirements**," endorsed by multiple jurisdictions. The Global Privacy Recognition for Processors (Global PRP) provides analogous certifications for organizations operating as data processors.

CHARACTERISTICS OF GLOBAL CBPR & GLOBAL PRP

- ⇨ Voluntary
- ⇨ Enforceable
- ⇨ Flexible
- ⇨ Multilateral
- ⇨ Accountability-based
- ⇨ Co-exists with other transfer mechanisms

Organizations may certify any number of subsidiaries under one Global CBPR or Global PRP certification, so long as they all follow the same data protection and privacy policy and procedures. Participating jurisdictions ensure that the Program Requirements can be enforced under their laws, or they legally recognize the Global CBPR and Global PRP Systems as valid data transfer mechanisms.

Importantly, **the Global CBPR and Global PRP are able to co-exist alongside other transfer and due diligence mechanisms**; they do not intend to replace these other mechanisms in contexts where such mechanisms might be more appropriate or effective. However, due to the multilateral and flexible nature of Global CBPR and Global PRP certifications, their utility will increase as the number of participating jurisdictions and certified organizations grows.

II. GLOBAL CBPR & GLOBAL PRP: THE BASICS

A. Origins: APEC CBPR

The Global CBPR and Global PRP Systems are based on the identically titled regional transfer mechanisms first developed by Asia-Pacific Economic Cooperation (APEC), a forum of Asia-Pacific economies.

APEC created the CBPR system in 2011; the PRP followed in 2015. The CBPR and PRP are based on the nine Privacy Principles set forth in the APEC Privacy Framework—specifically: (1) preventing harm, (2) notice, (3) collection limitations, (4) uses of personal information, (5) choice, (6) integrity of personal information, (7) security safeguards, (8) access and correction, and (9) accountability. The APEC CBPR and PRP operationalized the Privacy Principles through Program Requirements, which specified practical measures for organizations to implement and therefore demonstrate their compliance with the principles. For example, to ensure that the "notice" principle is met, the CBPR's Program Requirements stipulated that an organization's data protection and privacy policy must (among other things) inform individuals whether their personal information will or may be made available to third parties.

B. Global CBPR Forum

In 2022, the nine APEC economies participating in the APEC CBPR system at the time established the **Global CBPR Forum** for the purpose of expanding CBPR and PRP globally to address interest from jurisdictions outside APEC.[1] The Forum also seeks to share and promote best practices on privacy and data protection, as well as promote interoperability with other data protection and privacy frameworks. These objectives are outlined in the **2022 Global CBPR Declaration**.

The Forum's **Global CBPR Framework** takes reference from the APEC Privacy Framework. It establishes the **Global CBPR Privacy Principles** which form the basis for the **Global CBPR and Global PRP System Program Requirements**. The Framework is consistent with the core principles of the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The Forum's **Terms of Reference** define the structure and operational aspects of the Forum, including the Forum's membership application process.[2] The Forum's policy-making body is the **Global Forum Assembly (GFA)**, which consists of Members and operates on a consensus basis.

WHAT IS THE GLOBAL CBPR FORUM?

- ⇨ A group of jurisdictions established to transform CBPR and PRP into global transfer mechanisms.
- ⇨ Extends membership to jurisdictions that accept the principles and objectives of Global CBPR Declaration and Framework.
- ⇨ Invites other jurisdictions to participate as Associates to learn more.

The Forum has administrative, operational, and oversight functions with respect to the Global CBPR and Global PRP Systems. These are described in the **Global CBPR and Global PRP Systems Policies, Rules, and Guidelines**, which also describe the Systems—their core elements, governance structure,

and the roles and responsibilities of participating stakeholders, i.e., Global CBPR Forum Members, Privacy Enforcement Authorities (PEAs), and Accountability Agents (AAs).[3]

C. Participation in the Forum

Jurisdictions can participate in the Global CBPR Forum as either **Members** or **Associates**, depending on their level of readiness to operationalize the Global CBPR and Global PRP Systems in their jurisdictions.

Jurisdictions that are **not ready** to operationalize the Systems, but want to find out more, can apply to participate in the Forum as Associates. Associates can participate in Forum activities and in GFA meetings. However, because the GFA comprises jurisdictions that are *Members* of the Forum, Associates may not participate in the GFA's decision-making processes.

Becoming an Associate is a pathway for a jurisdiction to join the Global CBPR and/or Global PRP Systems. It is envisaged that participation as an Associate will help a jurisdiction prepare for eventual membership.

To apply:

1. they ***express support*** for the principles and goals of the Forum (and by extension, the Global CBPR and Global PRP Systems);
2. they confirm they ***have*** **a data protection and privacy law** (or laws that protect personal information when enforced); and
3. they show they ***have*** **at least one Privacy Enforcement Authority (PEA)**.

KEY FORUM DOCUMENTS

- ⇨ 2022 Global CBPR Declaration
- ⇨ Global CBPR Framework
- ⇨ Terms of Reference
- ⇨ Global CBPR & PRP Systems Policies, Rules, & Guidelines
- ⇨ Global CBPR System Program Requirements
- ⇨ Global PRP System Program Requirements
- ⇨ Global Cooperation Arrangement for Privacy Enforcement (CAPE)

See Appendix B

Jurisdictions that are **ready** to operationalize the Systems can apply for membership. The membership application demands a higher level of commitment:

1. they ***concur*** with the Forum's principles and goals and ***demonstrate alignment*** of their data protection and privacy law (and/or other relevant laws) to the Global CBPR Framework;
2. they confirm they have at least one Privacy Enforcement Authority (PEA) as a ***participant*** of the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE) (discussed in Section II.D.2., below); and
3. either of the following:
    a. they commit to make use of at least one ***Accountability Agent*** (discussed in Section II.D.3., below), which would allow organizations primarily located in these jurisdictions to seek Global CBPR and/or Global PRP certifications), and they provide an ***explanation of how they may enforce*** the Global CBPR and/or Global PRP System Program Requirements in their jurisdiction; or
    b. if they do not intend to make use of an Accountability Agent, they must demonstrate that their legal system ***recognizes*** the Global CBPR and/or Global PRP Systems as ***valid data transfer mechanism(s)***. For example, if Jurisdiction X does not intend to use an Accountability Agent but demonstrates that its law recognizes Global CBPR and Global

PRP as valid data transfer mechanisms, organizations located in Jurisdiction X would be able to transfer personal data to Global CBPR- and Global PRP- certified businesses in other participating jurisdictions, but organizations primarily located within Jurisdiction X would not be able to seek certification for themselves.

It is not compulsory for a jurisdiction to become an Associate before seeking membership; interested jurisdictions that consider themselves ready can apply directly for membership.

Current members and associates are listed on the Forum's website.

See Section IV.A. for specific details on the requirements and application process for jurisdictions seeking to join the Forum as a Member or Associate.

D. Overview of Stakeholders' Roles

1. Jurisdictions

Participation by jurisdictions forms the foundation of the Global CBPR and Global PRP Systems. Their participation demonstrates that their data protection and privacy frameworks are aligned with the Program Requirements of the Global CBPR and/or Global PRP Systems, resulting in interoperability. This gives businesses the assurance that their Global CBPR or Global PRP certifications will facilitate seamless transfer of personal data across participating jurisdictions.

Domestic laws and regulations provide participating jurisdictions with the **legal basis for enforcing** the Global CBPR or Global PRP Systems. For example, in jurisdictions that have data protection and privacy laws with specific notice requirements, these requirements can be used to enforce the equivalent notice obligations under the Global CBPR. Where a jurisdiction (such as the United States) has a consumer protection law that prohibits unfair and deceptive business practices, that law can be used to enforce a certified organization's public promise to adhere to the Global CBPR System Program Requirements, including the notice requirements. **A jurisdiction need not have a single, comprehensive data protection and privacy law to participate in the Global CBPR and/or Global PRP**; indeed, there could be multiple or sectoral data protection and privacy laws, or, as noted, a consumer protection law that prohibits public misrepresentations or deception by organizations. Organizations can certify to the Global CBPR or Global PRP System as long as they are subject to the enforcement jurisdiction of a PEA (or other relevant public

WHO ARE THE STAKEHOLDERS?

- ⇨ Jurisdictions
  - *may join the Global CBPR Forum as Members or Associates*
- ⇨ Privacy Enforcement Authorities
  - *Public bodies responsible for enforcing the data protection and privacy laws of a given jurisdiction*
- ⇨ Accountability Agents
  - *Third-party certification bodies recognized by the Forum to assess whether an organization satisfies the program requirements of the Global CBPR or Global PRP.*
- ⇨ Businesses
  - *Organizations principally located within a member jurisdiction acting as data controllers or processors*
- ⇨ Individuals
  - *Persons whose personal information is being transferred from one jurisdiction to another via the Global CBPR and/or Global PRP Systems*

body) in the jurisdiction in which they seek certification.[4] Domestic laws also provide the available remedies and sanctions for violations.

It is important to note that the Global CBPR and Global PRP System Program Requirements **do not replace** domestic laws and regulations. Where the data and privacy protections in domestic laws and regulations exceed or differ from the Global CBPR and Global PRP System Program Requirements, they continue to apply in addition to the Program Requirements. That said, when considering whether to participate in the Global CBPR and/or Global PRP Systems, interested jurisdictions may need to make changes to domestic laws and regulations to ensure the necessary elements for the Global CBPR and/or PRP Systems are in place.[5]

ENFORCEABILTY IS KEY

- ⇨ A jurisdiction's underlying law provides the legal basis for enforcing the Global CBPR & Global PRP.
- ⇨ A jurisdiction must show the law's alignment with the Global CBPR & Global PRP Program Requirements or other means for enforcement.
- ⇨ A Privacy Enforcement Authority enforces the Program Requirements by reference to analogous or otherwise relevant legal provisions.

In summary, **jurisdictions have flexibility in operationalizing the Global CBPR and/or Global PRP; they only need to demonstrate how the Global CBPR and/or Global PRP Program Requirements can be enforced under their domestic legal system.** The Forum does not mandate whether or how the data protection and privacy laws of a given jurisdiction should be modified. If a jurisdiction identifies an enforcement gap, it is up to the jurisdiction to determine whether the gap is material and, if so, how it should be addressed.

INVESTIGATIONS *AND/OR* ENFORCEMENT

- ⇨ The Global CBPR Framework provides that a Privacy Enforcement Authority must have power to conduct investigations "and/or" pursue enforcement proceedings. The use of "and/or" is meant to address situations where a PEA has power only to investigate violations and other entities (such as courts) have authority to enforce.

2. Privacy Enforcement Authorities

Any jurisdiction wishing to join the Forum must have at least one Privacy Enforcement Authority (PEA), a public body responsible for enforcing the data protection and privacy laws of that jurisdiction. A jurisdiction may have multiple PEAs, such as in the case of a legal regime based on multiple sectoral laws. A consumer protection authority may also be a PEA if the relevant consumer protection law can be used to enforce against pertinent violations (as in the case of the U.S., where the Federal Trade Commission has power to enforce an organization's promise to adhere to a privacy certification). Regardless, the PEA must have power to conduct investigations "and/or" pursue enforcement proceedings. [For an explanation of the use of "and/or," please see the blue box to the left.]

For a jurisdiction to become a *member* of the Global CBPR Forum, it must have at least one PEA participating in the **Global Cooperation Arrangement for Privacy Enforcement (Global CAPE)**,[6] which is a practical

multilateral mechanism that enables PEAs to cooperate in cross-border data protection and privacy enforcement matters. If multiple PEAs within a given jurisdiction will be enforcing the Global CBPR or Global PRP, each such PEA must participate in the CAPE. The Global CAPE aims to:

- facilitate information sharing among participating Privacy Enforcement Authorities;
- provide mechanisms to promote effective cross-border cooperation between Privacy Enforcement Authorities in the enforcement of data protection and privacy laws[7]; and
- encourage information sharing and cooperation on data protection and privacy investigation and enforcement with Privacy Enforcement Authorities not participating in the Global CAPE.[8]

3. Accountability Agents

An Accountability Agent is a third-party certification body approved (i.e., "recognized") by the Forum to assess whether a data controller (or data processor) satisfies the program requirements of the Global CBPR (or Global PRP). An Accountability Agent can be for-profit or not-for profit, or a public body, including a Privacy Enforcement Authority (see discussion below in Section IV.B.). Until an Accountability Agent has been identified by a member jurisdiction and recognized by the Forum, controllers and processors "primarily located" in that jurisdiction cannot be certified.

There is no limit to the number of Accountability Agents a participating jurisdiction can use, but each must meet specific **Accountability Agent Recognition Criteria**[9] in order to be approved by the Forum. These Recognition Criteria address a number of issues, including:

WHO MAY BE AN ACCOUNTABILITY AGENT?

⇨ Privacy Enforcement Authority
- *The PEA or another public body of a Forum Member may serve as its Accountability Agent. The Accountability Agent Recognition Criteria and Recognition Application Process still apply.*

⇨ For-profit or not-for-profit entities
- *Both for-profit and not-for-profit entities may serve as Global CBPR and Global PRP Accountability Agents so long as they meet the recognition criteria.*

- **No actual or potential conflict of interest.** An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the Global CBPR and/or Global PRP Systems.
- **Ongoing monitoring and compliance review.** An Accountability Agent must have comprehensive written procedures designed to ensure the integrity of the certification process and to monitor certified organizations throughout their certification periods to ensure continued compliance with the Global CBPR and/or Global PRP Program Requirements.
- **Re-certification and annual attestation**. An Accountability Agent must require certified entities to attest to continued compliance with the Program Requirements annually. The Accountability Agent must also carry out regular comprehensive reviews of certified entities' policies and practices before re-certification. Additionally, where a certified entity makes a material change to its privacy policies, the Accountability Agent must immediately review the entity's policies and practices to ensure continued compliance with the Program Requirements.

- **Dispute Resolution Process.** An Accountability Agent must have a mechanism to receive and investigate complaints about certified entities and to resolve disputes between complainants and certified entities in relation to non-compliance with the Program Requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents when appropriate and where possible.

- **Mechanism for Enforcing Program Requirements.** An Accountability Agent must have the authority to enforce its program requirements against certified entities, either through contract or by law. It must also have a process in place for notifying certified entities immediately of non-compliance with the Program Requirements and for requiring certified entities to remedy the non-compliance within a specified time period. An Accountability Agent must also have processes in place to impose penalties.[10]

- **Reporting non-compliance.** An Accountability Agent must refer a matter to the appropriate PEA(s) and other relevant government entities for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a certified entity's failure to remedy a non-compliance with the Program Requirements within a reasonable time can be a violation of applicable law.[11]

- **Case notes.** An Accountability Agent has an obligation to release case notes on a selection of resolved complaints related to the Global CBPR System in order to: (1) promote understanding and increase transparency about the Global CBPR System, (2) aid consistent interpretation of the Global CBPR Privacy Principles and the Global CBPR System; (3) provide additional guidance to organizations on the application of the Global CBPR Privacy Principles and the Global CBPR System; and (4) promote accountability of those involved in dispute resolution and build stakeholders' trust in the process.[12]

- **Complaint statistics.** Accountability Agents must attest that as part of their dispute resolution mechanism they have a process for releasing complaint statistics and for communicating that information to PEA(s) and relevant government entities.[13]

CERTIFICATION FEE

Accountability Agents may charge businesses a certification fee determined by local market factors. The AA's evaluation of the business's policies and practices usually takes two-to- six months, depending on the complexity of the business's existing program and the business's level of preparedness for compliance with the Global CBPR or Global PRP Program Requirements.

4. Businesses (Controllers and Processors)

To receive the Global CBPR or Global PRP certification, an organization acting as a data controller or data processor must start with a self-assessment of its data protection and privacy policies and practices against the applicable Program Requirements. The Global Forum provides **Intake Questionnaires** for this very purpose.[14] The applicant organization then provides the completed

Intake Questionnaire(s), along with any associated documentation, to an Accountability Agent for confidential review against the Global CBPR or Global PRP System Program Requirements.

As mentioned above, the Program Requirements specify practical measures that organizations must implement in order to operationalize compliance with the Global CBPR Privacy Principles.

Specifically, the Global CBPR Program Requirements[15] list questions for applicant organizations to ensure that:

- personal information protection policies are designed to prevent the misuse of personal information and consequent harm to individuals (i.e., the principle of preventing harm);
- individuals understand the organization's personal information policies (i.e., the principle of notice);
- collection of information is limited to the specific purposes stated at the time of collection (i.e., the collection limitation principle);
- the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes (i.e., the use limitation principle);
- individuals are provided with choice in relation to collection, use, and disclosure of their personal information (i.e., the principle of choice);
- the organization maintains the accuracy and completeness of records and keeps them up-to-date (i.e., the principle of integrity);
- the organization will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses (i.e., the security safeguards principle);
- individuals are able to access and correct their information (i.e., the principle of access and correction);
- the organization is accountable for complying with measures that give effect to the Privacy Principles (i.e., the accountability principle).

WHAT DO THE GLOBAL CBPR PROGRAM REQUIREMENTS ADDRESS?

- ⇨ Preventing the misuse of personal information (PI) and consequent harm to individuals
- ⇨ Notifying individuals of PI privacy policies and practices
- ⇨ Limiting collection of PI to specific purposes
- ⇨ Limiting use of PI to specified purposes and compatible/related purposes
- ⇨ Providing choice to individuals in relation to the collection, use, and disclosure of their PI
- ⇨ Maintaining accuracy and completeness of PI records and keeping them up-to-date
- ⇨ Implementing reasonable security safeguards
- ⇨ Providing individuals with the ability to access and correct their PI
- ⇨ Demonstrating that accountability measures are in place

The Global PRP System Program Requirements[16] focus on just two principles—security safeguards and accountability measures—asking questions to ensure that processors will implement reasonable security safeguards and responsible data practices (such as limiting the processing of personal information to the purposes specified by the controller).

If the Accountability Agent determines that the organization is compliant with the Global CBPR and/or Global PRP System Program Requirements, the Accountability Agent will certify the organization as Global CBPR and/or Global PRP compliant and will publish the relevant details of the certification on the Global CBPR Forum website[17] so that consumers and other stakeholders can be made aware that the organization is an active participant in the Global CBPR and/or Global PRP Systems.

As a condition for certification, an organization must publicly state that it will comply with the Global CBPR and/or Global PRP System Program Requirements. This public statement must link to the applicable Global CBPR and/or Global PRP System Program Requirements on the certifying Accountability Agent's website and on the Forum's website.[18]

Certifications are subject to annual attestation and re-certification.[19]

For enforceability, organizations may certify only in jurisdictions in which they are "primarily located."[20] In practice, this has been interpreted to refer to the jurisdiction in which the organization is headquartered.

A Global CBPR and/or Global PRP certification can cover multiple organizations within the same corporate family (e.g. affiliates and subsidiaries of the certifying entity), so long as they follow the same data protection and privacy policies and practices. Subsidiaries can be included in the certifications of parent companies, but not vice versa. Subsidiaries may obtain certifications for themselves in jurisdictions in which they are "primarily located." An organization can also limit a Global CBPR or Global PRP certification to a specific business line within the organization so long as it is clearly identifiable and distinguishable from others to avoid consumer confusion. The specific scope of a certification as a transfer mechanism can be defined by the participating jurisdiction consistent with their domestic law.

5. Individuals

Individuals whose personal information is being transferred from one jurisdiction to another via the Global CBPR System and/or Global PRP System are able to report complaints about a Global CBPR or Global PRP-certified organization to:

- the certified organization itself;
- the Accountability Agent that certified the organization;
- the relevant Privacy Enforcement Authority listed in the compliance directory; or
- the email address: aa@globalcbpr.org.

Compliance Directory and Contact Information. The Forum maintains a publicly accessible directory of organizations that have been certified by Accountability Agents as compliant with the Global CBPR and/or Global PRP Systems, which includes relevant details of each certification. The directory includes contact point information that consumers can use to contact certified organizations. Each organization's listing includes the contact point information for the Accountability Agent that certified the organization and the relevant PEA. Contact point information allows consumers or other interested parties to direct questions and complaints to the appropriate contact point in an organization or to the relevant Accountability Agent, or if necessary, to contact the relevant PEA.[21]

E. How Global CBPR Certification Works

If a data controller is "primarily located"[22] in a jurisdiction that is a Member of the Global CBPR Forum, the controller may apply on behalf of itself or also its subsidiaries to a Forum-recognized Accountability Agent.[23] The Accountability Agent then evaluates whether the controller's data protection and privacy policies and practices comply with the Global CBPR System Program Requirements[24] and assists the company to come into compliance with them if they do not. Once a controller is certified, its compliance with the Global CBPR System becomes an enforceable obligation. The certification is subject to annual recertification.

As noted above, the Global CBPR System does not replace domestic data protection and privacy laws or other laws. In addition to complying with the Global CBPR System Program Requirements, Global CBPR-certified organizations must also comply with domestic data protection and privacy laws. The Global CBPR System is enforceable under the domestic laws of participating jurisdictions. When a Global CBPR-certified organization transfers covered personal data across borders, it must apply the Global CBPR protections plus any additional domestic requirements.

Certified organizations are required to have effective privacy complaint and redress mechanisms to address customer complaints concerning Global CBPR violations. Companies that fail to comply with their certification are subject to sanctions by their certifying Accountability Agent, including suspension or revocation of certification. They are also subject to enforcement actions by the Privacy Enforcement Authority in the jurisdiction in which they certified.

F. How Global PRP Certification Works

To obtain a Global PRP certification, data processors go through a similar certification process.

An interested data processor should approach an Accountability Agent that operates in the jurisdiction that the data processor is "primarily located." The same rules with respect to certifying corporate affiliates under a single certification apply under the Global PRP as well. The Accountability Agent evaluates whether the processor's data protection and privacy policies and practices comply with the Global PRP System Program Requirements[25] and assists the processor to come into compliance with them if they do not. Once a processor is certified, its compliance with the Global PRP becomes an enforceable obligation. The certification is subject to annual recertification.

III. GLOBAL CBPR & GLOBAL PRP: THE BENEFITS

A. Benefits for Jurisdictions and PEAs

Participation in the Global CBPR and Global PRP Systems affords jurisdictions an opportunity to facilitate cross-border trade with participating jurisdictions, and, in a more limited way, with non-participating jurisdictions (e.g., in cases where subsidiaries of certified organizations are located in non-participating jurisdictions). By enabling commerce with other jurisdictions, participation boosts the economy of a jurisdiction while protecting the personal information of citizens.

Participation in the Global CBPR Forum also allows jurisdictions to shape international data protection and privacy standards as the Forum seeks to ensure that the Program Requirements remain up to date with international trends and practices. Indeed, the Forum updated the CBPR Program Requirements in March 2026 to better align data protection and privacy requirements among Global CBPR Forum Members and Associates and to enhance data privacy and protection for individuals.[26] The Program Requirements, as updated, become effective April 1, 2027.

Jurisdictions are able to participate in the Global CBPR and Global PRP Systems by recognizing these Systems as valid data transfer mechanism(s) in their legal regimes, without having to nominate an Accountability Agent. This means that smaller jurisdictions can reap the benefits of these Systems and participation in the Forum without putting in the resources associated with setting up a domestic certification body.

Jurisdictions can also attract business for local industry, particularly in the data processing context, by participating in the Global CBPR and Global PRP Systems. Global PRP certifications can streamline due diligence, giving certified processors in a given jurisdiction a competitive advantage over processors in jurisdictions that do not participate in the Global CBPR or Global PRP Systems.

Moreover, Global CBPR and Global PRP certifications enable more streamlined and efficient data protection and privacy investigations and enforcement actions, providing added benefits to local and/or national enforcement authorities. For starters, these certifications raise the general level of data protection and privacy compliance, therefore giving rise to fewer consumer complaints and enforcement actions. Furthermore, since organizations must have formal dispute resolution mechanisms in place as part of their Global CBPR compliance, enforcement authorities will be relieved of complaints resolved by the organizations themselves. Also, the Global CBPR System delegates many basic, frontline enforcement functions to Accountability Agents, thereby freeing up enforcement authorities to focus on more serious violations.

Additionally, the Global CAPE, which is open to all jurisdictions (i.e., not limited to Forum members), enables cross-border enforcement cooperation in relation to violations of the Global CBPR and Global PRP systems as well as violations of privacy laws not related to Global CBPR or Global PRP.

B. Benefits for Businesses

Businesses that certify to the Global CBPR and Global PRP can reap substantial benefits, including:

- **Facilitating Data Transfers:** Global CBPR and Global PRP certifications serve as a trustmark for organizations in the transfer of personal data.

- **Enabling Compliance**: Global CBPR and Global PRP are comprehensive data and privacy management programs that can facilitate compliance with domestic data protection and privacy laws as well as with relevant internationally recognized standards.
- **Assisting SMEs:** Global CBPR and Global PRP can be particularly helpful for SMEs that may lack the expertise, staff, or resources to devise their own comprehensive data protection and privacy programs.
- **Promoting Due Diligence**: Global CBPR and Global PRP can serve as due diligence and risk management tools for companies seeking qualified third-party vendors, processors, and business partners.
- **Stepping Stone to Other Certifications.** Global CBPR and Global PRP certification can facilitate and enhance preparation for participating in other similar certifications and transfer mechanisms, such as EU Binding Corporate Rules or ISO 27701.
- **Demonstrating Accountability**: Certifications such as the Global CBPR and Global PRP allow an organization to demonstrate corporate digital responsibility to consumers, potential business partners, and Privacy Enforcement Authorities, increasing the level of trust in the data management practices of that organization.
- **Mitigating Factor in Enforcement**: Global CBPR and Global PRP certifications can serve as a mitigation factor in enforcement contexts where data protection and privacy laws allow consideration of good faith compliance efforts (such as participation in privacy codes of conduct and certifications) in enforcement and fine-setting decisions.

C. Benefits for Individuals

Global CBPR and Global PRP certifications ensure that a company has an effective data protection and privacy program in place that meets high standards, which results in stronger and more effective and consistent privacy protections for consumers. Moreover, certification provides complaint and dispute resolution mechanisms for consumers that might otherwise not be available.

IV. GLOBAL CBPR & GLOBAL PRP: THE APPLICATION PROCESS

A. Jurisdictions: Application for Membership

a. Application for Admission as a Forum Member.

A jurisdiction seeking to become a member must take the following steps:[27]

1. Contact the Chair of the Membership Committee in writing to express interest in joining as a member and to initiate consultations with the Membership Committee.
2. Prepare an application that comprises a **Letter of Intent** and relevant supporting documents, to be submitted to the Chair and Deputy Chair of the Global Forum Assembly and the Chair of the Membership Committee. The Letter of Intent should confirm that the applicant jurisdiction:
   a. concurs[28] with the principles and objectives of the Forum as set forth in the **Global CBPR Declaration** and the **Global CBPR Framework**;
   b. identifies at least one Privacy Enforcement Authority[29] in its jurisdiction that is participating in the **Global Cooperation Arrangement for Privacy Enforcement** ("Global CAPE")[30]; and
   c. **demonstrates alignment**[31] of its domestic legal system with the Global CBPR Framework by either:
      i. stating that it intends to make use of at least one Global CBPR Forum-recognized **Accountability Agent**[32] and submits an **explanation** of how the Global CBPR and/or Global PRP program requirements may be enforced in its jurisdiction[33]; or
      ii. demonstrating that its **domestic legal system recognizes the Global CBPR System and/or Global PRP System as a valid data transfer mechanism(s)**, in the event that the Applicant does not intend to make use of a Global CBPR Forum-recognized Accountability Agent.[34]

APPLICATION FOR MEMBERSHIP

- ⇨ Contact Membership Committee Chair to initiate consultations
- ⇨ Prepare Letter of Intent that confirms:
  - *Agreement with principles and objectives of Global CBPR Forum*
  - *Participation of Privacy Enforcement Authority in Global CAPE*
  - *Alignment of domestic law through either an enforcement map (if intending to use an Accountability Agent) or confirmation that domestic law recognizes Global CBPR*

b. Application for Admission as Associate.

A jurisdiction seeking Associate status must take similar steps, specifically:

1. Contact the Chair of the Membership Committee in writing to express interest in joining as an Associate and to initiate consultations with the Membership Committee.
2. Prepare an application that comprises a **Letter of Intent** to be submitted to the Chair and Deputy Chair of the Global Forum Assembly and the Chair of the Membership Committee.[35]

Differing slightly from that required of those seeking full membership, the Letter of Intent for Associate Status should state that the applicant jurisdiction:

a. **supports** the principles and objectives of the Forum as set forth in the Global CBPR Declaration and the Global CBPR Framework;

b. has laws and/or regulations that protect personal information; and

c. has a public body that is responsible for enforcing the jurisdiction's data protection and privacy law and has power to conduct investigations or pursue enforcement proceedings.

WHO REPRESENTS PARTICIPATING JURISDICTIONS?
as of June 2026

—— MEMBERS ——

⇨ AUSTRALIA:	*Attorney-General's Department*
⇨ CANADA:	*Innovation, Science and Economic Development Canada*
⇨ DUBAI INT'L FINANCIAL CENTRE:	*DIFC Data Protection Commissioner*
⇨ JAPAN:	*Ministry of Economy, Trade and Industry*
⇨ REPUBLIC OF KOREA:	*Ministry of Foreign Affairs*
⇨ MEXICO:	*Ministry of Economy*
⇨ PHILIPPINES:	*National Privacy Commission*
⇨ SINGAPORE:	*Infocomm Media Development Authority*
⇨ CHINESE TAIPEI:	*National Development Council and Ministry of Foreign Affairs*
⇨ UNITED STATES:	*Department of Commerce*

—— ASSOCIATES ——

⇨ BERMUDA:	*The Cabinet Office*
⇨ MAURITIUS:	*Data Protection Office*
⇨ NIGERIA:	*Nigeria Data Protection Commission*
⇨ UNITED KINGDOM:	*Department for Science, Innovation and Technology*

B. Accountability Agents: Application and Nomination for Recognition

There are two ways by which an organization can be recognized as an Accountability Agent:

a. an application supported by the Member in which it wishes to operate, or
b. nomination by a Member.

In both cases, the process outlined in the Global CBPR Forum Accountability Agent Application[36] applies; the organization seeking to become an Accountability Agent or the Member nominating the organization must prepare an application which comprises the following:

- Explanation of how the organization is subject to enforcement by a Privacy Enforcement Authority or other relevant enforcement authority of a member jurisdiction;

  AND

- Description of how the organization has met each of the Accountability Agent Recognition Criteria[37]. The Accountability Agent Recognition Criteria Checklist[38] is to be used for this purpose;

  AND

- The organization's agreement to use the Global CBPR System Intake Questionnaire[39] and/or the Global PRP System Intake Questionnaire[40] to assess an entity's compliance with the applicable Program Requirements;

  - **OR** use the Global CBPR System Program Requirements Map[41] and/or the Global PRP System Program Requirements Map[42] to demonstrate how its own intake and review processes meet the program requirements, and publish its program requirements;

  AND

- Signed attestation from the organization, using the signature and contact information sheet.[43]

An organization seeking to become an Accountability Agent should submit the completed application to the government entity in the jurisdiction where it intends to operate; the jurisdiction should be a Member of the Global CBPR Forum.[44]

Upon receipt of an application, the Member should forward the application to the Chair and Deputy Chair of the Global Forum Assembly (GFA)[45] and the Chair of the Accountability Agent Oversight and Engagement Committee (AA Committee).[46] The Member should also include a description of the relevant domestic laws and regulations which may apply to the activities of Accountability Agents operating within its jurisdiction and the enforcement authority associated with these laws and regulations.

Use of Accountability Agent operating in another jurisdiction. A Forum member may propose to the AA Committee to make use of an Accountability Agent operating in another member jurisdiction to certify organizations principally located within its borders. The proposing Member should describe to the AA Committee the relevant domestic laws and regulations which may apply to the activities of such an Accountability Agent operating within its jurisdiction and the domestic enforcement authority associated with these laws and regulations.[47]

Review of the Application/Nomination. The Forum processes applications and nominations for Accountability Agent recognition via the following steps:

- The AA Committee reviews applications and nominations for Forum recognition of Accountability Agents. It may consult the organization seeking to become an Accountability Agent or the nominating Member for more information to ensure that the Accountability Agent Recognition Criteria have been met.
- The AA Committee drafts a recommendation on whether the GFA should recognize that the organization seeking to become an Accountability Agent has met the criteria established in the Accountability Agent Recognition Application. This recommendation describes how each of the criteria have or have not been met.[48] The AA Committee transmits its recommendation to the GFA for consensus decision. The GFA may consult stakeholders, such as business or civil society representatives, when considering the AA Committee's recommendation.
- Upon the GFA's endorsement, the AA Committee Chair will communicate the outcome in writing to the applicant. The AA Committee's recommendation is also made publicly available on the Forum's website.[49]

Recognition period. An Accountability Agent's first recognition is limited to one year from the date of recognition. Recognition for the same Accountability Agent is then for two years thereafter. One month prior to the end of the recognition period, an Accountability Agent must re-apply for Forum recognition, following the same process as described above.[50]

C. Businesses: Application for Certification and Ongoing Compliance

Businesses interested in Global CBPR certifications (for data controllers) or Global PRP certifications (for data processors) should approach an Accountability Agent operating in the jurisdiction where the business is "primarily located."[51] The certification process is summarized below:

- The Accountability Agent provides the Intake Questionnaire[52] to the applicant organization for a self-assessment of its data protection and privacy policies and practices against the Program Requirements.
- The Accountability Agent verifies the completed Intake Questionnaire and any supporting documentation against the Program Requirements. To do so, the Accountability Agent may conduct in-person or phone interviews, inspection of the personal data system, website scans, or use automated security tools.
- The Accountability Agent produces a comprehensive report to the organization, outlining the Accountability Agent's findings regarding the organization's level of compliance with the Program Requirements. To help the organization address gaps in its data protection and privacy policies which result in non-fulfilment of any of the Program Requirements, the Accountability Agent would recommend changes the organization needs to complete for purposes of obtaining certification, and verify the changes after they are made. This is an iterative process and allows for back-and-forth discussions between the organization and the Accountability Agent.[53]
- Once the Accountability Agent is satisfied that the organization is in compliance with the Program Requirements, it certifies the organization and provides the certification details for the Forum's Compliance Directory.

Upon certification, businesses are subject to ongoing compliance monitoring by their Accountability Agents. In the event of suspected non-compliance, Accountability Agents will undertake an appropriate review of the issue and may notify the certified business about any necessary corrections and the timeframe by which they must be made. Businesses are also subject to an annual re-certification requirement under the Global CBPR and Global PRP. Accountability Agents have a range of options to ensure that certified organizations comply with the Program Requirements, including suspension or withdrawal of the certification.

V. CHECKLIST

A. For Jurisdictions Seeking Membership

- ✓ Contact Chair of Membership Committee to express interest and initiate consultations to help prepare for the membership application;
- ✓ Prepare Letter of Intent that confirms:
  - agreement with principles and objectives of Global CBPR Forum and demonstration of alignment of legal system with the Global CBPR Framework;
  - participation of Privacy Enforcement Authority in Global CAPE;
  - either of the following:
    - Intent to use at least one Accountability Agent and demonstrate enforceability of the Global CBPR and/or Global PRP System Program Requirements
    - Recognition of Global and/or Global PRP as valid transfer mechanisms in legal system if there is no intent to use Accountability Agent.

B. For Jurisdictions Seeking Associate Status

- ✓ Contact Chair of Membership Committee to express interest and initiate consultations to prepare for the Associate application;
- ✓ Prepare Letter of Intent that confirms:
  - support for principles and objectives of Global CBPR Forum;
  - presence of legal system that protects personal information; and
  - presence of public body with investigatory and enforcement powers on data protection and privacy issues.

C. For Organizations Seeking to Become Accountability Agents

- ✓ Prepare application which:
  - Explains how organization is subject to enforcement by a Privacy Enforcement Authority or other relevant authorities in that jurisdiction;
  - Describes how Accountability Agent Recognition Criteria have been met;
  - Confirms that the organization will make use of the Intake Questionnaires or Program Requirements Maps to assess the compliance of organizations seeking Global CBPR and/or Global PRP certifications;
  - Includes the completed signature and contact information sheet.

D. For Businesses

- ✓ Be “primarily located” in a jurisdiction with at least one Forum-recognized Accountability Agent;
- ✓ Prepare self-assessment using the Intake Questionnaire;
- ✓ Provide completed questionnaire to an Accountability Agent in that jurisdiction;
- ✓ Work with Accountability Agent to satisfy Program Requirements.

APPENDIX A: Glossary of Abbreviations

AA	**Accountability Agent** *A Forum-recognized third-party certification body that assesses whether a data controller (or data processor) satisfies the program requirements of the Global CBPR (or Global PRP).*
AA Committee	**Accountability Agent Oversight and Engagement Committee** *Reviews and makes recommendations to the GFA on matters relating to Accountability Agents, including applications for recognition as an Accountability Agent*
APEC	**Asia-Pacific Economic Cooperation** *A regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific.*
CBPR	**Cross-Border Privacy Rules** *A voluntary enforceable accountability-based scheme to facilitate data protection- and privacy-respecting personal information flows across jurisdictions.*
GFA	**Global Forum Assembly** *The policy-making body of the Global CBPR Forum. It comprises jurisdictions that are Members of the Forum.*
Global CAPE	**Global Cooperation Arrangement for Privacy Enforcement** *A multilateral mechanism that enables Privacy Enforcement Authorities to cooperate in cross-border enforcement of data protection and privacy laws.*
OECD	**Organisation for Economic Cooperation and Development** *An international organization that, among other things, developed in 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*
PEA	**Privacy Enforcement Authority** *A public body responsible for enforcing data protection and privacy laws with power to conduct investigations and pursue enforcement proceedings.*
PRP	**Privacy Recognition for Processors** *A voluntary accountability-based scheme to help data processors demonstrate their ability to provide effective implementation of a personal information controller's data protection and privacy obligations related to the processing of personal information.*

APPENDIX B: Key Documents

Note: ***The following documents can be accessed on the Global CBPR Forum's website: https://www.globalcbpr.org/documents/.***

Global Cross-Border Privacy Rules (CBPR) Declaration

Establishes the Global CBPR Forum.

Global Cross-Border Privacy Rules (CBPR) Framework

Sets forth the principles and objectives of the Forum, including the Global CBPR Privacy Principles upon which the Global CBPR System and Global PRP System are designed.

Terms of Reference

Defines the structure of the Forum and the process for admitting Members and Associates.

Template Letter of Intent for Membership

For jurisdictions seeking to become Members of the Forum.

Template Letter of Intent for Associate Status

For jurisdictions seeking to become Associates of the Forum.

Global Cooperation Arrangement for Privacy Enforcement (Global CAPE)

Describes the structure and processes for PEAs – not limited to those of Members or Associates – to cooperate in cross-border data protection and privacy enforcement matters.

Template Letter of Intent for Global CAPE

For PEAs seeking to participate in Global CAPE.

Global CBPR and Global PRP Systems Policies, Rules, and Guidelines

Describes the core elements, governance structure, and the roles and responsibilities of participating organizations, Accountability Agents, PEAs, and Global CBPR Forum Members.

Global CBPR Forum Accountability Agent Application

Guides the application process for an organization seeking recognition as an Accountability Agent; explains the necessary recognition criteria and provides the program requirements of the Global CBPR and Global PRP Systems

Global CBPR System Program Requirements

Provide the baseline requirements that operationalize the Global CBPR Privacy Principles and assist Accountability Agents in reviewing an Applicant Organization's compliance with the Global CBPR System.

Global CBPR System Program Requirements Map

A tool for Accountability Agents to use when reviewing an Applicant Organization's compliance with the Global CBPR System

Global PRP System Program Requirements

Provide the baseline requirements that operationalize the Global CBPR Privacy Principles and assist Accountability Agents in reviewing an Applicant Organization's compliance with the Global PRP System

Global PRP System Program Requirements Map

A tool for Accountability Agents to use when reviewing an Applicant Organization's compliance with the Global PRP System.

Global CBPR System Intake Questionnaire

A tool for a controller seeking Global CBPR certification from a Forum-recognized Accountability Agent.

Global PRP System Intake Questionnaire

A tool for a processor seeking Global PRP certification from a Forum-recognized Accountability Agent.

NOTES

[1] The nine are Australia, Canada, Japan, Republic of Korea, Mexico, Philippines, Singapore, Chinese Taipei, and the United States. The Global CBPR Forum website is available at https://www.globalcbpr.org/. The Global Cross-Border Privacy Rules Declaration, issued Apr. 21, 2022, is available at https://www.globalcbpr.org/documents/.

[2] The referenced documents are available at https://www.globalcbpr.org/documents/. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are available at https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.

[3] The referenced document is available at https://www.globalcbpr.org/documents/.

[4] A certified organization is also subject to enforcement (through law or contract) by the Accountability Agent from which it received its certification. See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 28, available at https://www.globalcbpr.org/documents/.

[5] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 62, available at https://www.globalcbpr.org/documents/.

[6] See the Global Cooperation Arrangement for Privacy Enforcement, available at https://www.globalcbpr.org/documents/.

[7] "Data Protection and Privacy Laws" are defined as "laws and regulations of a Participant's jurisdiction, the enforcement of which has the effect of protecting personal information consistent with the Global CBPR Framework." See Global Cooperation Arrangement for Privacy Enforcement, paragraph 3.1(b). This broad definition is designed to capture laws that are not traditional data protection and privacy laws but that can be used to protect privacy, such as consumer protection laws.

[8] Global CBPR Framework, p. 7. Available at https://www.globalcbpr.org/documents/.

[9] Set forth in Annex A of the Global CBPR Forum Accountability Agent Application, available at https://www.globalcbpr.org/documents/.

[10] Specific penalties are identified in Annex A, paragraph 13, of the Global CBPR Forum Accountability Agent Application.

[11] See Annex A, paragraph 14, of the Global CBPR Forum Accountability Agent Application.

[12] See Annex E of the Global CBPR Forum Accountability Agent Application. See also, Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 46.

[13] See Annex F of the Global CBPR Forum Accountability Agent Application. See also, Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 47.

[14] The Intake Questionnaires for the Global CBPR and PRP Systems are available at https://www.globalcbpr.org/documents/.

[15] Available at https://www.globalcbpr.org/documents/.

[16] Available at https://www.globalcbpr.org/documents/.

[17] Available at www.globalcbpr.org.

[18] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 37.

[19] See Global CBPR Forum Accountability Agent Application, Annex A, paragraph (2)(a).

[20] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 59.

[21] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 23.

[22] While APEC's CPBR System, to date, has interpreted "primarily located" as where a company is headquartered, the notion of "primarily located" may not be limited to "headquartered." The Global CBPR System may further elaborate on the meaning of "primarily located" in the context of Global CBPR and PRP.

[23] Forum-recognized Accountability Agents are listed on the Global Forum's website.

[24] The Global CBPR Program Requirements are the baseline requirements that operationalize the Global CBPR Privacy Principles and assist Accountability Agents in reviewing an Applicant Organization's compliance with the Global CBPR System. Accountability Agents use a set of specific assessment criteria associated with each of these Program Requirements to assess the privacy policies and practices of the applicants. The Global CBPR System Program Requirements are available at https://www.globalcbpr.org/documents/. See also the discussion above at Section II.D.4.

[25] The Global PRP System Program Requirements are the baseline requirements that operationalize the Global CBPR Privacy Principles and assist Accountability Agents in reviewing a processor's compliance with the Global PRP System. The Global PRP System Program Requirements are available at https://www.globalcbpr.org/documents/. See also the discussion above at Section II.D.4.

[26] See "Updates to the Global Cross-Border Privacy Rules System Strengthen Global Interoperability and Privacy," available at https://www.globalcbpr.org/updates-to-the-global-cross-border-privacy-rules-system-strengthen-global-interoperability-and-privacy/.

[27] The criteria for admission as a member jurisdiction of the Global CBPR Forum is outlined in the Annex of the Terms of Reference, available at https://www.globalcbpr.org/documents/.

[28] Those seeking Associate Status need only express "support" for the principles and objectives; they need not "concur."

[29] A Privacy Enforcement Authority is a public body that is responsible for enforcing laws and regulations addressing the protection of personal information and that has powers to conduct investigations and/or pursue enforcement proceedings. See Global CBPR Forum Terms of Reference, Annex A, available at https://www.globalcbpr.org/documents/.

[30] The Global CAPE is a practical multilateral mechanism for Privacy Enforcement Authorities to cooperate in cross-border data protection and privacy enforcement. See Global Cooperation Arrangement For Privacy Enforcement, available at https://www.globalcbpr.org/documents/.

[31] Those seeking Associate Status need not demonstrate "alignment'; rather, they need only demonstrate that they have domestic law that promotes the protection of personal information.

[32] An "Accountability Agent" is a Forum-recognized third-party certification body in the jurisdiction in which the company is "primarily located."

[33] An explanation of enforceability is done via an "enforcement map." Examples will be made available on the Global CBPR Forum's website.

[34] For example, Bermuda and the Dubai International Financial Centre (DIFC) have laws recognizing the CBPR and PRP Systems as a valid data transfer mechanisms.

[35] A template Letter of Intent for Associate Status is available at https://www.globalcbpr.org/documents/. The letter of intent should be submitted by an appropriate governmental representative of the Jurisdiction to the Chair of the Global Forum Assembly, with copy to the Deputy Chair of the Global Forum Assembly and Chair of the Membership Committee. Pertinent contact information is available on the Global CBPR Forum website.

[36] Available at https://www.globalcbpr.org/documents/.

[37] The Recognition Criteria, described in Section II.D.3, are set forth in Annex A of the Global CBPR Forum Accountability Agent Application.

[38] The Checklist appears in Annex B of the Global CBPR Forum Accountability Agent Application.

[39] The Global CBPR System Intake Questionnaire is available at https://www.globalcbpr.org/documents/.

[40] The Global PRP System Intake Questionnaire is available at https://www.globalcbpr.org/documents/.

[41] The Global CBPR Program Requirements Map appears in Annex C of the Global CBPR Forum Accountability Agent Application.

[42] The Global PRP Program Requirements Map appears in Annex D of the Global CBPR Forum Accountability Agent Application.

[43] The signature and contact information sheet appears in Annex G of the Global CBPR Forum Accountability Agent Application.

[44] As of June 2026, the following governmental entities represent the jurisdictions participating as Members in the Global CBPR Forum:

- Australia: Attorney-General's Department
- Canada: Innovation, Science and Economic Development Canada
- Dubai International Financial Centre: DIFC Data Protection Commissioner
- Japan: Ministry of Economy, Trade and Industry
- Republic of Korea: Ministry of Foreign Affairs
- Mexico: Ministry of Economy
- Philippines: National Privacy Commission
- Singapore: Infocomm Media Development Authority
- Chinese Taipei: National Development Council and Ministry of Foreign Affairs
- United States: Department of Commerce

The following participate as Associates:

- Bermuda: The Cabinet Office
- Mauritius: Data Protection Office
- Nigeria: Nigeria Data Protection Commission
- United Kingdom: Department for Science, Innovation and Technology

[45] The GFA is the policy-making body of the Forum. It comprises jurisdictions that are Members of the Forum. Associates may participate in GFA meetings, unless the GFA Chair designates a meeting or part of a meeting as participation by Members only. See Terms of Reference, paragraph 3.1, available at https://www.globalcbpr.org/documents/.

[46] The AA Committee (1) reviews and make recommendations to the GFA on applications for recognition as an Accountability Agent; (2) leads engagement with recognized AAs; (3) provides oversight of and manages complaints against recognized AAs; and (4) perform other tasks as assigned by the GFA Chair. See Terms of Reference, paragraph 3.2.vi., available at https://www.globalcbpr.org/documents/.

[47] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 34, available at https://www.globalcbpr.org/documents/.

[48] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 37.

[49] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraphs 39-43.

[50] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraph 44.

[51] While APEC's CPBR System has interpreted "primarily located" as where a company is headquartered, the Global CBPR System may elaborate on the meaning of "primarily located."

[52] The Global CBPR System and Global PRP Intake Questionnaires are available at https://www.globalcbpr.org/documents/.

[53] See Global CBPR and Global PRP Systems: Policies, Rules, and Guidelines, paragraphs 60-61.