Mapping Updated Global CBPR and Global PRP Systems' Program Requirements to the GDPR

March 2026

A comparative analysis of the General Data Protection Regulation (GDPR) with the Updated 2026 Program Requirements of the Global Cross-Border Privacy Rules (CBPR) and Global Privacy Recognition for Processors (PRP) Systems

Prepared by the Centre for Information Policy Leadership (CIPL)

Mapping Updated Global CBPR and Global PRP Systems' Program Requirements to the EU General Data Protection Regulation

March 2026

KEY TAKEAWAYS

- The digital economy relies on the flow of data across borders, and businesses need legal certainty to operate and innovate. Among the options available for data flows, only the Global Cross-Border Privacy Rules (Global CBPR) and the Global Privacy Recognition for Processors (Global PRP) Systems offer a **truly multilateral solution**.
- The Global CBPR and Global PRP Systems are not self-regulatory best practices—they are **government-recognized privacy compliance programs** enforceable by the participating jurisdictions' relevant Privacy Enforcement Authorities (PEAs).
- Certifications ensure that organizations have implemented practical measures, called "**Program Requirements**," that fulfill the privacy and data security principles set forth in the Global CBPR and Global PRP Systems.
- Participating jurisdictions ensure that the Program Requirements can be enforced under their domestic legal system. Domestic laws and regulations provide participating jurisdictions with the **legal basis for enforcing** the Global CBPR and Global PRP Systems.
- The 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 Program Requirements, they continue to apply in addition to the Program Requirements.

- The Center for Information Policy Leadership (CIPL) has examined the European Union's General Data Protection Regulation (GDPR) to analyze **whether and to what extent the GDPR aligns** with the Global CBPR Program Requirements, as updated in 2026, and the existing Global PRP Program Requirements.
- CIPL's analysis shows that **72% of the Global CBPR** Program Requirements, as updated in 2026, **fully align** with provisions found in the GDPR, and more than **75% of the Global PRP** Program Requirements align with GDPR provisions. The balance of the Program Requirements find implicit support in—i.e., are deemed "similar" to—certain provisions of the GDPR.
- Given the overwhelming degree of alignment, coupled with provisions that could be read to support the remainder of the Program Requirements, the EU's potential participation in the Global CBPR and Global PRP Systems does not appear to face significant obstacles from an enforcement perspective. In other words, **EU supervisory authorities would be able to enforce** the Program Requirements through the GDPR.
- That said, the Global CBPR and Global PRP Systems do not address certain issues covered by the GDPR, specifically **legitimate interests**, **data portability**, **automated decision making**, **data protection by design and by default**, and **onward transfers**.
- The Systems' silence on these issues, however, does not automatically present a roadblock to the EU's participation. Rather, they would serve as a **starting point for a conversation** about whether the EU views them as materially relevant to its participation.
- Furthermore, CIPL's evaluation of **pertinent guidelines issued by the European Data Protection Board** (EDPB)—i.e., Guidelines 1/2018 and Guidelines 07/2022—reveals potential gaps pertaining to the use of the Systems as certification measures pursuant to GDPR Art. 42(5). Those gaps, however, are principally the same as those identified in the reverse mapping analysis (i.e., data portability, automated decision making, data protection by design and by default, and onward transfers).
- Given that GDPR Art. 42 **encourages** the "establishment of data protection certification mechanisms … for the purpose of demonstrating compliance with this Regulation," and given the significant degree of alignment between the GDPR and the Global CBPR/Global PRP Systems, **CIPL encourages the EU to explore the Systems' benefits** and commence conversations with the Global CBPR Forum.

TABLE OF CONTENTS

I. OVERVIEW

A. Background

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. This has resulted in increasing complexity and substantial compliance challenges for organizations with multinational or global business operations. The **Global Cross Border Privacy Rules (Global CBPR) System** provides 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) System** provides analogous certifications for private sector organizations operating as data processors.

Significantly, the Global CBPR and Global PRP Systems are not self-regulatory best practices—they are **government-recognized privacy compliance programs** enforceable by the participating jurisdictions' relevant Privacy Enforcement Authorities (PEAs). Certifications ensure that organizations have implemented practical measures, called "**Program Requirements**," that fulfill the privacy and data security principles set forth in the Global CBPR and Global PRP Systems. Participating jurisdictions ensure that the Program Requirements can be enforced under their domestic legal system.

The **Global CBPR Forum**, which administers the Global CBPR and Global PRP Systems, has proposed a number of revisions to the Global CBPR Program Requirements. At the time of this writing, those revisions have not yet been finalized, but CIPL has reproduced in the Appendix the draft version of the updated Program Requirements as provided to us. The proposed updates—which appear in red text—address topics commonly found in domestic privacy laws but not previously covered by the Global CBPR System. Specifically they address:

- Sensitive personal information[1]
- Children's personal information[2]
- Parental consent or other bases for processing children's personal information[3]

[1] See proposed and renumbered Program Requirement ("PR") 1.

[2] See proposed and renumbered PR 2.

[3] See proposed and renumbered PR 3.

- Risk assessments[4]
- Breach notification protocols[5]
- Choice mechanism for direct marketing[6]
- Withdrawal of consent[7]
- Maintaining records of processing activities[8]
- Appointment of qualified individual to oversee compliance[9]

It should be noted that the proposed updates affect only the Global CBPR System. The Global PRP System at present remains unchanged.

The Global CBPR Forum invites jurisdictions worldwide to participate in the Global CBPR and/or PRP Systems. Participation by jurisdictions forms the foundation of the Global CBPR and Global PRP Systems. Participating jurisdictions have determined that their domestic legal systems are substantially aligned with the Program Requirements of the Global CBPR and/or Global PRP Systems, resulting in interoperability. Domestic laws and regulations provide participating jurisdictions with the **legal basis for enforcing** the Global CBPR or Global PRP Systems. Thus, jurisdictions interested in seeking full membership must be able to demonstrate (among other things) that the Global CBPR and PRP Program Requirements are enforceable under their laws by their relevant PEAs.

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 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 that the necessary elements for the Systems are in place.

Significantly, Global CBPR and Global PRP certifications are able to **co-exist alongside other transfer and due diligence mechanisms** like adequacy decisions, standard contractual clauses, and binding corporate rules. These and other transfer mechanisms are still available if desired

[4] See proposed and renumbered PR 4.

[5] See proposed and renumbered PR 5.

[6] See proposed and renumbered PR 22.

[7] See proposed and renumbered PR 27.

[8] See proposed and renumbered PR 46.

[9] See proposed and renumbered PR 47.

or needed. 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.

To be clear, 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.

B. CIPL's Mapping Project

The Center for Information Policy Leadership (CIPL)[10] has examined the European Union's General Data Protection Regulation (GDPR) to analyze whether and to what extent the GDPR aligns with the Global CBPR Program Requirements, as revised, and the existing Global PRP Program Requirements. In essence, this exercise is intended to support a determination by the EU as to whether the Global CBPR/Global PRP Systems' requirements are reflected in the GDPR and whether they are therefore enforceable by the supervisory authority of a given Member State.[11]

GDPR Art. 46, para. 1, provides that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country "only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

GDPR Art. 46, para. 2(f), further clarifies that "appropriate safeguards" may be provided by "**an approved certification mechanism** pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights."

[10] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this report should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[11] Most member countries of the Global CBPR Forum enforce the Program Requirements of these certifications via equivalent provisions in their own data protection laws. Where a country (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 and Global PRP Systems' Program 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.

Accordingly, the purpose of the mapping project is twofold:

(1) to determine which of the Program Requirements a supervisory authority can enforce under the GDPR (i.e., "Mapping" the Global CBPR and Global PRP Systems to the GDPR); and
(2) to identify any substantive privacy protections included in the GDPR that are not addressed in the Global CBPR/Global PRP Program Requirements (i.e., "Reverse Mapping")

The detailed chart found in the Appendix itemizes each of the recently revised Program Requirements for the Global CBPR System (in Part 1) and the Global PRP System (in Part 2) and maps them to comparable provisions in the GDPR. Part 3 is the "reverse map" that identifies substantive GDPR provisions not addressed by the Global CBPR or Global PRP Systems. Importantly, highlighting these provisions could be useful to members of the Global CBPR Forum as they contemplate whether and to what extent any of these issues should be addressed and/or included in a subsequently updated version of the Program Requirements.

In addition to the above, we also examined guidelines issued by the European Data Protection Board (EDPB) that pertain to certification measures.[12] Those guidelines set forth 82 factors to consider when approving criteria for certification pursuant to GDPR Art. 42(5). In Part 4 of the Appendix, we mapped those factors to the Program Requirements as well as to other pertinent documentation relating to the Global CBPR and Global PRP Systems.

C. Law Examined

The law principally examined in this exercise is the EU GDPR: Regulation (EU) 2016/679.[13] Although the EU has proposed a new Digital Package to simplify EU digital rules, including the GDPR,[14] this analysis will comment on proposed revisions to the GDPR only where relevant.

[12] See Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, version 3.0, adopted 4 June 2019, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en and Guidelines 07/2022 on certification as a tool for transfers, Version 2.0, adopted 14 February 2023, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en.

[13] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[14] See https://digital-strategy.ec.europa.eu/en/faqs/digital-package.

D. Analytical Procedure

To conduct our analysis, we identified provisions from the GDPR that addressed each of the Global CBPR/Global PRP Systems' Program Requirements and then assessed whether the quoted provisions aligned with, were similar to, or were different from the given Program Requirement. We used the following color-coded symbols to facilitate at-a-glance comparisons:

- 🟢 **= Aligned:** Legal provision directly supports enforcement of the Program Requirement.
- 🟡 **= Similar:** Legal provision implicitly supports enforcement of the Program Requirement (or accomplishes the same result as the Program Requirement in a different way).
- 🔴 **= Different:** No legal provision supports enforcement of the Program Requirement.[15]

It should be noted that our assessments are based on **enforceability**. In other words, our guiding question was "could a supervisory authority rely on the cited GDPR provision to enforce the Program Requirement at issue?"

[15] The extent to which a particular provision aligns with a specific Program Requirement is in some cases open to interpretation. That said, the question as to a given supervisory authority can enforce a particular Program Requirement would need to be analyzed by local experts.

E. Overall Results

To get an overall picture of how the Program Requirements align with the GDPR, we compiled individual "scores" (i.e., green, yellow, or red) from each of the Program Requirements to deliver the following high-level findings:

1. MAPPING GDPR TO THE GLOBAL CBPR SYSTEM

More than 70% of Global CBPR Program Requirements, as revised, align with the with the GDPR, with the remaining requirements classified as being similar to GDPR provisions. Given the overwhelming degree of alignment, the EU's potential participation in the Global CBPR System would not appear to face significant obstacles.

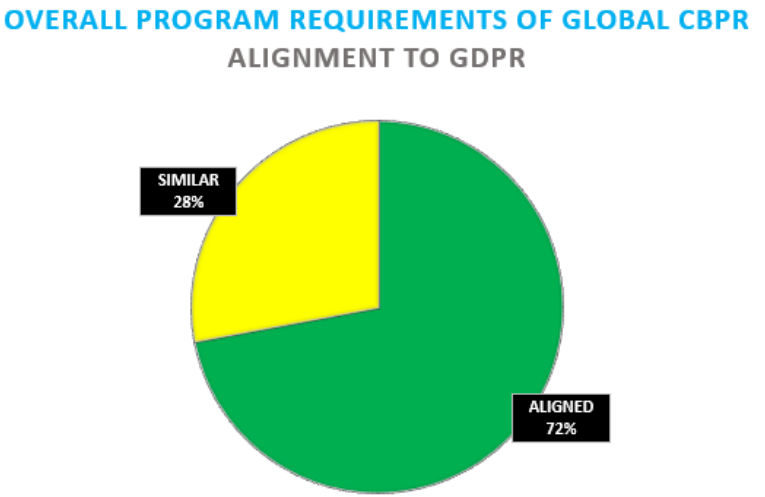

Figure 1

Our detailed Global CBPR System Mapping is available here.

2. MAPPING GDPR TO THE GLOBAL PRP SYSTEM

The Global PRP Program Requirements reveal a similar breakdown, with 76% of the Program Requirements aligned with the GDPR and the remainder deemed similar to GDPR provisions. *[See Figure 2]*. Again, our analysis shows no significant obstacles to the EU's potential participation in the Global PRP System.

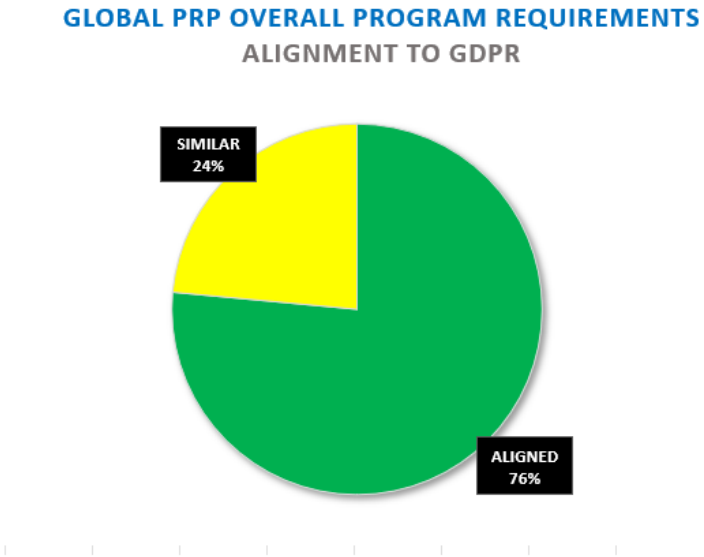

Figure 2

Our detailed Global PRP Mapping is available here.

3. REVERSE MAPPING GLOBAL CBPR/GLOBAL PRP SYSTEMS' PROGRAM REQUIREMENTS TO GDPR

Notwithstanding the updates to the Program Requirements, the "Reverse Mapping" exercise shows that the Global CBPR and PRP Program Requirements are still silent on a few issues covered by the GDPR. *[See Figure 3.]* Notably:

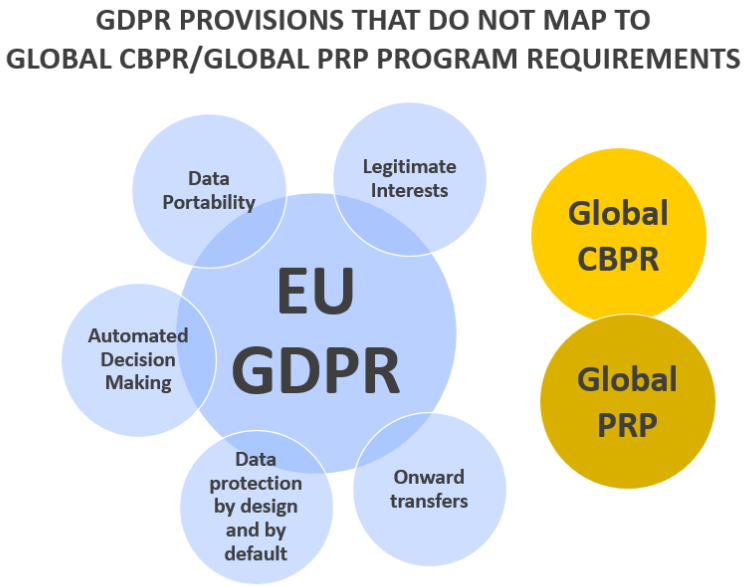

Figure 3

- Legitimate interests *[GDPR Art. 6, para. 1(f)]*
- Data portability *[GDPR Art. 20]*
- Automated decision making *[GDPR Art. 22]*
- Data protection by design and by default *[GDPR Art. 25]*
- Onward transfers *[GDPR Art. 44]*

Of course, the Global CBPR/Global PRP Systems' silence on these issues does not automatically present a roadblock to the EU's participation in the Global CBPR/Global PRP Systems. Rather, they serve as a starting point for a conversation about whether the EU views them as materially relevant to its participation. The biennial meetings of the Global CBPR Forum provide an opportunity for jurisdictions to have such conversations and address whether a given issue could or should be included in a subsequently revised set of Program Requirements at some point in the future.

Our detailed Reverse Mapping is available here.

4. MAPPING EDPB CERTIFICATION GUIDELINES THE GLOBAL CBPR & GLOBAL PRP SYSTEMS

GDPR Art. 42 ***encourages*** the "establishment of data protection certification mechanisms … for the purpose of demonstrating compliance with this Regulation …."[16] Significantly, data protection certification mechanisms, seals, or marks "may be established for the purpose of demonstrating the existence of appropriate safeguards … within the framework of personal data transfers to third countries or international organisations."[17]

The European Data Protection Board (EDPB) has issued guidance on the use of certification measures generally[18] and on the use of certification measures as tools for transfers specifically.[19] Among other things, these documents provide guidance for reviewing and identifying certification criteria pursuant to GDPR Art. 42(5). Read together, the documents set forth 82 factors to consider when approving criteria for certification pursuant to GDPR Art. 42(5).

We examined the elements identified in the two sets of Guidelines and compared them to the Program Requirements. To the extent a given factor was not addressed by the Program Requirements themselves, we looked to other documents issued by the Global CBPR Forum, including the Forum's "Global CBPR Framework"; its

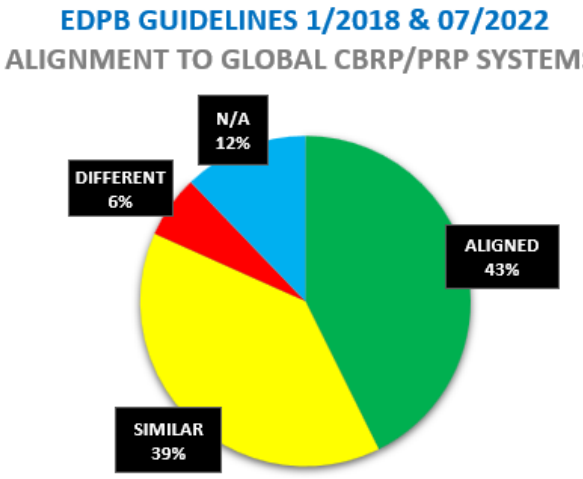

Figure 4

[16] GDPR Art. 42, para. 1.

[17] GDPR Art. 42, para. 2.

[18] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, version 3.0, adopted 4 June 2019, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en.

[19] Guidelines 07/2022 on certification as a tool for transfers, Version 2.0, adopted 14 February 2023, available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_en.

"Policies, Rules and Guidelines"; and the "Accountability Agent Recognition Application."[20]

As indicated in Figure 4, more than 80% of the EDPB's factors are either aligned with or similar to the Global CBPR and Global PRP Systems.

We classified a number of factors—principally those identified in Guidelines 07/2022—as not being relevant ("N/A"), as they address issues that are inapplicable in the Global CBPR context. For example, the Systems do not require independent assessments of a given country's laws and regulations since the jurisdictions participating in the Systems are already agreeing to a certification that promotes interoperability and helps bridge different regulatory approaches to data protection and privacy.

A small percentage of the EDPB factors (6%) differ from the Global CBPR and Global PRP Systems, but those factors reflect the gaps already noted in the reverse mapping, i.e., data portability, automated decision making, data protection by design and default, and onward transfers.

Our detailed EDPB Guidelines Mapping is available here.

[20] These and other documents are available at https://www.globalcbpr.org/documents/.

II. SPECIFIC FINDINGS ON PROGRAM REQUIREMENTS

Below we highlight key alignment and similarities between the categories of Global CBPR/Global PRP Program Requirements and the GDPR.

A. Global CBPR System Program Requirements

1. Preventing Harm

The Preventing Harm section in the Global CBPR System's Program Requirements is totally new, as it comprises the majority of the proposed revisions the Program Requirements. These new Program Requirements recognize that certain categories of personal information, including children's information, require more care because of the higher risk of harm that may result from wrongful collection or misuse. They further require controllers to evaluate risks to personal information collected and to implement remedial measures proportionate to the likelihood and severity of potential harm from misuse. Moreover, they provide that controllers should inform individuals if their personal information has been breached and provide information to enable individuals to take steps to protect themselves against misuse of their personal information.

Inasmuch as the GDPR covers all of these elements—i.e., the processing of sensitive (or special categories of) data, the processing of children's personal data; securing parental consent for such processing; an assessment of risks; and breach notification—the provisions of the GDPR fully align with these first five Program Requirements. *[See Figure 5.]*

Our detailed mapping of the Global CBPR System Preventing Harm Requirements is available here.

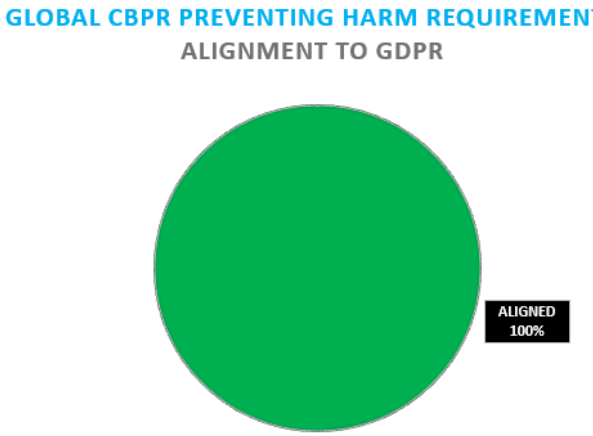

Figure 5

2. Notice

The Notice section in the Global CBPR System's Program Requirements seeks to ensure that data subjects understand not only the organization's data protection policies and practices, but also *when* personal information is being collected, for *what purpose*, and *whether and to whom* it may be shared. It places an affirmative obligation on controllers to provide such information in a privacy statement.

The GDPR mostly aligns with the Program Requirements in this section. *[See Figure 6.]* For example, GDPR Art. 12, para. 1, specifically requires controllers to provide notice of processing activities "in a concise, transparent, intelligible and easily accessible form …." Moreover, GDPR Arts. 13 and 14 specifically require the controller to provide information regarding the intended purposes of the processing at the time of collection, as well as any intended "recipients or categories of recipients" of the data.

While the GDPR does not expressly require a privacy statement to describe ***how*** personal information is collected, the language of GDPR Art 13 – "[w]here personal data relating to a data subject are collected from the data subject" – implies ***how*** it is collected, i.e., "from the data subject." Similarly, the language of GDPR Art 14—"[w]here personal data have not been obtained from the data subject—also implies ***how*** it is collected, i.e., "*not* from the data subject."

Our detailed mapping of the Global CBPR System Notice Requirements is available here.

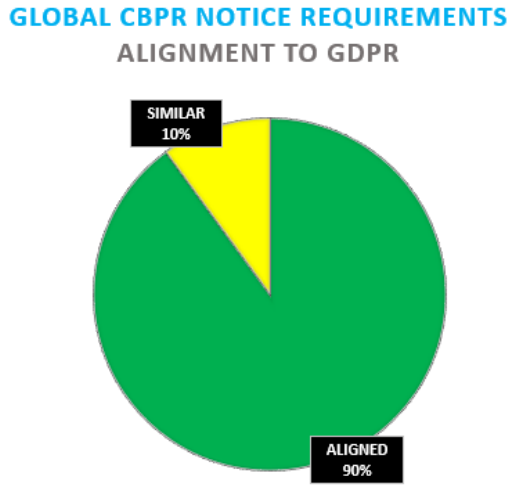

Figure 6

3. Collection Limitation

The questions in the Global CBPR System's section on collection limitation are directed toward ensuring that collection of data is limited to the stated purposes for which it is collected.

Again, the GDPR fully aligns with the Program Requirements in this section. *[See Figure 7.]*

GDPR Art. 5 addresses the lawfulness, fairness and transparency principle, as well as the purpose limitation principle. Moreover, GDPR Arts. 12 – 14, when read together, specifically require providing information of the identity and the contact details "of the **controller's representative**," i.e., a third party collecting on the controller's behalf.

Our detailed mapping of the Global CBPR System Collection Limitation Requirements is available here.

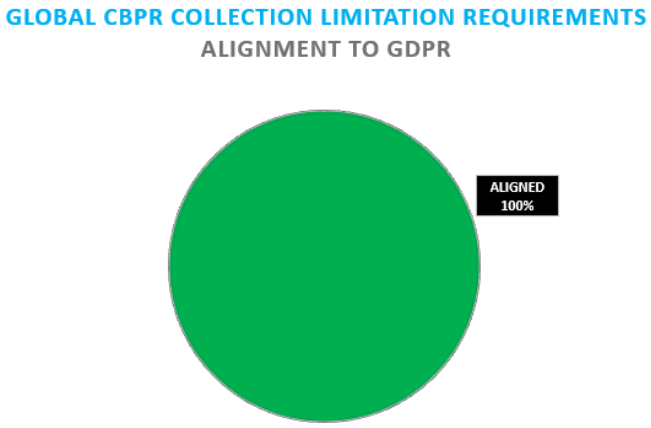

Figure 7

4. Uses of Personal Information

The Global CBPR System's questions addressing uses of personal information are directed toward ensuring that such uses are limited to fulfilling the purposes of collection and other compatible or related purposes. While the GDPR does not fully align with all of the elements of this section, some provisions could be read to infer alignment. *[See Figure 8.]*

For example, to the extent controllers must inform whether they disclose personal information to other controllers or processors, the text of para. 1(e) under GDPR Arts. 13 and 14—which requires a controller to disclose "the recipients or categories of recipients of the personal data"—could be read to infer a requirement to state whether those recipients are controllers or processors.

Similarly, to the extent controllers must describe whether such disclosures fulfill the original or another compatible or related purpose of the collection, GDPR Arts. 13 and 14 could be read to infer a requirement to state the purposes for sharing with other controllers or processors.

Our detailed mapping of the Global CBPR System Use Requirements is available here.

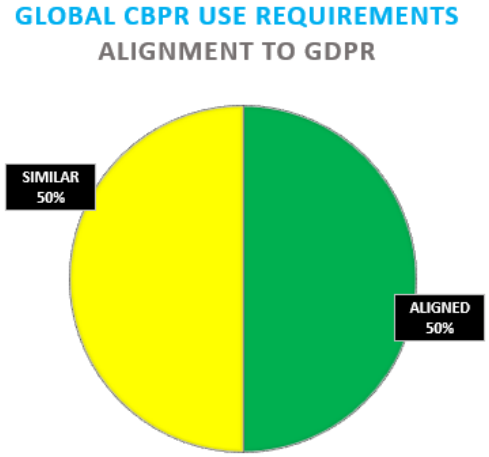

Figure 8

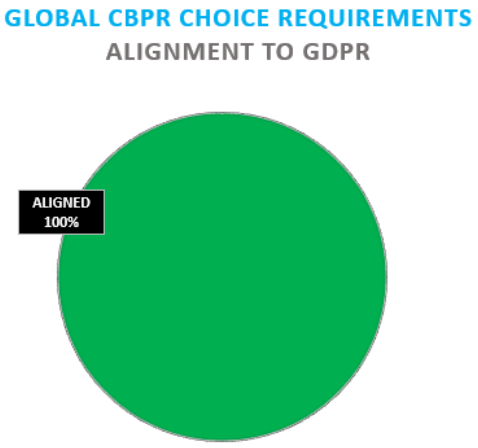

Figure 9

5. Choice

The Global CBPR System seeks to ensure that individuals are provided with *choice* in relation to collection, use, and disclosure of their personal information, where appropriate. The GDPR fully aligns with these Program Requirements, as it provides consent as a legal basis for processing. *[See Figure 9.]*

The GDPR allows for six bases upon which personal data can be processed, one of which is consent. GDPR Art. 6, para. 1(a). With the exception of legitimate interest (GDPR Art. 6, para. 1(f)), the other legal bases for processing (listed under para.1 (b)-(e)) arguably fall within the Global CBPR System's Qualifications to the Provision of Choice Mechanisms.

Where consent is relied upon as the legal basis for processing (which includes collection, use, and disclosure – see GDPR Art. 4, para. 2), the consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes. GDPR Art. 4, para. 11.

Notably, the proposed revisions to the Program Requirements add two new elements regarding choice: (1) choice regarding direct marketing (found in Program Requirement 22),and (2) choice to withdraw content (found in Program Requirement 27). Both of these requirements are reflected in the GDPR, under Art. 21 and Art. 7, respectively.

Our detailed mapping of the Global CBPR System Choice Requirements is available here.

6. Integrity of Personal Information

The Global CBPR System seeks to ensure that controllers maintain the accuracy and completeness of records, and that they keep them up to date. The GDPR's provisions are largely aligned with the Program Requirements. *[See Figure 10.]*

GDPR Art. 5 requires personal data to be accurate and, where necessary, kept up to date. To the extent inaccuracies exist, the data must be erased or rectified without delay. GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, including the right to rectification under Art. 16.

Moreover, GDPR Art. 19 expressly requires controllers to communicate "any rectification … of processing carried out in accordance with Article 16 … to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort."

While the GDPR does not expressly state that controllers must inform processors of any corrections made to the data post-transfer, such a requirement could be inferred by GDPR Art. 28, which requires a data processing agreement to stipulate that the processor must assist the controller in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights, which would include the right to rectification**.**

Our detailed mapping of the Global CBPR System Integrity Requirements is available here.

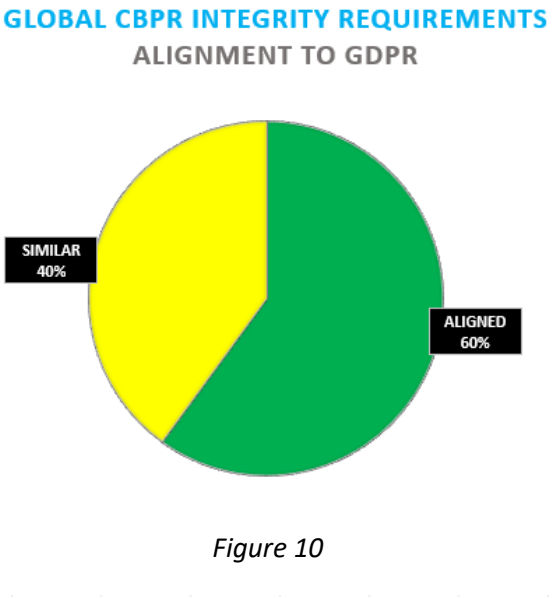

Figure 10

7. Security Safeguards

The Global CBPR System's questions addressing security safeguards seek to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification, or disclosure of information. The GDPR's provisions largely align with the Program Requirements. *[See Figure 11.]*

GDPR Art. 30, read in conjunction with GDPR Art. 32, requires the existence of a written information security policy, and Art. 32 specifically refers to the implementation of security measures "appropriate to the risk." It also provides guidance on assessing the appropriate level of security based on the risks presented.

While the GDPR does not expressly require the training of employees on the importance of maintaining security safeguards, such a requirement could be inferred from GDPR Art. 39—which tasks the DPO with "awareness-raising and training of staff involved in processing operations"—as well as GDPR Art. 32, which requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

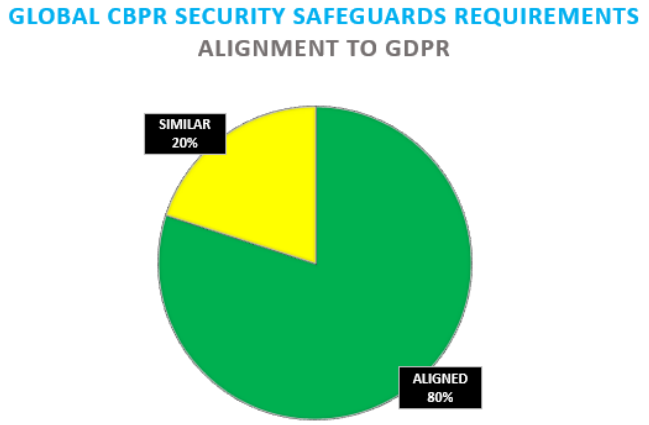

Figure 11

Moreover, the GDPR adopts the storage limitation principle (GDPR Art. 5, para. 1(e)), which requires the erasure (or deletion) of personal data no longer necessary in relation to the purposes for which they were collected or otherwise processed.

Our detailed mapping of the Global CBPR System Security Safeguards Requirements is available here.

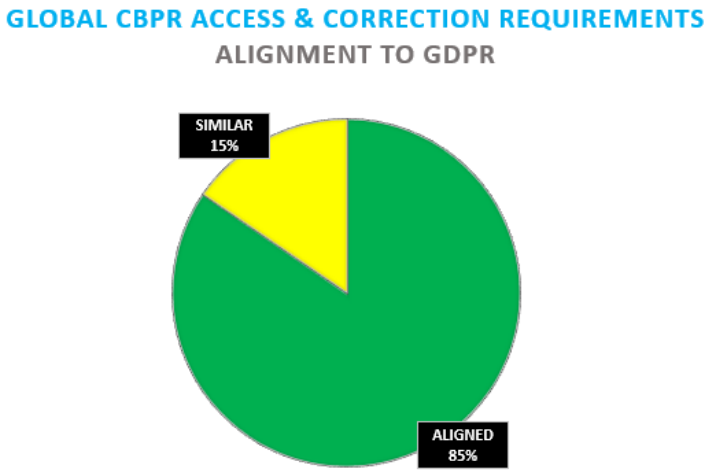

Figure 12

8. Access and Correction

The Global CBPR System's section on access and correction includes specific conditions for what would be considered reasonable in the provision of access. It also recognizes limitations to the rights of access and correction. The GDPR's provisions largely align with the Program Requirements. *[See Figure 12.]*

GDPR Arts. 12, 15 and 16, when read together, require controllers to provide confirmation of whether they hold personal data about one making an access request, and GDPR Art. 12 requires controllers to respond "without undue delay and in any event within one month of receipt of the request." Furthermore, Recital 64 provides that a controller should use all reasonable measures to verify the identity of a data subject who requests access.

While the GDPR does not expressly mandate that information be provided in a way "compatible with the regular form of interaction" with the data subject, such a requirement could be implied by the language of GDPR Art. 12, which requires the controller to communicate in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."

Furthermore, reflecting the Global CBPR's Program Requirements, the GDPR permits data subjects to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted.

While the GDPR does not expressly require controllers to provide data subjects with a copy of the corrected personal data or a confirmation of a correction/deletion, GDPR Art. 12 could be interpreted to require as much, as it requires a controller to "provide information on action taken."

Our detailed mapping of the Global CBPR System Access and Correction Requirements is available here.

9. Accountability

The Global CBPR System seeks to ensure that controllers are accountable for complying with measures that give effect to the Global CBPR Privacy Principles. In particular, they require controllers to take reasonable steps to ensure that personal information remains protected after it is transferred. Generally speaking, the GDPR's provisions are mostly similar to the Program Requirements. *[See Figure 13.]*

While the GDPR is built upon principles of accountability, the principal reason why it does not align more closely with the Global CBPR is because the Global CBPR requires controllers to provide internal complaint and dispute resolution mechanisms for data subjects.

Whereas GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, nothing in the GDPR expressly requires controllers to respond to "privacy-related complaints." Under GDPR Art. 77, complaints are to be brought before the supervisory authority, not the controller. That said, handling disputes internally is arguably implicit in GDPR Art. 12, which mandates the facilitation of data subject rights, and Art. 24, which requires the use of "appropriate organizational measures."

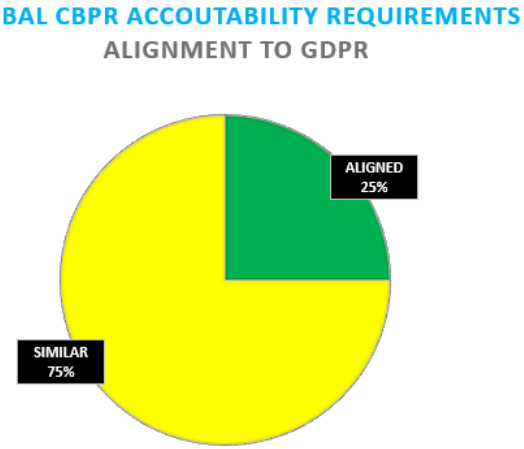

Figure 13

Our detailed mapping of the Global CBPR System Accountability Requirements is available here.

B. Global PRP System Program Requirements

1. Global PRP System Security Safeguards

The Global PRP System requires processors to implement an information security policy that covers personal information processed on behalf of a controller (echoing the Global CBPR System's requirement that controllers implement an information security policy). The GDPR's provisions are largely aligned with these Program Requirements. *[See Figure 14.]*

The GDPR requires the existence of a written information security policy, and Art. 32 specifically requires processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

While the GDPR does not expressly require processers to notify controllers of security incidents, such a requirement could be inferred by the data security provisions of GDPR Art. 32, as well as by GDPR Art. 28, which specifically requires contractors to enter into a contract with processors that, inter alia, ensures that processors take all measures required by Art. 32 (i.e., security safeguards).

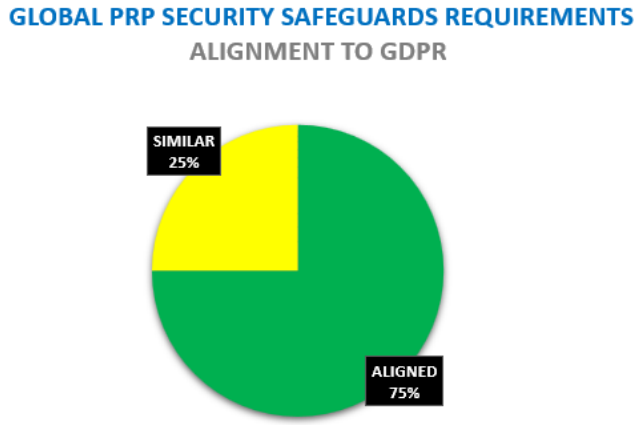

Figure 14

Furthermore, GDPR Art. 28 specifically requires the contract to include a provision stipulating that the processor "deletes or returns all the personal data to the controller after the end of the provision of services relating to processing …."

Our detailed mapping of the Global PRP System Security Safeguards Requirements is available here.

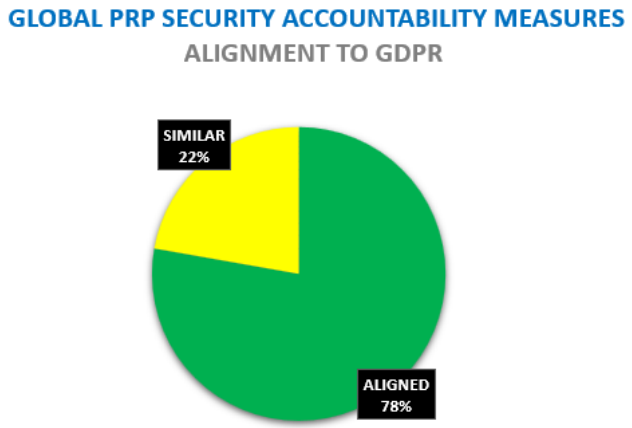

Figure 15

2. Global PRP System Accountability Measures

The Global PRP System generally requires data processors to implement procedures to comply with controllers' instructions and requests. The GDPR's provisions substantially align with these Program Requirements. *[See Figure 15.]*

GDPR Art. 28 specifically requires contractors to enter into a contract with processors, setting forth "the nature and purpose of the processing" and ensuring that the processor processes the personal data "only on documented instructions from the controller."

GDPR Art. 39 further provides that processors shall not process data "except on instructions from the controller."

Notably, a data processing agreement must include provisions stipulating that the processor will fulfill the controller's obligation with regard to data subject requests and will make available to the controller all information necessary to demonstrate compliance.

Our detailed mapping of the Global PRP System Accountability Requirements is available here.

III. CIPL RECOMMENDATIONS

Given that GDPR Art. 42 encourages the "establishment of data protection certification mechanisms … for the purpose of demonstrating compliance with this Regulation," and given that GDPR Art. 46(2)(f) permits the use of an approved certification mechanism as an "appropriate safeguard" for international transfers, **CIPL encourages the EU to explore the benefits of participation the Global CBPR/Global PRP Systems.**

Among other things, our analysis shows:

- **Significant alignment between the GDPR and the Systems' Program Requirements.** More than 70% of Global CBPR Program Requirements, as revised, align with provisions of the GDPR, and more than 75% of the Global PRP do the same. Inasmuch as GDPR provisions could be read to support the remainder of the Program Requirements, EU supervisory authorities would be able to enforce the Program Requirements through the GDPR.

- **The availability of redress mechanisms.** The Global CBPR requires certified organizations to have procedures in place to receive, investigate, and respond to privacy-related complaints. If an issue cannot be resolved by the certified organization in the first instance, redress is available from the Accountability Agent and ultimately, the Privacy Enforcement Authority. As for specific remedies, the Global CBPR Framework provides that member jurisdictions should take into account enforcement powers "which may include rights of individuals to pursue legal action."

- **Mechanisms for responding to government requests.** The Global CBPR goes further than the GDPR by requiring certified organizations to have procedures in place to place for responding to judicial or other government subpoenas, warrants or orders. It also requires organizations to provide the necessary training to employees regarding this subject.

- **Ability to co-exist with existing data transfer mechanisms**. The Global CBPR and Global PRP are purely voluntary, so organizations continue to have the option to rely on adequacy decisions, standard contractual clauses, binding corporate rules, and other transfer mechanisms as needed.

- **No displacement of GDPR.** To the extent GDPR obligations exceed what is expected in the Global CBPR and Global PRP Systems, the full extent of those obligations continues to apply.

It should be noted that 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. **CIPL encourages the EU to apply as an Associate** so that it may participate in Forum activities and in Global Forum Assembly meetings.

Among other things, 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.

In addition, 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. 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.[21]

[21] For additional information regarding benefits and for an overview of how the Systems work, see CIPL's "Global CBPR and Global PRP Systems Playbook," available at https://www.informationpolicycentre.com/resources/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/.

APPENDIX: CIPL MAPPING CHART
Table of Contents

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

Updates to the Program Requirements appear in red text.

PART 1 – MAPPING UPDATED GLOBAL CBPR PROGRAM REQUIREMENTS TO THE EU GDPR

I. PREVENTING HARM (QUESTIONS 1-5)

***Assessment Purpose** – To ensure that the Applicant Organization's personal information protection policies are designed to prevent the misuse of personal information and consequent harm to individuals. This Privacy Principle recognizes that certain categories of personal information, including children's information require more care because of the higher risk of harm that may result from wrongful collection or misuse. It further requires that the Applicant Organization evaluate risks to personal information it collects and to implement remedial measures proportionate to the likelihood and severity of potential harm from misuse. Finally, an Applicant Organization should inform individuals if their personal information has been breached and provide information to enable them to take steps to protect themselves against misuse of their personal information.*

Global_CBPR_1. Take steps to provide safeguards for sensitive PI. **PROGRAM REQUIREMENT QUESTION** ***1. Do you take steps to identify and provide appropriate additional safeguards for personal information that is considered sensitive or categorized to require special protection based on the laws governing your collection or processing of the personal information or where an organization transferring the personal information to you has identified it as such? If YES, describe.*** **ASSESSMENT CRITERIA** The Accountability Agent must verify that the Applicant Organization has written policies and procedures that demonstrate that the Applicant Organization has taken steps to determine whether all or some of the information it collects or receives is considered sensitive or categorized to require	**GDPR Art. 9 – Processing of special categories of personal data** 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. **Paragraph 1 shall not apply if one of the following applies**: (a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;	 The GDPR generally prohibits the processing of sensitive data, but it provides a list of exceptions to the general rule under Art. 9 para. 2. Processing sensitive data pursuant to the constraints of Art. 9 para. 2 mandates an identification and classification of data considered sensitive. Accordingly, the provisions of GDPR Art. 9 reflect the elements of Global CBPR Program Requirement 1. The EU Digital Omnibus Package proposes two additional exemptions to the processing of special categories of data: It would provide for an exemption from the general prohibition on the processing of biometric data, when it is necessary for confirming the identity of the data subject and when the data and means for such verification are under the sole control of that data subject. It would also provide for an exemption for the residual processing of special categories of personal data for development and operation of an AI system or an AI model, subject to certain conditions, including

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
special protection under the law governing the collection, processing or disclosure or whether it processes information transferred from an organization that has identified it as such and to apply the appropriate safeguards to the processing of such information as required. Due to its sensitive nature the safeguards should be applied to information in this category with more care compared to the safeguards applied to other types of personal information. Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle if the Applicant Organization processes sensitive personal information.	(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment and social security and social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the **vital interests of the data subject** or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its **legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body** with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are **manifestly made public by the data subject**;	appropriate organisational and technical measures to avoid collecting special categories of personal data and removing such data.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	(f) processing is necessary for the establishment, **exercise or defence of legal claims** or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to (i) the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; (h) processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; (i) processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the **public interest, scientific or historical research purposes or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. 3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_2. Take steps to assess whether you process children's PI. **PROGRAM REQUIREMENT QUESTION** ***2. Do you take steps to assess whether you collect or process personal information that is considered or categorized as children's personal information based on the laws governing your collection or processing of the personal information?*** **ASSESSMENT CRITERIA** The Accountability Agent must verify that the Applicant Organization has written policies and procedures that enable the Applicant Organization to assess whether it collects, processes or discloses children's personal information as defined under the law governing its collection or processing of the personal information. Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	**GDPR Art. 8 – Conditions applicable to child's consent in relation to information society services** 1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. 2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	To the extent the personal data of children under the age of 16 may be processed on the basis of consent, GDPR Art. 8 para. 1 requires consent to be given by the parent. Abiding by this parental consent requirement necessarily presupposes an assessment of whether the personal data of children is collected or processed pursuant to Global CBPR Program Requirement 2.
Global_CBPR_3. Take steps to verify parental consent or other basis for processing children's PI. **PROGRAM REQUIREMENT QUESTION** ***3. If you do collect or process children's personal information, do you take steps to verify***	**GDPR Art. 8 –Conditions applicable to child's consent in relation to information society services** 1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the	GDPR Art. 8 mirrors the elements of Global CBPR Program Requirement 3.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
parental consent where appropriate, or other appropriate legal basis for the collection and processing of personal information that is considered children's personal information based on the laws governing your collection or processing of the personal information or where an organization transferring the personal information to you has identified it as such? **ASSESSMENT CRITERIA** The Accountability Agent must verify that the Applicant Organization provides a description of the mechanism provided to verify parental consent or other appropriate legal basis for the collection if the Applicant Organization processes children's personal information. Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle if the Applicant Organization processes children's personal information.	child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. 2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	
Global_CBPR_4. Have procedures in place to identify and assess risk of misuse of PI. **PROGRAM REQUIREMENT QUESTION** ***4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your***	**GDPR Art. 24 – Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the **risks of varying likelihood and severity** for the rights and freedoms of natural persons, the controller shall implement **appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is	🟢 The risk-based approach is a foundational concept of the GDPR, and the legal requirement to assess risk is explicit and implicit in many GDPR provisions, including Arts. 24 and 35. Those requirements reflect the intent of Global CBPR Program Requirement 4. Significantly, Art. 24 para. 3 explicitly states that "**adherence to … approved**

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm? **ASSESSMENT CRITERIA** The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary. Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.	performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or **approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller**. **GDPR Art. 35 – Data protection impact assessment** 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out **an assessment of the impact of the envisaged processing operations on the protection of personal data**. A single assessment may address a set of similar processing operations that present similar high risks. 2. The controller shall seek the advice of the data protection officer, where designated, when	**certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller."** The Global CBPR could therefore be an approved certification mechanism under the GDPR.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	carrying out a data protection impact assessment. 3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale. 4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68. 5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	authority shall communicate those lists to the Board. 6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union. 7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	and legitimate interests of data subjects and other persons concerned. 8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment. 9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. 10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities. 11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	assessment at least when there is a change of the risk represented by processing operations.	
Global_CBPR_5. Establish breach notification protocols. **PROGRAM REQUIREMENT QUESTION** ***5. Do you have a process in place to notify affected individuals without unreasonable delay if a breach is likely to result in significant harm to the affected individuals after confirming the loss, unauthorized access, destruction, use, modification or disclosure of information or other misuses of personal information? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers YES, the Accountability Agent must verify that the Applicant Organization has written policies and procedures to notify affected individuals without unreasonable delay. Notifications to affected individuals should include information about the nature and extent of the breach and the types of information involved; steps affected individuals may take to protect themselves from potential harm; a brief description of what the Applicant Organization is doing to investigate the breach, mitigate the harm, and prevent further breaches; and contact information for the privacy personnel at the Applicant Organization.	**GDPR Art. 34 – Communication of a personal data breach to the data subject** 1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3). 3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects	🟢 GDPR Art. 34 mirrors the elements of Global CBPR Program Requirement 5, as it requires notification of a personal data breach to the data subject.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such policies and procedures is required for compliance with this Privacy Principle.	referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. 4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	

II. NOTICE (QUESTIONS 6-9)

Assessment Purpose *– To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. The list of acceptable Qualifications to the Provision of Notice is below.*

QUALIFICATIONS TO THE PROVISION OF NOTICE

The following are situations in which the application at the time of collection of the Global CBPR Notice Principle may not be necessary or practical.

i. ***Obviousness****: PI controllers do not need to provide notice of the collection, use or third-party sharing of PI in those circumstances where consent by the individual can be inferred from the provision of the individual's information (e.g., if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information).*

ii. ***Collection of publicly-available information****: PI controllers do not need to provide notice regarding the collection and use of publicly available information.*

iii. ***Technological impracticability:*** *PI controllers do not need to provide notice at or before the time of collection in those cases where electronic technology automatically collects information when a prospective customer initiates contact (e.g., through the use of cookies). However, the notice should be provided to the individuals as soon after as is practicable.*

iv. ***Disclosure to a government institution which has made a request for the information with lawful authority****: PI controllers do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation.*

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
v. ***Disclosure to a third party pursuant to a lawful form of process:*** *PI controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.* *vi.* ***Third-party receipt:*** *Where PI is received from a third party, the recipient PI controller does not need to provide notice to the individuals at or before the time of collection of the information.* *vii.* ***For legitimate investigation purposes:*** *When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.* *viii.* ***Action in the event of an emergency****: PI controllers do not need to provide notice in emergency situations that threaten the life, health or security of an individual.*		
Global_CBPR_6. Provide a clear easily accessible privacy statement about your data collection practices and policies. **PROGRAM REQUIREMENT QUESTION** ***6. Do you provide clear and easily accessible statements about your practices and policies that govern the PI described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.*** **ASSESSMENT CRITERIA** If **YES,** the AA must verify that the Applicant Organization's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant Organization's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified);	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. **The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.** When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * * **GDPR Art. 13 – Information to be provided where personal data are collected from the data subject**	🟢 GDPR Arts. 12 - 14 generally mirror the elements of Global CBPR Program Requirement 6. GDPR Art. 12 para. 1 specifically requires controllers to provide notice of processing activities "in a concise, transparent, intelligible and easily accessible form …." Moreover, it requires the information to be "provided in writing, or by other means, including, where appropriate, by electronic means." While the GDPR does not expressly require a privacy statement to include an effective date of publication (as mentioned in the Global CBPR's Assessment Criteria), that requirement could be inferred by the GDPR's terms "concise" and "transparent."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
• Is in accordance with the principles of the Global CBPR Framework; • Is easy to find and accessible; • Applies to all PI; whether collected online or offline; and • States an effective date of Privacy Statement publication. Where Applicant Organization answers **NO to question 1**, and does not identify an applicable Qualification [listed here], the AA must inform the Applicant Organization that Notice as described herein is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	* * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	of them or where they have been made available. * * *	
Global_CBPR_6a. Your privacy statement should describe how your organization collects PI. **PROGRAM REQUIREMENT QUESTION** ***6.a. Does this privacy statement describe how PI is collected?*** **ASSESSMENT CRITERIA** If **YES**, the AA must verify that: • the statement describes the collection practices and policies applied to all covered PI collected by the Applicant Organization. • the Privacy Statement indicates what types of PI, whether collected directly or through a third party or agent, is collected, and • the Privacy Statement reports the categories or specific sources of all categories of PI collected. If **NO**, the AA must inform the Applicant Organization that Notice as described herein is required for compliance with this Privacy Principle.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers	While the GDPR does not expressly require a privacy statement to describe ***how*** PI is collected, the language of GDPR Art 13 – "[w]here personal data relating to a data subject are collected from the data subject" – implies ***how*** it is collected, i.e., "from the data subject." Similarly, the language of GDPR Art 14—"[w]here personal data have not been obtained from the data subject—also implies ***how*** it is collected, i.e., "*not* from the data subject."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. * * *	
Global_CBPR_6b. Your privacy statement should describe the purpose(s) for which PI is collected. **PROGRAM REQUIREMENT QUESTION** ***6.b. Does this privacy statement describe the purpose(s) for which PI is collected?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides notice to individuals of the purpose for which PI is being collected. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification [listed here], the AA must notify the Applicant Organization that notice of the purposes for which PI is collected is required and must be included in their Privacy Statement. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (c) **the purposes of the processing for which the personal data are intended** as well as the legal basis for the processing; * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	🟢 GDPR Art. 13, para. 1(c) and GDPR Art. 14, para. 1(c) mirror the elements of Global CBPR Program Requirement 6b, as they specifically require the controller to provide information regarding the intended purposes of the processing at the time of collection.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	* * * (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; * * *	
Global_CBPR_6c. Your privacy statement should Inform individuals as to whether and for what purpose(s) PI is made available to third parties. **PROGRAM REQUIREMENT QUESTION** ***6.c. Does this privacy statement inform individuals whether their PI is made available to third parties and for what purpose?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization notifies individuals that their PI will or may be made available to third parties, **identifies the categories or specific third parties, and the purpose for which the PI will or may be made available.** Where the Applicant Organization answers **NO** and does not identify an applicable Qualification [listed here], the AA must notify the Applicant Organization that notice that PI will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant Organization identifies an applicable Qualification,	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; * * * (e) the recipients or categories of recipients of the personal data, if any; * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: * * *	When para. 1(c) of GDPR Art. 13 (and para. 1(c) of GDPR Art. 14) is read together with corresponding para. 1(e), the GDPR appears to mirror the Global CBPR Program Requirement 6c, as it requires the controller to provide information regarding the intended purposes as well as any intended "recipients or categories of recipients" of the data.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the AA must verify whether the applicable Qualification is justified.	(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; * * * (e) the recipients or categories of recipients of the personal data, if any; * * *	
Global_CBPR_6d. Your privacy statement should disclose your company's name and location, and how individuals can contact you about your data collection practices. **PROGRAM REQUIREMENT QUESTION** ***6.d. Does this privacy statement disclose the name of the Applicant Organization's company and location, including contact information regarding practices and handling of PI upon collection? Where YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides name, address and a **functional** e-mail address. Where the Applicant Organization answers NO and does not identify an applicable Qualification [listed here], the AA must inform the Applicant Organization that such disclosure of information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:	GDPR Arts. 13 and 14 reflect the elements of Global CBPR Program Requirement 6d, as they state that the controller must provide: "the identity and the contact details of the controller and, where applicable, of the controller's representative." While "location" is not explicitly stated, "contact details" could be interpreted to include a physical address.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
applicable Qualification, the AA must verify whether the applicable Qualification is justified.	(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; * * *	
Global_CBPR_6e. Your privacy statement should provide information regarding the use and disclosure of PI. **PROGRAM REQUIREMENT QUESTION** ***6.e. Does this privacy statement provide information regarding the use and disclosure of an individual's PI?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization's Privacy Statement includes, if applicable, information regarding the use and disclosure of all PI collected. Refer to question 8 for guidance on permissible uses of PI. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification [listed here], the AA must inform the Applicant Organization, that such information is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. * * *	🟢 GDPR Arts. 13 and 14 reflect the elements of Global CBPR Program Requirement 6e, as subsections (1)(e) and (1)(f) of both Articles require disclosure of "the recipients or categories of recipients of the personal data" as well as "the fact that the controller intends to transfer personal data to a third country or international organization…."

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available. * * *	
Global_CBPR_6f. Your privacy statement should provide information regarding whether and how individuals can access and correct PI. **PROGRAM REQUIREMENT QUESTION**	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent,	🟢 GDPR Arts. 12, 15 and 16, when read together, reflect the elements of Global CBPR Program Requirement 6f.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
6.f. Does this privacy statement provide information regarding whether and how an individual can access and correct their PI? **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Privacy Statement includes: • The process through which the individual may access his or her PI (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her PI Where the Applicant Organization answers **NO** and does not identify an applicable Qualification [listed here], the AA must inform the Applicant Organization that providing information about access and correction, including the Applicant Organization's typical response times for access and correction requests, is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 15 – Right of access by the data subject** 1. The data subject shall have the right to obtain from the controller confirmation as to **whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data** and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) **the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;** (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. * * * **GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	personal data completed, including by means of providing a supplementary statement.	
Global_CBPR_7. Provide notice at the time of collection that you (or others on your behalf) are collecting PI. **PROGRAM REQUIREMENT QUESTION** ***7. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides notice to individuals that their PI is being (or, if not practicable, has been) collected **and that the notice is reasonably available to individuals**. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the notice that PI is being collected is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, **at the time when personal data are obtained**, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the	🟢 GDPR Art. 13 expressly provides that notice must be provided "at the time when personal data are obtained," thereby reflecting the elements of Global CBPR Program Requirement 7.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. * * *	
Global_CBPR_8. Provide notice at the time of collection of the purpose(s) for collecting PI. **PROGRAM REQUIREMENT QUESTION** ***8. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which PI is being collected?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization explains to individuals the purposes for which PI is being collected. The purposes must be communicated orally or in writing, for example on the Applicant Organization's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant Organization answers NO and does not identify an applicable Qualification, the AA must inform the Applicant Organization of the need to provide notice to individuals of the purposes for which PI is being collected. Where the	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, **at the time when personal data are obtained**, provide the data subject with all of the following information: * * * (c) the **purposes of the processing** for which the personal data are intended as well as the legal basis for the processing; * * *	GDPR Art. 13, para 1(c) provides that the purposes of the processing be provided at the time of collection, thereby reflecting the elements of Global CBPR Program Requirement 8.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.		
Global_CBPR_9. Provide notice at the time of collection that PI may be shared with third parties. **PROGRAM REQUIREMENT QUESTION** ***9. Subject to the Qualifications [listed here], at the time of collection of PI, do you notify individuals that their PI may be shared with third parties?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides notice to individuals that their PI will be or may be shared with third parties and for what purposes. Where the Applicant Organization answers NO and does not identify an applicable Qualification, the AA must inform the Applicant Organization to provide notice to individuals that the PI collected may be shared with third parties. Where the Applicant Organization identifies an applicable Qualification, the AA must determine whether the applicable Qualification is justified.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, **at the time when personal data are obtained**, provide the data subject with all of the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. * * *	GDPR Art. 13, para 1(e) and 1(f) provide that, at the time of collection, the controller must provide information regarding recipients and potential cross-border transfers of personal information, thereby reflecting the elements of Global CBPR Program Requirement 9.

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different

Updates to the Program Requirements appear in red text.

III. COLLECTION LIMITATION (QUESTIONS 10-12)

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.*

Global_CBPR_10. Explain whether you collect PI directly from individuals, from third parties acting on your behalf, or in other ways.

PROGRAM REQUIREMENT QUESTION

10. How do you obtain PI:

10.a. Directly from the individual?

10.b. From third parties collecting on your behalf?

10.c. Other. If YES, describe.

ASSESSMENT CRITERIA

The AA must verify that the Applicant Organization indicates from whom they obtain PI.

Where the Applicant Organization answers **YES to any of these sub-parts**, the AA must verify the Applicant Organization's practices in this regard.

There should be at least one 'yes' answer to these three questions. If not, the AA must inform the Applicant Organization that it has incorrectly completed the questionnaire.

GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. **The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.** When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

* * *

GDPR Art. 13 – Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data

🟢

GDPR Arts. 12 – 14, when read together, reflect the elements of Global CBPR Program Requirement 10, inasmuch as GDPR Art 13 governs collection directly from the data subject and GDPR 14 governs collection from persons other than the data subject. In both circumstances, the GDPR specifically requires providing information of the identity and the contact details "of the **controller's representative**," i.e., a third party collecting on the controller's behalf.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. * * *	

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	* * *	
Global_CBPR_11. Limit your collection to PI that is relevant to fulfill your stated purpose(s) or to other compatible or related purposes. **PROGRAM REQUIREMENT QUESTION** ***11. Do you limit your PI collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES** and indicates it only collects PI which is relevant to the identified collection purpose or other compatible or related purposes, the AA must require the Applicant Organization to identify: • Each type of data collected; • The corresponding stated purpose of collection for each; • All uses that apply to each type of data; and • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection Using the above, the AA will verify that the Applicant Organization limits the amount and type of PI to that which is relevant to fulfill the stated purposes.	**GDPR Art. 5 – Principles relating to processing of personal data** 1. Personal data shall be: * * * (b) collected for **specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); * * *	🟢 GDPR Art. 5, para. 1(b) expresses the purpose limitation principle conveyed in Global CBPR Program Requirement 11.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that it must limit the use of collected PI to those uses that are relevant to fulfilling the purpose(s) for which it is collected.		
Global_CBPR_12. Collect PI (whether directly or through the use of third parties) only by lawful and fair means. **PROGRAM REQUIREMENT QUESTION** ***12. Do you collect PI (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such PI? Where YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES,** the AA must require the Applicant Organization to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such PI and that it is collecting information by fair means, without deception. Where the Applicant Organization Answers **NO**, the AA must inform that Applicant Organization that lawful and fair procedures are required for compliance with this Privacy Principle.	**GDPR Art. 5 -- Principles relating to processing of personal data** 1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); * * *	● GDPR Art. 5, para. 1(a) expresses the fairness principle conveyed in Global CBPR Program Requirement 12.

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

Updates to the Program Requirements appear in red text.

IV. USES OF PERSONAL INFORMATION (QUESTIONS 13-18)

Assessment Purpose - Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Privacy Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or the use of information collected by an Applicant Organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that Applicant Organization.

Global_CBPR_13. Limit the use of PI to the purposes identified in your privacy statement or notice at collection, or to other compatible or related purposes.

PROGRAM REQUIREMENT QUESTION

13. Do you limit the use of the PI you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.

ASSESSMENT CRITERIA

Where the Applicant Organization answers **YES**, the AA must verify the existence of written policies and procedures to ensure that all covered PI collected either directly or indirectly through an agent is done so in accordance with the purposes for which

GDPR Art. 5 -- Principles relating to processing of personal data

1. Personal data shall be:

* * *

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

* * *

GDPR Art. 5, para. 1(b) expresses the purpose limitation principle conveyed in Global CBPR Program Requirement 13.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the information was collected as identified in the Applicant Organization's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Organization Answers **NO**, the AA must consider answers to Question 14 below.		
Global_CBPR_14. Obtain consent or specify legal obligation for use of PI unrelated to the purposes of collection. **PROGRAM REQUIREMENT QUESTION** ***14. If you answered NO, do you use the PI you collect for unrelated purposes under one of the following circumstances? Describe below.*** ***14.a. Based on express consent of the individual?*** ***14.b. Compelled by applicable laws?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **NO** to question 13, the Applicant Organization must clarify under what circumstances it uses PI for purposes unrelated to the purposes of collection and specify those purposes. Where the Applicant Organization selects 14a, the AA must require the Applicant Organization to provide a description of how such consent was obtained, and the AA must verify that the Applicant Organization's use of the PI is based on express consent of the individual (14.a), such as: • Online at point of collection • Via e-mail	**GDPR Art. 6 -- Lawfulness of processing** 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where	● GDPR Art. 6, para. 1 lists the lawful bases for processing, which includes consent under subsection 1(a) and legal obligation under 1(c). GDPR Art. 6, para. 4—which addresses circumstances where processing is for a purpose "other than that for which the personal data have been collected"—lists factors for a controller to assess in order to determine whether a new purpose is compatible with the purpose for which the personal information was initially collected.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant Organization answers 14.a, the AA must require the Applicant Organization to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 23-25 below. Where the Applicant Organization selects 14.b, the AA must require the Applicant Organization to provide a description of how the collected PI may be shared, used or disclosed as compelled by law. Where the Applicant Organization does not answer 14.a or 14.b, the AA must inform the Applicant Organization that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this Privacy Principle.	such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * * 4. Where the processing for a **purpose other than that for which the personal data have been collected** is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	
Global_CBPR_15. Describe whether you disclose the PI you collect to other controllers. **PROGRAM REQUIREMENT QUESTION** ***15. Do you disclose PI you collect (whether directly or through the use of third parties acting on your behalf) to other PI controllers? If YES, describe.*** **ASSESSMENT CRITERIA*** *[*Global_CBPR_15, Global_CBPR_16, and Global_CBPR_17 use the same Assessment Criteria.]* Where the Applicant Organization answers **YES** in questions 15 and 16, the AA must verify that if PI is disclosed to other PI controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: * * * (e) the recipients or categories of recipients of the personal data, if any;	Given that para. 1(e) under GDPR Arts. 13 and 14 requires a controller to disclose "the recipients or categories of recipients of the personal data," these provisions could be read to infer a requirement to state whether those recipients are other controllers.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Also, the AA must require the Applicant Organization to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g., order fulfillment etc.). Using the above, the AA must verify that the Applicant Organization's disclosures or transfers of all PI is limited to the purpose(s) of collection, or compatible or related purposes.	* * *	
Global_CBPR_16. Describe whether you disclose the PI you collect to processors. **PROGRAM REQUIREMENT QUESTION** ***16. Do you transfer PI to PI processors? If YES, describe.*** **ASSESSMENT CRITERIA*** *[*Global_CBPR_15, Global_CBPR_16, and Global_CBPR_17 use the same Assessment Criteria.]* Where the Applicant Organization answers **YES** in questions 15 and 16, the AA must verify that if PI is disclosed to other PI controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; * * * **GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall	Given that para. 1(e) under GDPR Arts. 13 and 14 requires a controller to disclose "the recipients or categories of recipients of the personal data," these provisions could be read to infer a requirement to state whether those recipients are processors.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
Also, the AA must require the Applicant Organization to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g., order fulfillment etc.). Using the above, the AA must verify that the Applicant Organization's disclosures or transfers of all PI is limited to the purpose(s) of collection, or compatible or related purposes.	provide the data subject with the following information: * * * (e) the recipients or categories of recipients of the personal data, if any; * * *	
Global_CBPR_17. If you disclose PI to other controllers or processors, describe whether such disclosure fulfills the original or another compatible or related purpose of the collection. **PROGRAM REQUIREMENT QUESTION** ***17. If you answered YES to question 15 and/or question 16, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.*** **ASSESSMENT CRITERIA*** *[*Global_CBPR_15, Global_CBPR_16, and Global_CBPR_17 use the same Assessment Criteria.]* Where the Applicant Organization answers **YES** in questions 15 and 16, the AA must verify that if PI is disclosed to other PI controllers or transferred to processors, such disclosure and/or transfer must be	**GDPR Art. 13 – Information to be provided where personal data are collected from the data subject** 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: * * * (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; * * * (e) the recipients or categories of recipients of the personal data, if any; * * *	🟡 Where para. 1(c) is read in conjunction with para. 1(e) under GDPR Arts. 13 and 14, these provisions could be read to infer a requirement to state the purposes for sharing with other controllers or processors.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the AA must require the Applicant Organization to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g., order fulfillment etc.). Using the above, the AA must verify that the Applicant Organization's disclosures or transfers of all PI is limited to the purpose(s) of collection, or compatible or related purposes.	**GDPR Art. 14 –Information to be provided where personal data have not been obtained from the data subject** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: * * * (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; * * * (e) the recipients or categories of recipients of the personal data, if any; * * *	
Global_CBPR_18. If you disclose PI to other controllers or processors for a purpose unrelated to the original purpose, describe whether such disclosure is based on consent, is necessary to provide a product or service, or is compelled by law. **PROGRAM REQUIREMENT QUESTION** ***18. If you answered NO to question 17 or if otherwise appropriate, does the disclosure***	**GDPR Art. 6 -- Lawfulness of processing** 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	🟢 GDPR Art. 6, para. 1 lists the lawful bases for processing, which includes consent under subsection 1(a) and legal obligation under 1(c). GDPR Art. 6, para. 4—which addresses circumstances where processing is for a purpose "other than that for which the personal data have been collected"—lists factors for a controller to assess in order to determine whether a new purpose is compatible with the purpose for which the personal information was initially collected.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
and/or transfer take place under one of the following circumstances? ***18.a. Based on express consent of the individual?*** ***18.b. Necessary to provide a service or product requested by the individual?*** ***18.c. Compelled by applicable laws?*** **ASSESSMENT CRITERIA** Where [the] Applicant Organization answers **NO** to question 18, the Applicant Organization must clarify under what circumstances it discloses or transfers PI for unrelated purposes, specify those purposes. Where the Applicant Organization answers **YES** to 18.a., the AA must require the Applicant Organization to provide a description of how individual's provide consent to having their PI disclosed and/or transferred for an unrelated use, such as: • Online at point of collection; • Via e-mail; • Via preference/profile page; • Via telephone; • Via postal mail; or • Other (in case, specify). Where the Applicant Organization answers **YES** to 18.b., the AA must require the Applicant Organization to provide a description of how the disclosure and/or transfer of collected PI is necessary to provide a service or product requested by the individual. The AA must verify that the	(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * * 4. Where the processing for a **purpose other than that for which the personal data have been collected** is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant Organization answers **YES** to 18.c., the AA must require the Applicant Organization to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant Organization must also outline the legal requirements under which it is compelled to share the PI, unless the Applicant Organization is bound by confidentiality requirements. The AA must verify the existence and applicability of the legal requirement. Where the Applicant Organization answers NO to 18.a., b. and c., the AA must inform the Applicant Organization that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this Privacy Principle.	(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

Updates to the Program Requirements appear in red text.

V. CHOICE (QUESTIONS 19-27)

***Assessment Purpose** - Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Privacy Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in the Qualifications to the Provision of Choice Mechanisms listed below.*

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the Global CBPR Choice Principle may not be necessary or practical.

i. ***Obviousness:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information.*

ii. ***Collection of Publicly-Available Information:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the collection and use of publicly available information.*

iii. ***Technological Impracticability:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in relation to those cases where electronic technology automatically collects information when a prospective customer initiates contact [e.g., use of cookies]. However, a mechanism to exercise choice as to use and disclosure should be provided after collection of the information.*

iv. ***Third-Party Receipt:** Where personal information is received from a third party, the recipient personal information controller does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if the personal information controller engages a third party to collect personal information on its behalf, the personal information controller should instruct the collector to provide such choice when collecting the personal information.*

v. ***Disclosure to a government institution which has made a request for the information with lawful authority:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.*

vi. ***Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.*

vii. ***For legitimate investigation purposes:** When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.*

viii. ***Action in the event of an emergency:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.*

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_CBPR_19. Provide a mechanism for individuals to exercise choice in relation to the collection of their PI and describe how it works. **PROGRAM REQUIREMENT QUESTION** ***19. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the collection of their PI? Where YES describe such mechanisms below.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their PI, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The AA must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and the AA must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not	**GDPR Art. 4 – Definitions** * * * (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as **collection**, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; * * * **GDPR Art. 6 -- Lawfulness of processing** 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the	🟢 GDPR Art. 4, para. 2 defines "processing" as including collection. GDPR Art. 6, para. 1 lists the lawful bases for processing, which includes consent under subsection 1(a). It therefore provides a mechanism for individuals to exercise choice in relation to the collection of their PI, as mentioned in Global Program Requirement 19. GDPR Art. 4, para. 11 defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes. GDPR Art. 7, para. 1 provides that where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. With the exception of legitimate interest (GDPR Art. 6, para. 1(f)), the other legal bases for processing—i.e., those not based on consent—arguably fall within the Global CBPR System's Qualifications to the Provision of Choice Mechanisms: • Art. 6, para. 1(b): Performance of a contract … ***Obviousness*** • Art. 6, para. 1(c): Compliance with legal obligation … ***Disclosure pursuant to lawful form of process*** • Art. 6, para. 1(d): Protect vital interests … ***Action in the event of an emergency***

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
identify an applicable Qualification the AA must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to the collection of their PI must be provided.	data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * * **GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also	• Art. 6, para. 1(e): Public interests … ****Disclosure to a government institution* and/or *Action in the event of an emergency****

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	
Global_CBPR_20. Provide a mechanism for individuals to exercise choice in relation to the use of their PI and describe how it works. **PROGRAM REQUIREMENT QUESTION** ***20. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the use of their***	**GDPR Art. 4 – Definitions** * * * (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, **use**, disclosure by transmission, dissemination	🟢 GDPR Art. 4, para. 2 defines "processing" as including use. GDPR Art. 6, para. 1 lists the lawful bases for processing, which includes consent under subsection 1(a). It therefore provides a mechanism for individuals to exercise choice in relation to the

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
PI? Where YES describe such mechanisms below. **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their PI, such as: Online at point of collection • Via e-mail; • Via preference/profile page; • Via telephone; • Via postal mail; or • Other (in case, specify). The AA must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the Qualifications [listed here], the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of PI. Subject to the Qualifications [listed here], the opportunity to exercise choice may be provided to the individual after collection, but before:] • being able to make use of the PI, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • PI may be disclosed or distributed to third parties, other than Service Providers.	or otherwise making available, alignment or combination, restriction, erasure or destruction; * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; * * * **GDPR Art. 6 -- Lawfulness of processing** 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;	use of their PI, as mentioned in Global Program Requirement 20. GDPR Art. 4, para. 11 defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes. GDPR Art. 7, para. 1 provides that where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where the Applicant Organization answers **NO**, the Applicant Organization must identify the applicable Qualification to the provision of choice, and provide a description and the AA must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an acceptable Qualification, the AA must inform the Applicant Organization a mechanism for individuals to exercise choice in relation to the use of their PI must be provided.	(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * * **GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** = **Aligned;** = **Similar;** = **Different**
	withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	
Global_CBPR_21. Provide a mechanism for individuals to exercise choice in relation to the disclosure of their PI and describe how it works. **PROGRAM REQUIREMENT QUESTION** ***21. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their PI? Where YES describe such mechanisms below.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization provides a description of how individuals may exercise choice in relation to the disclosure of their PI, such as: • Online at point of collection;	**GDPR Art. 4 – Definitions** * * * (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, **disclosure** by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies	GDPR Art. 4, para. 2 defines "processing" as including disclosure. GDPR Art. 6, para. 1 lists the lawful bases for processing, which includes consent under subsection 1(a). It therefore provides a mechanism for individuals to exercise choice in relation to the disclosure of their PI, as mentioned in Global Program Requirement 21. GDPR Art. 4, para. 11 defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes. GDPR Art. 7, para. 1 provides that where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
• Via e-mail; • Via preference/profile page; • Via telephone; • Via postal mail; or • Other (in case, specify). The AA must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the Qualifications [listed here], the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of PI. Subject to the Qualifications [listed here], the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the PI to third parties, other than Service Providers, for a purpose that is not related or when the AA finds that the Applicant Organization's choice mechanism is not displayed in a clear and conspicuous manner , or compatible with that for which the information was collected.] Where the Applicant Organization answers **NO**, the Applicant Organization must identify the applicable Qualification and provide a description and the AA must verify whether the applicable Qualification is justified. Where the Applicant Organization answers **NO** and does not identify an acceptable Qualification, the AA must inform the Applicant Organization that a mechanism for individuals to exercise choice in	agreement to the processing of personal data relating to him or her; * * * **GDPR Art. 6 -- Lawfulness of processing** 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a **legal obligation** to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
relation to the disclosure of their PI must be provided.	freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * * **GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	
Global_CBPR_22. Provide choice mechanisms regarding direct marketing. **PROGRAM REQUIREMENT QUESTION** ***22. As applicable, do you permit individuals to exercise choice in relation to receiving direct marketing at any time? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers YES, the AA must verify that the Applicant Organization provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to receiving direct marketing if applicable. The AA must verify that a mechanism is in place and operational if applicable. Where an Applicant Organization answers NO, the AA must inform the Applicant Organization that a mechanism for individuals to exercise choice in relation to receiving direct marketing must be provided if they are engaging in direct marketing.	**GDPR Art. 21 -- Right to object** 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. 2. **Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing**, which includes profiling to the extent that it is related to such direct marketing. 3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. 4. At the latest **at the time of the first communication with the data subject**, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data	GDPR Art. 21, para. 2 specifically grants individuals the right to object at any time to the processing of personal data for direct marketing "at any time." GDPR Art. 21, para. 4 further clarifies that the right to object shall "at the time of the first communication with the data subject" be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. Read together, these two provisions would permit individuals to exercise choice in relation to receiving direct marketing at any time, thereby reflecting the elements of Global CBPR Program Requirement 22.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	subject and shall be presented clearly and separately from any other information. 5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications. 6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.	
Global_CBPR_23. Provide choice mechanisms (offering individuals the ability to limit the collection, use, and disclosure of their PI) in clear and conspicuous manner. **PROGRAM REQUIREMENT QUESTION** ***23. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or disclosure (question 21) of their PI, are they displayed or provided in a clear and conspicuous manner?*** **ASSESSMENT CRITERIA**	**GDPR Art. 4 – Definitions** * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; * * * **GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to demonstrate that the	● GDPR Art. 4, para. 11, defines consent as being "freely given, specific, informed and unambiguous." GDPR Art. 7, para. 4, further provides that a request for consent be presented in a manner that is "clearly distinguishable from the other matters, **in an intelligible and easily accessible form, using clear and plain language**." GDPR Art. 12, para. 1, generally requires a controller to convey information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant Organization answers **NO**, or when the AA finds that the Applicant Organization's choice mechanism is not displayed in a clear and conspicuous manner, the AA must inform the Applicant Organization that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their PI, must be clear and conspicuous in order to comply with this Privacy Principle.	data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, **using clear and plain language**. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. **GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject**	

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject **in a concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * *	
Global_CBPR_24. Provide choice mechanisms (offering individuals the ability to limit the collection, use, and disclosure of their PI) that are clearly worded and understandable. **PROGRAM REQUIREMENT QUESTION** ***24. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or disclosure (question 21) of their PI, are they clearly worded and easily understandable?*** **ASSESSMENT CRITERIA**	**GDPR Art. 4 – Definitions** * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; * * * **GDPR Art. 7 – Conditions for consent**	🟢 GDPR Art. 4, para. 11, defines consent as being "freely given, specific, informed and unambiguous." GDPR Art. 7, para. 4, further provides that a request for consent be presented in a manner that is "clearly distinguishable from the other matters, **in an intelligible and easily accessible form, using clear and plain language**." GDPR Art. 12, para. 1, generally requires a controller to convey information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization's choice mechanism is clearly worded and easily understandable. Where the Applicant Organization answers **NO**, and/or when the AA finds that the Applicant Organization's choice mechanism is not clearly worded and easily understandable, the AA must inform the Applicant Organization that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their PI, must be clearly worded and easily understandable in order to comply with this Privacy Principle.	1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, **using clear and plain language**. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject **in a concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * *	
Global_CBPR_25. Provide choice mechanisms (offering individuals the ability to limit the collection, use, and disclosure of their PI) that are easily accessible and affordable. **PROGRAM REQUIREMENT QUESTION** ***25. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or disclosure (question 21) of their PI, are these***	**GDPR Art. 4 – Definitions** * * * (11) 'consent' of the data subject means any **freely given, specific, informed and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; * * *	🟢 GDPR Art. 4, para. 11, defines consent as being "freely given, specific, informed and unambiguous." GDPR Art. 7, para. 4, further provides that a request for consent be presented in a manner that is "clearly distinguishable from the other matters, **in an intelligible and easily accessible form, using clear and plain language**." GDPR Art. 12, para. 1, generally requires a controller to convey information "in a concise,

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
choices easily accessible and affordable? Where YES, describe. **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization's choice mechanism is easily accessible and affordable. Where the Applicant Organization answers **NO**, or when the AA finds that the Applicant Organization's choice mechanism is not easily accessible and affordable, the AA must inform the Applicant Organization that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their PI, must be easily accessible and affordable in order to comply with this Privacy Principle.	**GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, **using clear and plain language**. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	transparent, intelligible and easily accessible form, using clear and plain language." GDPR Art. 12, para. 5, requires a controller to provide actions related to data subject rights **free of charge**.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject **in a concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * * 5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided **free of charge**. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. * * *	
Global_CBPR_26. Ensure that choice mechanisms (offering individuals the ability to limit the collection, use, and disclosure of their PI) are honored in effective and expeditious manner. **PROGRAM REQUIREMENT QUESTION** ***26. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.*** **ASSESSMENT CRITERIA** Where the Applicant Organization does have mechanisms in place, the AA must require the Applicant Organization to provide ~~of~~ the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 19, 20 and 21) are recorded and honored. Where the Applicant Organization does not have mechanisms in place, the Applicant Organization must identify the applicable Qualification to the provision of choice and provide a description and	**GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a	● GDPR Art. 12, para. 3, generally requires a controller take actions related to data subject rights "**without undue delay and in any event within one month of receipt of the request**." To the extent the Assessment Criteria of Global CBPR Program Requirement 26 requires that preferences expressed through choice mechanisms be **recorded**, GDPR Art. 30 requires a controller to maintain a record of processing activities. GDPR Art. 7, para. 1, further provides that where processing is based on consent, the controller must be able to **demonstrate** that the data subject has consented to processing of his or her personal data.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the AA must verify whether the applicable Qualification is justified. Where the Applicant Organization answers NO and does not provide an acceptable Qualification, the AA must inform the Applicant Organization that a mechanism to ensure that choices, when offered, can be honored, must be provided.	contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. **GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt of the request**. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. 4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	supervisory authority and seeking a judicial remedy. * * * **GDPR Art. 30 -- Records of processing activities** 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	(f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). * * *	
Global_CBPR_27. Permit individuals to withdraw consent where information is no longer needed and provide procedures to respond to requests. **PROGRAM REQUIREMENT QUESTION** ***27. Subject to the Qualifications described below, do you permit individuals to withdraw consent where the information is no longer needed by the organization for the purposes for which consent was provided, and do you have procedures to respond to individuals' requests to cease the use or disclosure of their personal information?*** **ASSESSMENT CRITERIA** The Accountability Agent must verify that the Applicant Organization provides a description of the mechanisms provided to individuals so that they may withdraw consent for or request for ceasing the use and disclosure of their personal information at any time where their information is no longer required for the stated purposes, and subject to legal or contractual obligations to retain	**GDPR Art. 7 – Conditions for consent** 1. Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. **The data subject shall have the right to withdraw his or her consent at any time.** The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal**. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.**	🟢 GDPR Art. 7, para. 3, specifically grants individuals the right to withdraw consent at any time, and controllers must inform individuals of the right to withdraw consent "prior to giving consent." Furthermore, the right to exercise withdrawal of the consent must be as easy as it is to give consent. GDPR Art. 12, para. 2, requires controllers to facilitate the exercise of data subject rights. Note: The right to withdraw consent under the GDPR is not restricted to cases where the information is no longer needed. In any event, the GDPR does not permit the retention of personal data for longer than necessary. *Cf.*, GDPR Art. 5, para.1(e).

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the information. The Accountability Agent must verify that these mechanisms are in place and operational. Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. **GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * *	

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

Updates to the Program Requirements appear in red text.

VI. INTEGRITY OF PERSONAL INFORMATION (QUESTIONS 28-32)

Assessment Purpose *- The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Privacy Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.*

Global_CBPR_28. Describe procedures in place to verify that the PI is up-to-date, accurate, and complete.

PROGRAM REQUIREMENT QUESTION

28. Do you take steps to verify that the PI held by you is up-to-date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.

ASSESSMENT CRITERIA

Where the Applicant Organization answers **YES**, the AA must require the Applicant Organization to provide the procedures the Applicant Organization has in place to verify and ensure that the PI held is up-to-date, accurate and complete, to the extent necessary for the purposes of use.

The AA will verify that reasonable procedures are in place to allow the Applicant Organization to maintain PI that is up-to-date, accurate and complete, to the extent necessary for the purpose of use.

Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that procedures to verify and ensure that the PI held is up to date, accurate and complete, to the extent

GDPR Art. 5 -- Principles relating to processing of personal data

1. Personal data shall be:

* * *

(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

* * *

GDPR Art. 16 -- Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

GDPR Art. 5, para 1(d) requires personal data to be accurate and, where necessary, kept up to date. To the extent inaccuracies exist, the data must be erased or rectified without delay.

GDPR Art. 16 grants data subjects a right to rectification.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
necessary for the purposes of use, are required for compliance with this Privacy Principle.		
Global_CBPR_29. Provide a mechanism for correcting inaccurate, incomplete, and out of-date PI and describe how it works. **PROGRAM REQUIREMENT QUESTION** ***29. Do you have a mechanism for correcting inaccurate, incomplete and outdated PI to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must require the Applicant Organization to provide the procedures and steps the Applicant Organization has in place for correcting inaccurate, incomplete and out- dated PI, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information **such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The AA must verify that this process is in place and operational.** Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that procedures/steps to verify and ensure that the PI held is up to date, accurate and complete, to the	**GDPR Art. 5 -- Principles relating to processing of personal data** 1. Personal data shall be: * * * (d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); * * * **GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 16 -- Right to rectification**	🟢 GDPR Art. 12, para. 2, requires controllers to facilitate the exercise of data subject rights, including the right to rectification under GDPR Art. 16.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
extent necessary for the purposes of use, are required for compliance with this Privacy Principle.	The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	
Global_CBPR_30. Where PI has been transferred to processors and other service providers, inform them of any substantive corrections made to the PI post-transfer. **PROGRAM REQUIREMENT QUESTION** ***30. Where inaccurate, incomplete or out-of-date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to PI processors, agents, or other service providers to whom the PI was transferred? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must require the Applicant Organization to provide the procedures the Applicant Organization has in place to communicate corrections to PI processors, agent, or other service providers to	**GDPR Art. 24 –Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. **Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller**.	While the GDPR does not expressly state that controllers must inform processors of any corrections made to the data post-transfer, such a requirement could be inferred by GDPR Art. 28, para. 3(e), which requires a data processing agreement to stipulate that the processor must assist the controller in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights, which would include the right to rectification**.** Alternatively, GDPR Art. 24, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global CBPR) could provide a source of enforcement for Program Requirement 30. A reference to approved codes of conduct and certification mechanisms also appears in GDPR Art. 28, para. 5.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
whom the PI was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant Organization's behalf. The AA must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant Organization's behalf. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that procedures to communicate corrections to PI processors, agent, or other service providers to whom the PI was transferred, are required for compliance with this Privacy Principle.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (e) taking into account the nature of the processing, **assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights** laid down in Chapter III;	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	* * * 4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. 5. **Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article**. * * *	
Global_CBPR_31. Where PI has been disclosed to third parties, inform them of any substantive corrections made to the PI post-disclosure.	**GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data**	GDPR Art. 19 expressly requires controllers to communicate "any rectification … of processing carried out in accordance with Article 16 … to each

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
PROGRAM REQUIREMENT QUESTION ***31. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the PI was disclosed? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must require the Applicant Organization to provide the procedures the Applicant Organization has in place to communicate corrections to other third parties, to whom PI was disclosed. The AA must verify that these procedures are in place and operational. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that procedures to communicate corrections to other third parties to whom PI was disclosed, are required for compliance with this Privacy Principle.	concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **GDPR Art. 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing** The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.	recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort."
Global_CBPR_32. Require processors, agents, or other service providers who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date. **PROGRAM REQUIREMENT QUESTION**	**GDPR Art. 24 –Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is**	🟡 GDPR Art. 29 requires processors to process data only upon the instructions of the controller, and GDPR Art. 28 requires such processing to be governed by a contract. Accordingly, the terms of such a contract could require the processor to inform the controller of any inaccurate, incomplete,

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
32. Do you require PI processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date? **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must require the Applicant Organization to provide the procedures the Applicant Organization has in place to receive corrections from PI processors, agents, or other service providers to whom PI was transferred or disclosed to ensure that PI processors, agents, or other service providers to whom PI was transferred inform the Applicant Organization about any PI known to be inaccurate incomplete, or outdated. The AA will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant Organization and by the processors, agents or other service providers. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that procedures to receive corrections from PI processors, agents, or other service providers to whom PI was transferred or disclosed, are required for compliance with this Privacy Principle.	**performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. **Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller**. **GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the	or out-of-date data, as mentioned in Global CBPR Program Requirement 32. Alternatively, GDPR Art. 24, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global CBPR) could provide a source of enforcement for Program Requirement 32. A reference to approved codes of conduct and certification mechanisms also appears in GDPR Art. 28, para. 5.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (e) taking into account the nature of the processing, **assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights** laid down in Chapter III; * * * 5. **Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article**. * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	

GLOBAL CBPR	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

Updates to the Program Requirements appear in red text.

VII. SECURITY SAFEGUARDS (QUESTIONS 33-42)

Assessment Purpose *- The questions in this section are directed towards ensuring that when individuals entrust their information to an Applicant Organization, that Applicant Organization will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses.*

Global_CBPR_33. Implement a data security policy.

PROGRAM REQUIREMENT QUESTION

33. Have you implemented an information security policy?

ASSESSMENT CRITERIA

Where the Applicant Organization answers **YES**, the AA must verify the existence of this written policy.

Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.

GDPR Art. 30 -- Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

* * *

(g) where possible, **a general description of the technical and organisational security measures** referred to in Article 32(1).

* * *

3. **The records referred to in paragraphs 1 and 2 shall be in writing**, including in electronic form.

* * *

GDPR Art. 32 -- Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security**

GDPR Art. 30, read in conjunction with GDPR Art. 32, requires the existence of a written information security policy, which would satisfy the elements of Global CBPR Program Requirement 33.

Alternatively, GDPR Art. 32, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), could provide a source of enforcement for Program Requirement 33.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.**	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks. **PROGRAM REQUIREMENT QUESTION** ***34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?*** **ASSESSMENT CRITERIA** Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include: • **Authentication and access control (e.g., password protections)** • **Encryption**	**GDPR Art. 30 -- Records of processing activities** 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: * * * (g) where possible, **a general description of the technical and organisational security measures** referred to in Article 32(1). * * * 3. **The records referred to in paragraphs 1 and 2 shall be in writing**, including in electronic form. * * * **GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the	GDPR Art. 32, para.1, appears to require the level of detail outlined by Global CBPR Program requirement 34. In addition, GDPR Art. 32, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), could provide a source of enforcement for Program Requirement 34.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
• **Boundary protection (e.g., firewalls, intrusion detection)** • **Audit logging** • **Monitoring (e.g., external and internal audits, vulnerability scans)** • **Other (specify)** The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that	controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) **the pseudonymisation and encryption of personal data**; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing**. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the**	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the implementation of such safeguards is required for compliance with this Privacy Principle.	**requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_35. Ensure that the above identified safeguards are proportionate to likelihood and severity of harm, the sensitivity of the information, and the context in which it is held. **PROGRAM REQUIREMENT QUESTION** ***35. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.*** **ASSESSMENT CRITERIA** Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify that these safeguards are proportional to the risks identified.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner	GDPR Art. 32, para.1, specifically refers to the implementation of security measures "appropriate to the risk." Para. 2 provides further guidance on assessing the appropriate level of security based on the risks presented. Para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which provides further support for Program Requirement 35.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** = Aligned; = Similar; = Different
The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the PI (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the **appropriate level of security account shall be taken in particular of the risks that are presented by processing**, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_36. Provide regular training and oversight to employees on the importance of maintaining security safeguards.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as	While the GDPR does not expressly require the training of employees on the importance of

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
PROGRAM REQUIREMENT QUESTION ***36. Describe how you make your employees aware of the importance of maintaining the security of PI (e.g., through regular training and oversight).*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization's employees are aware of the importance of, **and obligations respecting**, maintaining the security of PI through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees, • Regular staff meetings or other communications, • Security policy signed by employees, or • Other (specify) Where the Applicant Organization answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of PI through regular training and oversight, the AA has to inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: * * * (d) a process for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** * * * 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall **take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller**, unless he or she is required to do so by Union or Member State law. **GDPR Art. 39 -- Tasks of the data protection officer**	maintaining security safeguards, the elements of Global CBPR Program Requirement 36 could be implied from GDPR Art. 39, para.1(b)—which tasks the DPO with "awareness-raising and training of staff involved in processing operations"—as well as GDPR Art. 32, para. 1(d), which requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." Moreover, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which would provide further support for Program Requirement 36.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, **including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations**, and the related audits; * * *	
Global_CBPR_37. Implement reasonable safeguards proportionate to the likelihood and severity of the harm, the sensitivity of the information, and the context in which it is held. **PROGRAM REQUIREMENT QUESTION** ***37. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:***	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate:	GDPR Art. 32, para. 1, expressly requires the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk., including—under para 1(d)—"a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." These provisions, together with GDPR Art. 39, para.1(b)—which tasks the DPO with "awareness-raising and training of staff involved in processing operations"—can be

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
37.a. ***Employee training and management or other organizational safeguards?*** ***37.b.*** ***Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?*** ***37.c.*** ***Detecting, preventing, and responding to attacks, intrusions, or other security failures?*** ***37.d.*** ***Physical security?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES** (to questions 37.a. to 37.d.), the AA has to verify the existence of each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant Organization must employ suitable and reasonable means, such as encryption, to protect all PI. Where the Applicant Organization answers **NO** (to questions 37.a. to 37.d.), the AA must inform the Applicant Organization that the existence of safeguards on each category is required for compliance with this Privacy Principle.	(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the **appropriate level of security account shall be taken in particular of the risks that are presented by processing**, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor	read to comport with elements of Global CBPR Program Requirement 37. Moreover, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which would provide further support for Program Requirement 37.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_38. Implement a policy for secure disposal of PI. **PROGRAM REQUIREMENT QUESTION** ***38. Have you implemented a policy for secure disposal of PI?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the implementation of a policy for the secure disposal of PI. Where the Applicant Organization answers **NO**, the AA must inform Applicant Organization that the existence of a policy for the secure disposal of PI is required for compliance with this Privacy Principle.	**GDPR Art. 5 -- Principles relating to processing of personal data** 1. Personal data shall be: * * * (e) kept in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); * * * **GDPR Art. 17 -- Right to erasure ('right to be forgotten')** 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the **controller shall have the**	● The GDPR adopts the storage limitation principle (GDPR Art. 5, para. 1(e)), which requires the erasure (or deletion) of personal data no longer necessary in relation to the purposes for which they were collected or otherwise processed. See GDPR Art. 17, para. 1(a). GDPR Art. 24, paras. 1-2, further require controllers to implement appropriate technical and organisational measures and policies to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Moreover, GDPR Art. 24, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which would provide further support for Program Requirement 38.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; * * * **GDPR Art. 24 -- Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller **shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 **shall include the implementation of appropriate data protection policies** by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.	

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
Global_CBPR_39. Implement measures to detect, prevent, and respond to security threats. **PROGRAM REQUIREMENT QUESTION** ***39. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this Privacy Principle.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, **in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or**	🟢 GDPR Art. 32 generally mirrors the elements of Global CBPR Program Requirement 39.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	access to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_40. Implement measures to assess the effectiveness of safeguards. **PROGRAM REQUIREMENT QUESTION** ***40. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 39? Describe below.*** **ASSESSMENT CRITERIA** The AA must verify that such tests are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these tests.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and**	GDPR Art. 32, para.1(d), specifically requires a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational safeguards, as mentioned in Global CBPR Program Requirement 40.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, **in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.** 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
Global_CBPR_41. Employ third-party certifications or other risk assessments. **PROGRAM REQUIREMENT QUESTION** ***41. Do you use third-party certifications or other risk assessments? Describe below.*** **ASSESSMENT CRITERIA** The AA must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant Organization and if audits are carried out, the AA must verify whether recommendations made in the audits are implemented.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access	🟢 GDPR Art. 32, para.1(d), specifically requires a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational safeguards, thereby mirroring Global CBPR Program Requirement 41's reference to "other risk assessments." Moreover, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which would provide further support for Program Requirement 41.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	to personal data transmitted, stored or otherwise processed. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_CBPR_42. Employ measures to ensure that processors, agents, contractors, and other service providers protect PI against security threats. **PROGRAM REQUIREMENT QUESTION** ***42. Do you require PI processors, agents, contractors, or other service providers to whom you transfer PI to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:*** ***42.a. Implementing an information security program that is proportionate to the***	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the	The data security provisions of GDPR Art. 32 apply contractors and processors alike. That said, GDPR Art. 28, para. 3(c), specifically requires contractors to enter into a contract with processors that, inter alia, ensures that processors take all measures required by Art. 32 (i.e., security safeguards).

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
sensitivity of the information and services provided? ***42.b.*** ***Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the PI of the Applicant Organization's customers?*** ***42.c.*** ***Taking immediate steps to correct/address the security failure which caused the privacy or security breach?*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom PI is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (c) **takes all measures required pursuant to Article 32**; * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law. **GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the **controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security**	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (c) **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;** (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	

VIII. ACCESS AND CORRECTION (QUESTIONS 43-45)

Assessment Purpose *- The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. The Qualifications to the Provision of Access and Correction Mechanisms are listed below and set out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

QUALIFICATIONS TO THE PROVISION OF ACCESS AND CORRECTION MECHANISMS

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. ***Disproportionate Burden:*** *Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.*

ii. ***Protection of Confidential Information:*** *Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e. information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where*

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
confidential commercial information can be readily separated from other information subject to an access request, the personal information controller should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned. Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modeling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security. iii. ***Third Party Risk:*** *Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the personal information controller must release the information after redaction of the third party's personal information.*		
Global_CBPR_43. Respond to individuals' requests for confirmation on whether you hold their PI. **PROGRAM REQUIREMENT QUESTION** ***43. Upon request, do you provide confirmation of whether or not you hold PI about the requesting individual? Describe below.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to respond to such requests. The Applicant Organization must grant access to any individual, to PI collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant Organization's processes or mechanisms for access by individuals to PI must be reasonable having regard to the manner of request and the nature of the PI.	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the	GDPR Arts. 12, 15 and 16, when read together, reflect the elements of Global CBPR Program Requirement 43.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
The PI must be provided to individuals in an easily comprehensible way. The Applicant Organization must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 15 – Right of access by the data subject** 1. The data subject shall have the right to obtain from the controller confirmation as to **whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data** and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) **the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;** (f) the right to lodge a complaint with a supervisory authority;	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
	(g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. * * * **GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	
Global_CBPR_44. Respond to individuals' requests for access to their PI, and describe the procedures in place for receiving and handling access requests. **PROGRAM REQUIREMENT QUESTION** ***44. Upon request, do you provide individuals access to the PI that you hold about them? Where YES, answer questions 44(a) – (e) and describe your applicant's policies/procedures***	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or	🟢 GDPR Arts. 12 and 15, when read together, reflect the elements of Global CBPR Program Requirement 44. In particular, GDPR Art. 12, para. 3, requires the controller to provide information on action taken on a data subject request without undue delay and in any event within one month of receipt of the request.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
for receiving and handling access requests. Where NO, proceed to question 45. **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES** the AA must verify each answer provided. The Applicant Organization must implement reasonable and suitable processes or mechanisms to enable the individuals to access their PI, such as account or contact information. If the Applicant Organization denies access to PI, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that it may be required to permit access by individuals to their PI. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. **The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request.** That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. * * *	

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	GDPR Art. 15 – Right of access by the data subject 1. The data subject shall have the right to obtain from the controller confirmation as to **whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data** and the following information: * * *	
Global_CBPR_44a. Verify the identity of individuals requesting access to PI. **PROGRAM REQUIREMENT QUESTION** ***44.a. Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.***	**GDPR Recital 64** The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests. **GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate,	🟢 GDPR Recital 64 provides that a controller should use all reasonable measures to verify the identity of a data subject who requests access. GDPR Art 12, para. 6, permits a controller to request the provision of additional information necessary to confirm the identity of the data subject where the controller has reasonable doubts concerning the identity of the requester.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * 6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. * * * **GDPR Art. 15 – Right of access by the data subject** 1. The data subject shall have the right to obtain from the controller **confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data** and the following information: * * *	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_44b. Provide individuals with access to their PI within a reasonable time. **PROGRAM REQUIREMENT QUESTION** 44.b. Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe.	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 3. **The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request.** That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. * * *	GDPR Art. 12, para. 3, requires a controller to take action on a request "without undue delay and in any event within one month of receipt of the request."
Global_CBPR_44c. Provide individuals information about their PI in understandable manner. **PROGRAM REQUIREMENT QUESTION** 44.c. Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language,** in particular for any information addressed specifically to a child.	GDPR Art. 12, para. 1, requires a controller to provide information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * *	
Global_CBPR_44d. Provide individuals information about their PI in a way that is compatible with the regular form of interaction. **PROGRAM REQUIREMENT QUESTION** 44.d. Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g., email, same language, etc.)?	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language,** in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. * * *	 The GDPR does not expressly mandate that information be provided in a way "compatible with the regular form of interaction" with the data subject, but such a requirement could be implied by the language of GDPR Art. 12, para. 1, which requires the controller to communicate in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_44e. Ensure that any fee for providing individuals with access to their PI is not excessive. **PROGRAM REQUIREMENT QUESTION** 44.e. Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 **shall be provided free of charge.** Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. * * *	GDPR Art. 12, para. 5, provides that responses to requests be provided free of charge. Alternatively, where requests are " manifestly unfounded or excessive," the controller may charge a reasonable fee.
Global_CBPR_45. Permit individuals to correct, amend, or delete inaccurate PI, and describe the procedures in place for handling their requests for correction and/or deletion. **PROGRAM REQUIREMENT QUESTION** ***45. Do you permit individuals to challenge the accuracy of their information, and to have it***	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any	The elements of Global CBPR Program Requirement 45 are reflected in the provisions of GDPR Arts. 12, 16, 17, and 24.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
rectified, completed, amended and/or deleted? Describe your policies/procedures in this regard below and answer questions 38 (a) – (e). **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES to questions 45(a) – (e)**, the AA must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant Organization denies correction to the individual's PI, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant Organization answers **NO** to questions 45(a) – (e) and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where	information addressed specifically to a child. **The information shall be provided in writing**, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **GDPR Art. 17 -- Right to erasure ('right to be forgotten')**	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.	1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the **controller shall have the obligation to erase personal data** without undue delay where one of the following grounds applies: * * * **GDPR Art. 24 –Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, **the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of **appropriate data protection policies** by the controller. 3. **Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller**.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_45a. Provide access and correction mechanisms to individuals in a clear and conspicuous manner. **PROGRAM REQUIREMENT QUESTION** 45.a. Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. **The information shall be provided in writing**, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data**	GDPR Art. 12, para. 1, specifically requires controllers to provide communications related to the right to rectification (found in Art. 16) "in a concise, transparent, intelligible and easily accessible form, using clear and plain language."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	
Global_CBPR_45b. Make requested corrections and deletions where appropriate. **PROGRAM REQUIREMENT QUESTION** 45.b. If an individual demonstrates that PI about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. **The information shall be provided in writing**, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.	GDPR Art. 12, para. 2, specifically requires controllers to facilitate the exercise of data subject rights, including the right to rectification (Art. 16) and right to erasure (Art. 17).

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	* * * **GDPR Art. 16 –Right to rectification** The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **GDPR Art. 17 -- Right to erasure ('right to be forgotten')** 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the **controller shall have the obligation to erase personal data** without undue delay where one of the following grounds applies: * * *	
Global_CBPR_45c. Make requested corrections and deletions within a reasonable time. **PROGRAM REQUIREMENT QUESTION** 45.c. Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any	GDPR Art. 12, para. 3, specifically requires controllers to take action on a request to exercise of data subject rights, including the right to rectification (Art. 16) and the right to erasure (Art. 17), "without undue delay and in any event within one month of receipt of the request."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	information addressed specifically to a child. **The information shall be provided in writing**, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt of the request**. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. * * *	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	GDPR Art. 16 –Right to rectification The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **GDPR Art. 17 -- Right to erasure ('right to be forgotten')** 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the **controller shall have the obligation to erase personal data** without undue delay where one of the following grounds applies: * * *	
Global_CBPR_45d. Provide individuals with a copy of their PI as corrected or with a confirmation that their correction or deletion request has been handled. **PROGRAM REQUIREMENT QUESTION** 45.d. Do you provide a copy to the individual of the corrected PI or provide confirmation that the data has been corrected or deleted?	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** 1. The controller shall take appropriate measures to provide … **any communication under Articles 15 to 22** and 34 relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child.	 While the GDPR does not expressly require controllers to provide data subjects with a copy of the corrected PI or confirmation of a correction/deletion, GDPR Art. 12, para. 3, could be interpreted to require as much, as it requires a controller to "provide information on action taken."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt of the request**. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. * * *	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	GDPR Art. 16 –Right to rectification The data subject shall have the right to obtain from the controller without undue delay the **rectification of inaccurate personal data** concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **GDPR Art. 17 -- Right to erasure ('right to be forgotten')** 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the **controller shall have the obligation to erase personal data** without undue delay where one of the following grounds applies: * * *	
Global_CBPR_45e. Provide individuals with an explanation when access or correction has been denied, along with contact information for further inquiries. **PROGRAM REQUIREMENT QUESTION** 45.e. If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	**GDPR Art. 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a	 GDPR Art. 12, para. 4, requires the controller to provide the data subject with a statement of reasons for not taking action and with information regarding the taking remedial action.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	supervisory authority and seeking a judicial remedy. * * *	

IX. ACCOUNTABILITY (QUESTIONS 46-57)

Assessment Purpose *- The questions in this section are directed towards ensuring that the Applicant Organization is accountable for complying with measures that give effect to the other Privacy Principles stated above. Additionally, when transferring information, the Applicant Organization should be accountable for ensuring that the recipient will protect the information consistently with these Privacy Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Privacy Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Privacy Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Global_CBPR_46. Describe the measures you have taken to ensure compliance with the Global CBPR Privacy Principles. **PROGRAM REQUIREMENT QUESTION** ***46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.*** • ***Internal guidelines or policies (if applicable, describe how implemented) ___*** • ***Contracts ___*** • ***Compliance with applicable industry or sector laws and regulations ___***	**GDPR Art. 30 -- Records of processing activities** 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be	While the GDPR does not reference the Global CBPR Privacy Principles, **GDPR Art. 42** does "encourage" the establishment of data protection certification mechanisms like the Global CBPR. Moreover, GDPR Art. 30 requires a record of processing activities for purposes of maintaining accountability, as envisioned under Global CBPR Program Requirement 46.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
• ***Compliance with self-regulatory Applicant Organization code and/or rules ___*** • ***Maintaining records of processing activities ___*** • ***Other (describe) ___*** **ASSESSMENT CRITERIA** The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant processing activities which are capable of being provided upon request. Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.	disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). * * * **GDPR Art. 42 -- Certification** 1. **The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors**. The specific needs of micro, small and medium-sized enterprises shall be taken into account.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects. 3. The certification shall be voluntary and available via a process that is transparent. 4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56. 5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal. 6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure. 7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met. 8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_47. Appoint a qualified person to be responsible for overall compliance with data protection program and Global CBPR Privacy Principles. **PROGRAM REQUIREMENT QUESTION** ***47. Have you appointed ~~an~~ a qualified individual(s) to be responsible for ~~your~~ overall compliance with your data protection program and the Global CBPR Privacy Principles?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has ~~designated~~ appointed an ~~employee(s)~~ individual(s) who is responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles. The Applicant Organization should describe the individual(s)' qualifications that are appropriate to the nature of the data processing activities. The Applicant Organization must ~~designate~~ appoint an individual or individuals to be responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that	**GDPR Art. 37 -- Designation of the data protection officer** 1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. 2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. 3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.	GDPR Arts. 37 - 39 set forth specifications regarding the designation of a data protection officer, which reflect the elements of Global CBPR Program Requirement 47.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
~~designation~~ appointment of such an employee(s) is required for compliance with this Privacy Principle.	4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors. 5. **The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.** 6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. 7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority. **GDPR Art.38 -- Position of the data protection officer** 1. The controller and the processor shall ensure that the **data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.** 2. The controller and processor shall support the data protection officer in performing the tasks	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. 3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor. 4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation. 5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law. 6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests. **GDPR Art. 39 -- Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. 2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_48. Implement internal procedures to investigate and respond to privacy-related complaints. **PROGRAM REQUIREMENT QUESTION** ***48. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant Organization (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant Organization's compliance with the Global CBPR Framework and/or requests from individuals for access to PI; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	**GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt of the request**. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. 4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and	While GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, nothing in the GDPR expressly requires controllers to receive, investigate and respond to privacy-related "complaints." Under GDPR Art. 77, complaints are to be brought before the supervisory authority, not the controller That said, raising disputes with the controller is arguably implicit in GDPR Art. 12.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. * * * **GDPR Art. 77 -- Right to lodge a complaint with a supervisory authority** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. 2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.	
Global_CBPR_49. Implement internal procedures to ensure a timely response to privacy-related complaints. **PROGRAM REQUIREMENT QUESTION** ***49. Do you have procedures in place to ensure individuals receive a timely response to their complaints?***	**GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request	While GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, nothing in the GDPR expressly requires controllers to respond to "complaints." Under GDPR Art. 77, "complaints" are to be brought before the supervisory authority, not the controller.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
ASSESSMENT CRITERIA Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt of the request**. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. 4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. * * * **GDPR Art. 77 -- Right to lodge a complaint with a supervisory authority**	That said, a timely response to any concern raised by a data subject is arguably implicit in GDPR Art. 12, para. 3.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. 2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.	
Global_CBPR_50. Ensure that a response to a privacy-related complaint includes an explanation of the potential remedial actions to be taken. **PROGRAM REQUIREMENT QUESTION** ***50. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization indicates what remedial action is considered.	**GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject **without undue delay and in any event within one month of receipt**	While GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, nothing in the GDPR expressly requires controllers to respond to "complaints." Under GDPR Art. 77, complaints are to be brought before the supervisory authority, not the controller. That said, GDPR Art. 12, para. 4, requires controllers to inform data subjects about remedial action if a data subject request is denied—i.e., by lodging a complaint with the supervisory authority—which arguably reflects the overall intent of Global CBPR Program Requirement 50.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. 4. **If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.** * * * **GDPR Art. 77 -- Right to lodge a complaint with a supervisory authority** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	the processing of personal data relating to him or her infringes this Regulation. 2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.	
Global_CBPR_51. Implement procedures and training for employees on how to respond to privacy-related complaints. **PROGRAM REQUIREMENT QUESTION** ***51. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant Organization answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the AA must inform the	**GDPR Art. 12 -- Transparent information, communication and modalities for the exercise of the rights of the data subject** * * * 2. **The controller shall facilitate the exercise of data subject rights** under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject. * * * **GDPR Art. 39 -- Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to	While GDPR Art. 12 requires controllers to facilitate the exercise of data subject rights, nothing in the GDPR expressly requires controllers to respond to "complaints." Under GDPR Art. 77, "complaints" are to be brought before the supervisory authority, not the controller. That said, GDPR Art. 39, para. 1 (b), requires DPOs to train staff, and such training could arguably include training on how to respond to privacy-related complaints, as reflected in Global CBPR Program Requirement 51.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, **including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations**, and the related audits; * * * **GDPR Art. 77 -- Right to lodge a complaint with a supervisory authority** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. 2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_52. Implement procedures for responding to government orders, subpoenas, and warrants that require the disclosure of PI. **PROGRAM REQUIREMENT QUESTION** ***52. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI, as well as provide the necessary training to employees regarding this subject. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.	**GDPR Art. 2 -- Material scope** * * * 2. This Regulation does not apply to the processing of personal data: * * * (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. * * * **GDPR Art. 24 -- Responsibility of the controller** 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller **shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 **shall include the implementation of appropriate data protection policies** by the controller.	Responding to legitimate government requests for information appears to fall outside the scope of the GDPR (see Art. 2, para. 2(d)). Indeed, the GDPR does not contain an express requirement for controllers to implement procedures for responding to government orders, subpoenas, and warrants. That said, such a requirement could be implied by the obligation to use appropriate organizational measures under GDPR Art. 24, para. 1. Moreover, GDPR Art. 24, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global CBPR), which would provide further support for Program Requirement 52.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*:** 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	3. **Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.**	
Global_CBPR_53. Implement measures to ensure that processors, agents, contractors, and others processing PI on your behalf comply with data protection obligations. **PROGRAM REQUIREMENT QUESTION** ***53. Do you have mechanisms in place with PI processors, agents, contractors, or other service providers pertaining to PI they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?*** • ***Internal guidelines or policies ___*** • ***Contracts ___*** • ***Compliance with applicable industry or sector laws and regulations ___*** • ***Compliance with self-regulatory Applicant Organization code and/or rules ___*** • ***Others (describe) ___*** **ASSESSMENT CRITERIA**	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to	🟢 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors to ensure that processors take all measures in accord with the Regulation.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of agreement described. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.	transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant to Article 32; (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	

Go to TABLE OF CONTENTS

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different**
Global_CBPR_54. Employ appropriate measures to ensure that processors, agents, contractors, and others processing PI on your behalf abide by your instructions and the practices you uphold. **PROGRAM REQUIREMENT QUESTION** ***54. Do these agreements generally require that PI processors, agents, contractors or other service providers:*** • ***Abide by your Global CBPR-compliant privacy policies and practices as stated in your Privacy Statement?*** • ***Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement?*** • ***Follow instructions provided by you relating to the manner in which your PI must be handled?*** • ***Impose restrictions on subcontracting unless with your consent?*** • ***Be Global CBPR-certified by a Forum-recognized AA in their jurisdiction?*** • ***Notify the Applicant Organization in the case of a breach of the personal information of the Applicant Organization's customers?*** • ***Other (describe)***	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits	🟢 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors to ensure that processors take all measures in accord with the Regulation. GDPR Art. 29 further requires processors to process data only subject the instructions of the controller.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
ASSESSMENT CRITERIA The AA must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.	such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant to Article 32; (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;	

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	
Global_CBPR_55. Verify any self-assessments that PI processors, agents, contractors or other service providers provide to you to demonstrate compliance with your instructions.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that	While the GDPR does not expressly require processors to perform self-assessments, GDPR Art. 28, para. 3(h), requires processors to make available to the controller all information necessary to demonstrate compliance.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
PROGRAM REQUIREMENT QUESTION ***55. Do you require your PI processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.*** **ASSESSMENT CRITERIA** The AA must verify the existence of such self-assessments.	processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (h) **makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller**. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	The wording of the Global CBPR System's question makes clear that a self-assessment is not considered an affirmative obligation, but controllers must verify the existence of such self-assessments if processors, agents, contractors or other agents say they have undertaken such assessments Indeed, Global_PRP_17 supports the view that a self-assessment is not an affirmative obligation, as it refers to "self-assessments or other evidence of compliance ...."

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global_CBPR_56. Employ spot-checking or other monitoring mechanisms to ensure compliance by processors, agents, contractors, and others processing PI on your behalf. **PROGRAM REQUIREMENT QUESTION** ***56. Do you carry out regular spot checking or monitoring of your PI processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the existence of the Applicant Organization's procedures such as spot checking or monitoring mechanisms. Where the Applicant Organization answers **NO**, the AA must require the Applicant Organization to describe why it does not make use of such spot checking or monitoring mechanisms.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (h) **makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller**. With regard to point (h) of the first subparagraph, the processor shall immediately	 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors to ensure that processors take all measures in accord with the Regulation. To the extent GDPR Art. 28, para. 3(h), requires processors to make available to the controller all information necessary to demonstrate compliance, subparagraph (h) could arguably include the use of monitoring mechanisms. Moreover, since the GDPR requires the use of a Data Processing Agreement, the terms of that agreement could impose obligations related to spot-checking or other monitoring mechanisms.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
	inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.	
Global_CBPR_57. For situations where traditional methods to ensure compliance by recipients of PI are either impractical or impossible, describe how PI can nevertheless remain protected. **PROGRAM REQUIREMENT QUESTION** ***57. Do you disclose PI to other recipient persons or organizations in situations where due diligence and reasonable steps to ensure compliance with the Global CBPR System by the recipient as described above is impractical or impossible?*** **ASSESSMENT CRITERIA** If **YES**, the AA must ask the Applicant Organization to explain: 1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and the other means used by the Applicant Organization for ensuring that the information, nevertheless, is protected consistent with the	**GDPR Art. 89 -- Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes** 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. 2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the	The GDPR recognizes certain situations where exemptions or derogations from various obligations would be warranted, such as in cases of the public interest, scientific or historical research, and statistical purposes. See GDPR Art. 89.

GLOBAL CBPR	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information ***Updates to the Program Requirements appear in red text.***		**KEY*: = Aligned; = Similar; = Different**
Global CBPR Privacy Principles. Where the Applicant Organization relies on an individual's consent, the Applicant Organization must explain to the satisfaction of the AA the nature of the consent and how it was obtained.	rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.	

GLOBAL PRP	GDPR	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different

PART 2 – MAPPING GLOBAL PRP PROGRAM REQUIREMENTS TO EU GDPR

The purpose of this document is to provide the baseline program requirements of the Global Privacy Recognition for Processors (PRP) System which operationalize the Global CBPR Privacy Principles ("Privacy Principles") [described in the Global CBPR Framework], and assist Global CBPR Forum-recognized Accountability Agents in an Applicant Organization's compliance with the Global PRP System.

These program requirements are replicated in the Global PRP System Intake Questionnaire to help Applicant Organizations assess their compliance.

Accountability Agents are responsible for receiving an Applicant Organization's completed Intake Questionnaire and supporting documentation, verifying an Applicant Organization's compliance with the requirements of the Global PRP System and, where appropriate, assisting the Applicant Organization in modifying its policies and practices to meet the requirements of the Global PRP System. The Accountability Agent will certify those Applicant Organizations deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Certified Organizations' compliance with the Global PRP System based on these criteria.

I. GLOBAL PRP SECURITY SAFEGUARDS (QUESTIONS 1-8)

Global_PRP_1. Implement an information security policy that covers PI processed on behalf of a controller.

PROGRAM REQUIREMENT QUESTION

1. ***Has your organization implemented an information security policy that covers PI processed on behalf of a controller?***

ASSESSMENT CRITERIA

Where the Applicant Organization answers **YES**, the AA must verify the existence of this written policy.

Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.

GDPR Art. 30 -- Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

* * *

(g) where possible, **a general description of the technical and organisational security measures** referred to in Article 32(1).

* * *

3. **The records referred to in paragraphs 1 and 2 shall be in writing**, including in electronic form.

* * *

GDPR Art. 32 -- Security of processing

🟢

GDPR Art. 30, read in conjunction with GDPR Art. 32, requires the existence of a written information security policy, which would satisfy the elements of Global PRP Program Requirement 1.

Alternatively, GDPR Art. 32, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global PRP), could provide a source of enforcement for Program Requirement 1.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the **processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_PRP_2. Incorporate physical, technical, and administrative safeguards in your organization's information security policy. **PROGRAM REQUIREMENT QUESTION** ***2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.*** **ASSESSMENT CRITERIA** Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:	**GDPR Art. 30 -- Records of processing activities** 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: * * * (g) where possible, **a general description of the technical and organisational security measures** referred to in Article 32(1). * * * 3. **The records referred to in paragraphs 1 and 2 shall be in writing**, including in electronic form. * * *	🟢 GDPR Art. 32, para.1, appears to require the level of detail outlined by Global PRP Program requirement 2. In addition, GDPR Art. 32, para. 3, which refers to approved codes of conduct and certification mechanisms (such as the Global PRP), could provide a source of enforcement for Program Requirement 1.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
• Authentication and access control (e.g., password protections) • Encryption • Boundary protection (e.g., firewalls, intrusion detection) • Audit logging • Monitoring (e.g., external and internal audits, vulnerability scans) • Other (specify) The Applicant Organization must periodically review and reassess these measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) **the pseudonymisation and encryption of personal data**; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing**. 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_PRP_3. Educate employees on the importance of maintaining security safeguards. **PROGRAM REQUIREMENT QUESTION** ***3. Describe how your organization makes employees aware of the importance of maintaining the security of PI.*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization's employees are aware of the importance of, and obligations respecting, maintaining the security of PI through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: * * * (d) a process for **regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.**	🟡 While the GDPR does not expressly require the training of employees on the importance of maintaining security safeguards, the elements of Global PRP Program Requirement 3 could be implied from GDPR Art. 39, para.1(b)—which tasks the DPO with "awareness-raising and training of staff involved in processing operations"—as well as GDPR Art. 32, para. 1(d), which requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." Moreover, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global PRP), which would

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
• Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant Organization answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of PI through regular training and oversight, the AA has to inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	* * * 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall **take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller**, unless he or she is required to do so by Union or Member State law. **GDPR Art. 39 -- Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, **including the assignment of responsibilities, awareness-raising and training of staff**	provide further support for Program Requirement 3.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	involved in processing operations, and the related audits; * * *	
Global_PRP_4. Implement measures to detect, prevent, and respond to security threats. **PROGRAM REQUIREMENT QUESTION** ***4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to PI?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to PI. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the existence of such measures is required for compliance with this Privacy Principle.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;** (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 2. In assessing the **appropriate level of security account shall be taken in particular of the risks**	🟢 GDPR Art. 32, para. 1, expressly requires the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including—under para 1(c)—"the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." Moreover, para 1(d) requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." These provisions, together with GDPR Art. 39, para.1(b)—which tasks the DPO with "awareness-raising and training of staff involved in processing operations"—support the elements of Global PRP Program Requirement 4. Furthermore, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global PRP), which would provide further support for Program Requirement 4.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	that are presented by processing, in particular from **accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed**. 3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_PRP_5. Develop processes to test the effectiveness of security safeguards. **PROGRAM REQUIREMENT QUESTION** ***5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.*** **ASSESSMENT CRITERIA** The AA must verify that such tests are undertaken at appropriate intervals, and that the Applicant	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: * * *	🟢 GDPR Art. 32, para. 1(d) expressly requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing," thereby reflecting the elements of Global PRP Program Requirement 5.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Organization adjusts their security safeguards to reflect the results of these tests.	(d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing**. * * *	
Global_PRP_6. Implement procedures to notify the controller of security incidents. **PROGRAM REQUIREMENT QUESTION** ***6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's PI?*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization has in place appropriate processes to notify the controller of occurrences of a breach of the privacy or security of their organization's PI.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (c) **takes all measures required pursuant to Article 32**; * * *	🟡 While the GDPR does not expressly require processers to notify controllers of security incidents, such a requirement could be inferred by data security provisions of GDPR Art. 32, and by GDPR Art. 28, para. 3(c), which specifically requires contractors to enter into a contract with processors that, inter alia, ensures that processors take all measures required by Art. 32 (i.e., security safeguards).

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	GDPR Art. 29 – Processing under the authority of the controller or processor The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law. **GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the **controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (c) **the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;**	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	(d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article. 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
Global_PRP_7. Implement procedures for the secure disposal or return of PI. **PROGRAM REQUIREMENT QUESTION** ***7. Has your organization implemented procedures for the secure disposal or return of PI when instructed by the controller or upon***	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this	🟢 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors that includes a provision (pursuant to subpara. 3(g)) stipulating that the processor "deletes or returns all

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
termination of the relationship with the controller? **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the existence of procedures for the secure disposal or return of PI. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * * (g) **at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;** * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	the personal data to the controller after the end of the provision of services relating to processing ….”

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_PRP_8. Adopt the use of third-party certifications or risk assessments. **PROGRAM REQUIREMENT QUESTION** ***8. Does your organization use third-party certifications or other risk assessments? Please describe.*** **ASSESSMENT CRITERIA** The AA must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant Organization and if audits are carried out, the AA must verify whether recommendations made in the audits are implemented.	**GDPR Art. 32 -- Security of processing** 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk**, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) **the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;** (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.** 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	🟢 GDPR Art. 32, para.1(d), specifically requires a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational safeguards, thereby mirroring Global PRP Program Requirement 8's reference to "other risk assessments." Moreover, GDPR Art. 32, para. 3 specifically refers to approved codes of conduct and certification mechanisms (such as the Global PRP), which would provide further support for Program Requirement 8.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	3. **Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.** 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	
II. GLOBAL PRP ACCOUNTABILITY MEASURES (QUESTIONS 9-18)		
Global_PRP_9. Limit processing of PI to the purposes specified by the controller. **PROGRAM REQUIREMENT QUESTION** ***9. Does your organization limit its processing of PI to the purposes specified by the controller?*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization has policies in place to limit its processing to the purposes specified by the controller.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the	🟢 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors, setting forth "the nature and purpose of the processing" and ensuring that the processor processes the personal data "only on documented instructions from the controller." GDPR Art. 39 further provides that processors shall not process data "except on instructions from the controller."

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	processing, **the nature and purpose of the processing,** the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant to Article 32; (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. * * * **GDPR Art. 29 – Processing under the authority of the controller or processor**	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	
Global_PRP_10. Implement procedures to comply with controllers' requests for deletions, corrections, and updates. **PROGRAM REQUIREMENT QUESTION** ***10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation **and ensure the protection of the rights of the data subject**. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, **the nature and purpose of the processing,** the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an	🟢 GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors that includes a provision (pursuant to subpara. 3(e)) stipulating that the processors fulfill the controller's obligation to respond to requests for exercising data subjects' rights, which would include the rights to rectification and erasure.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; * * * (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, **for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III**; * * * (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. * * *	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	GDPR Art. 29 – Processing under the authority of the controller or processor The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	
Global_PRP_11. Implement measures to ensure compliance with the controller's instructions. **PROGRAM REQUIREMENT QUESTION** ***11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of PI processing? Please describe.*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization indicates the measures it takes to ensure compliance with the controller's instructions.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, **the nature and purpose of the processing,** the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: * * *	🟢 Pursuant to GDPR Art 28, para. 1, a processor must provide "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation." Furthermore, GDPR Art. 28, para. 3, specifically requires contractors to enter into a contract with processors that includes a provision (pursuant to subpara. 3(h)) stipulating that the processor "makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article."

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	(h) makes available to the controller **all information necessary to demonstrate compliance** with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.	
Global_PRP_12. Appoint an individual responsible for Global PRP System compliance. **PROGRAM REQUIREMENT QUESTION** ***12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the Global PRP System?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has designated an employee(s) who is responsible for the Applicant Organization's overall compliance with the Global PRP System. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that designation of such an employee(s) is required for compliance with the Global PRP System.	**GDPR Art. 37 -- Designation of the data protection officer** 1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. 2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	🟢 GDPR Arts. 37 - 39 set forth specifications regarding the designation of a data protection officer, which reflect the elements of Global PRP Program Requirement 12.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors. 5. **The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.** 6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. 7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority. **GDPR Art.38 -- Position of the data protection officer** 1. The controller and the processor shall ensure that the **data protection officer is involved, properly and in a timely manner, in all issues**	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	which relate to the protection of personal data. 2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge. 3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor. 4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation. 5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law. 6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests. **GDPR Art. 39 -- Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks:	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. 2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_PRP_13. Implement procedures to forward data subject requests to the controller or to handle them yourself when so instructed. **PROGRAM REQUIREMENT QUESTION** ***13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.	**GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation **and ensure the protection of the rights of the data subject**. * * * 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;	🟡 Pursuant to GDPR Art 28, para. 1, a processor must provide "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation **and ensure the protection of the rights of the data subject,**" which implies a process for forwarding or handling privacy-related requests or complaints. Furthermore, GDPR Art. 28, para. 3, requires processors to enter into a contract that includes a provision (pursuant to subpara. 3(e)) to assist the controller in the fulfillment of obligations related to the exercise of data subjects' rights.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	* * * (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, **for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III**; * * * (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions. * * * **GDPR Art. 29 – Processing under the authority of the controller or processor** The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_PRP_14. Notify the controller of subpoenas, warrants, and orders seeking disclosure of PI, unless notification is prohibited by law. **PROGRAM REQUIREMENT QUESTION** ***14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of PI?*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of PI, as well as provide the necessary training to employees regarding this subject. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.	**GDPR Art. 2 -- Material scope** * * * 2. This Regulation does not apply to the processing of personal data: * * * (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. * * * **GDPR Art. 28 –Processor** 1. Where processing is to be carried out on behalf of a controller, **the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of this Regulation **and ensure the protection of the rights of the data subject**. * * *	🟡 Responding to legitimate government requests for information appears to fall outside the scope of the GDPR (see Art. 2, para. 2(d)). Indeed, the GDPR does not contain an express requirement for controllers or processors to implement procedures for responding to government orders, subpoenas, and warrants. That said, such a requirement for processors could be implied by the obligation to provide "sufficient guarantees to implement appropriate technical and organisational measures" under GDPR Art 28, para. 1.
Global_PRP_15. Implement a process for notifying the controller of your engagement of subprocessors. **PROGRAM REQUIREMENT QUESTION**	**GDPR Art. 28 –Processor** * * * 2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any	🟢 The elements of Global PRP Program Requirement 15 are reflected in GDPR Art. 28, para. 2.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors? **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization has in place a procedure to notify controllers that the Applicant Organization is engaging subprocessors.	intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. * * *	
Global_PRP_16. Ensure that subprocessors comply with your Global PRP System obligations. **PROGRAM REQUIREMENT QUESTION** ***16. Does your organization have mechanisms in place with subprocessors to ensure that PI is processed in accordance with your obligations under the Global PRP System? Please describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of mechanism described. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such mechanisms is required for compliance with this Privacy Principle.	**GDPR Art. 28 –Processor** * * * 4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. * * *	🟢 The elements of Global PRP Program Requirement 16 are reflected in GDPR Art. 28, para. 4.

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_PRP_17. Ensure that compliance mechanisms require subprocessors to follow your instructions, restrict further subprocessing, provide evidence of compliance, and permit monitoring. **PROGRAM REQUIREMENT QUESTION** ***17. Do the mechanisms referred to above generally require that subprocessors:*** ***a) Follow instructions provided by your organization relating to the manner in which PI must be handled?*** ***b) Impose restrictions on further subprocessing?*** ***c) Be Global PRP-certified by a Global CBPR Forum-recognized Accountability Agent in their jurisdiction?*** ***d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If YES, describe.*** ***e) Allow your organization to carry out regular spot checking or other monitoring activities? If YES, describe.*** ***f) Other (describe)*** **ASSESSMENT CRITERIA** The AA must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.	**GDPR Art. 28 –Processor** * * * 2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. * * * 4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations. * * *	🟢 The elements of Global PRP Program Requirement 17 are reflected in GDPR Art. 28, paras. 2 and 4.

Go to TABLE OF CONTENTS

GLOBAL PRP	GDPR	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Global_PRP_18. Implement procedures for training employees related to PI management practices and related client instructions. **PROGRAM REQUIREMENT QUESTION** ***18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.*** **ASSESSMENT CRITERIA** Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place for training employees relating to PI management and the controller's instructions. Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.	**GDPR Art. 39 -- Tasks of the data protection officer** 1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor **and the employees who carry out processing of their obligations** pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, **including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations**, and the related audits; * * *	🟢 The elements of Global PRP Program Requirement 3 are reflected in GDPR Art. 39, para.1(b), which tasks the DPO with "awareness-raising and training of staff involved in processing operations."

GDPR	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

PART 3 – GDPR PROVISIONS THAT DO NOT MAP TO THE UPDATED GLOBAL CBPR/GLOBAL PRP SYSTEMS' PROGRAM REQUIREMENTS

I. LEGITIMATE INTERESTS

GDPR Art. 6 -- Lawfulness of processing 1. Processing shall be lawful only if and to the extent that at least one of the following applies: * * * (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. * * *	N/A	No legitimate interest basis for processing in the Global CBPR/Global PRP Systems.

II. DATA PORTABILITY

GDPR Art. 20 -- Right to data portability 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of	N/A	Although the Global CBPR/Global PRP Systems do not specifically address the right of data portability, the right is tangentially related to access requests (Global CBPR System Q43 et seq.) to the extent portability entitles data subjects to receive their personal data.

GDPR	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.		
III. AUTOMATED DECISION MAKING		
GDPR Art. 22 -- Automated individual decision-making, including profiling 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. 2. Paragraph 1 shall not apply if the decision:	N/A	🔴 No specific rules on automated decision making in the Global CBPR/Global PRP Systems.

GDPR	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent. 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.		
IV. DATA PROTECTION BY DESIGN AND BY DEFAULT		
GDPR Art. 25 -- Data protection by design and by default 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for	N/A	🔴 No specific rules on data protection by design or default in the Global CBPR/Global PRP Systems.

GDPR	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.		

GDPR	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different

V. ONWARD TRANSFERS

GDPR Art. 44 -- General principle for transfers

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

GLOBAL CBPR PROGRAM REQUIREMENT QUESTION

Q53. Do you have mechanisms in place with PI processors, agents, contractors, or other service providers pertaining to PI they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?

- **Internal guidelines or policies ___**
- **Contracts ___**
- **Compliance with applicable industry or sector laws and regulations ___**
- **Compliance with self-regulatory Applicant Organization code and/or rules ___**
- **Others (describe) ___**

Assessment Criteria

*Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of agreement described.*

*Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.*

🔴

While Global CBPR Program Requirement 53 requires mechanisms to be in place to ensure that obligations are assumed by "agents, contractors, or other service providers," nothing specifically addresses onward transfers of personal data to another third country.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different

PART 4 – MAPPING EDPB CERTIFICATION GUIDELINES TO THE UPDATED GLOBAL CBPR/GLOBAL PRP SYSTEMS' PROGRAM REQUIREMENTS

I. EDPB GUIDELINES 1/2018

The following criteria are taken from Annex 2 of Guidelines 1/2018.

A. SCOPE OF THE CERTIFICATION MECHANISM AND TARGET OF EVALUATION (TOE)

EDPB_1-2018_1. Clear description

ANNEX 2, SEC. 2, PARA. A

a. Is the scope of the certification mechanism (for which the data protection criteria shall be used) clearly described?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)

* * *

Part II. Scope

5. The purpose of Part II of the Global CBPR Framework is to make clear the extent of coverage of the Global CBPR Privacy Principles contained in Part III of this Framework.

CORE DEFINITIONS

6. **Personal information** means any information about an identified or identifiable individual.

   COMMENTARY

   6. The Framework is intended to apply to information about natural living persons, not legal persons. The Framework applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criterion alone, but when put together with other information would identify an individual. For example, certain

🟢

Part II of the Global CBPR Framework outlines the scope of the certification framework, a portion of which is reproduced in the column to the left.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behavior, social relationships, private preferences and identity. CORE DEFINITIONS 7. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs. *COMMENTARY* *7. The Framework applies to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information. For the purposes of the Framework, where a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf, the instructing person or organization is the personal information controller and is responsible for ensuring*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	compliance with the Global CBPR Privacy Principles. Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities. CORE DEFINITIONS 8. **Publicly available information** means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or that is legally obtained and accessed from: a) government records that are available to the public; b) journalistic reports; or c) information required by law to be made available to the public. *COMMENTARY* *8. The Framework has limited application to publicly available information. Notice and choice requirements, in particular, often are superfluous where the information is already publicly available, and the personal information controller does not collect the information directly from the individual concerned. Publicly available information may be contained in government records that are available to the public, such as registers of people who are entitled to vote, or in news items broadcast or published by the news media.* * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_2. Not misleading **ANNEX 2, SEC. 2, PARA. B** ***b. Is the scope of the certification mechanism meaningful to its addressed audience and not misleading?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **ELEMENT 3 – RECOGNITION** ***Compliance Directory and Contact Information*** 23. 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 (see para 15). 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. 24. The directory and contact lists are hosted on the Forum website (www.globalcbpr.org) and maintained by the Communications and Stakeholder Engagement Committee. This website contains FAQs and additional	🟡 The Systems' "Policies, Rules and Guidelines" include measures geared to making information regarding certifications available to the public, including a publicly available Compliance Directory.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	information on the Global CBPR and Global PRP Systems for potential Applicant Organizations and consumers. * * *	
EDPB_1-2018_3. Covers relevant processing **ANNEX 2, SEC. 2, PARA. C** ***c. Does the scope of the certification mechanism reflect all relevant aspects of the processing operations?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **Overview of the Global CBPR and Global PRP Systems** 8. Organizations that choose to participate in the Global CBPR System should implement data protection and privacy policies and practices consistent with the Global CBPR System Program Requirements for all personal information that they have collected or received that is within the scope of its certification. These data protection and privacy policies and practices should be evaluated by an Accountability Agent for compliance with the Global CBPR System Program Requirements. Once an organization has been certified for participation in the Global CBPR System, these data protection and privacy policies and practices become binding as to that organization and are enforceable as described under Element 4 - Enforcement below (see para 28).	🟢 The Polices, Rules and Guidelines note that the Framework covers all relevant aspects of processing operations, from collection to disposal.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	9. Organizations that choose to participate in the Global PRP System should implement data protection and privacy policies and practices consistent with the Global PRP System Program Requirements for all personal information that they process on behalf of controllers. These data protection and privacy policies and practices should be evaluated by an Accountability Agent for compliance with the Global PRP System Program Requirements. Once an organization has been certified as a participant in the Global PRP System, the organization's compliance with the Global PRP System Program Requirements become binding as to that organization and are enforceable as described under Element 4 - Enforcement below (see para 29-31)	
EDPB_1-2018_4. Account for risk **ANNEX 2, SEC. 2, PARA. D** ***d. Does the scope of the certification mechanism allow meaningful data protection certification taking into account the nature, the content, the risk of the related processing operations?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **Part III. Global CBPR Privacy Principles** * * * **PRINCIPLES** **I. Preventing Harm** 17. Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information. Further, **acknowledging the risk**	🟢 The Framework takes relevant risks into account.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. *COMMENTARY* *17. This Principle recognizes that one of the primary objectives of the Framework is to prevent misuse of personal information and consequent harm to individuals. Therefore, data protection and privacy approaches, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence,* ***organizational controls should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection, use or transfer of personal information.*** *Where there has been a significant security breach affecting personal information, it may help to reduce the risk of harmful consequences to the individuals concerned to give notice to Privacy Enforcement Authorities and/or the individuals concerned.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
EDPB_1-2018_5. Application to cross-border transfers **ANNEX 2, SEC. 2, PARA. E** ***e. Does the scope of the certification mechanism cover personal data processing in the relevant country of application or does it address cross border processing and/or transfers?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * 3. The Global CBPR System was developed to provide a simple and transparent system that can be used by organizations for the protection of personal information that moves across jurisdictions and to: • provide a practical mechanism for Members to implement the Global CBPR Framework in an international, cross-border context; domestic laws, regulations and guidelines would continue to cover the collection and management of personal information within jurisdictions; • provide a means for organizations to transfer personal information across jurisdictions in a manner in which individuals may trust that their personal information is protected; and • apply only to organizations (that is, businesses) – it is not intended to deal with the personal information handling practices of governments or individuals. * * * 7. The Global PRP System was designed to help processors demonstrate their capacity for processing of personal information in general,	🟢 The certification mechanism is designed to address both cross border processing and transfers.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	but also to assure that processing is at least consistent with a controller's applicable requirements for processing under the Global CBPR System. Note that while it can streamline compliance and promotes accountability, there is no requirement that a Global CBPR-certified controller must engage a Global PRP-recognized processor to perform information processing in order to comply with the Accountability principle in the Global CBPR Framework and the Global CBPR System. * * *	
EDPB_1-2018_6. Sufficiently describe object of certification **ANNEX 2, SEC. 2, PARA. F** ***f. Do the certification criteria sufficiently describe how the [Target of Evaluation] should be defined?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * CORE DEFINITIONS 7. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.	🟢 The CBPR Framework defines the "target of evaluation" as a "personal information controller."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	COMMENTARY 7. *The Framework applies to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information. For the purposes of the Framework, where a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf, the instructing person or organization is the personal information controller and is responsible for ensuring compliance with the Global CBPR Privacy Principles. Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities.* * * *	
EDPB_1-2018_7. Understandable to data subjects **ANNEX 2, SEC. 2, PARA. G** ***g. Do the criteria guarantee that the (individual) ToEs are understandable to its audience, including data subjects where relevant?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **ELEMENT 3 – RECOGNITION** ***Compliance Directory and Contact Information*** 23. The Forum maintains a publicly accessible directory of organizations that have been	🟡 The Systems' "Policies, Rules and Guidelines" include measures geared to making information regarding certifications available to the public, including a publicly available Compliance Directory.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	certified by Accountability Agents as compliant with the Global CBPR and/or Global PRP Systems, which includes relevant details of each certification (see para 15). 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. 24. The directory and contact lists are hosted on the Forum website (www.globalcbpr.org) and maintained by the Communications and Stakeholder Engagement Committee. This website contains FAQs and additional information on the Global CBPR and Global PRP Systems for potential Applicant Organizations and consumers. * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

B. GENERAL REQUIREMENTS

EDPB_1-2018_8. Describe terms

ANNEX 2, SEC. 3, PARA. A

a. Are all relevant terms used in the criteria catalogue (i.e. the full set of certification criteria) identified, explained and described?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)

* * *

CORE DEFINITIONS

6. **Personal information** means any information about an identified or identifiable individual.
7. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.
8. **Publicly available information** means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or that is legally obtained and accessed from: a) government records that are available to the public; b) journalistic reports; or c) information required by law to be made available to the public.

The CBPR Framework defines the key terms.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	9. **Data Protection and Privacy Laws** means laws and regulations of a Member, the enforcement of which have the effect of protecting personal information consistent with the Global CBPR Framework. 10. **Global CBPR System** is the abbreviation of the Global Cross-Border Privacy Rules System. 11. **Global PRP System** is the abbreviation of the Global Privacy Recognition for Processors System. 12. **Privacy Enforcement Authority** means any public body that is responsible for enforcing Data Protection and Privacy Laws, and that has powers to conduct investigations and/or pursue enforcement proceedings. 13. **Global CAPE** is the abbreviation of the Global Cooperation Arrangement for Privacy Enforcement which is a practical multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in crossborder data protection and privacy enforcement by creating a framework under which authorities may, on a voluntary basis, share information and request and render assistance in certain ways. * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_9. Describe references **ANNEX 2, SEC. 3, PARA. B** ***b. Are all normative references identified?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * CORE DEFINITIONS 6. **Personal information** means any information about an identified or identifiable individual. 7. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs. 8. **Publicly available information** means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or that is legally obtained and accessed from: a) government records that are available to the public; b) journalistic reports; or c) information required by law to be made available to the public. 9. **Data Protection and Privacy Laws** means laws and regulations of a Member, the enforcement of which have the effect of protecting personal	🟢 The CBPR Framework explains referenced terms.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	information consistent with the Global CBPR Framework. 10. **Global CBPR System** is the abbreviation of the Global Cross-Border Privacy Rules System. 11. **Global PRP System** is the abbreviation of the Global Privacy Recognition for Processors System. 12. **Privacy Enforcement Authority** means any public body that is responsible for enforcing Data Protection and Privacy Laws, and that has powers to conduct investigations and/or pursue enforcement proceedings. 13. **Global CAPE** is the abbreviation of the Global Cooperation Arrangement for Privacy Enforcement which is a practical multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in crossborder data protection and privacy enforcement by creating a framework under which authorities may, on a voluntary basis, share information and request and render assistance in certain ways. * * *	
EDPB_1-2018_10. Define responsibilities, procedures, processing **ANNEX 2, SEC. 3, PARA. C** ***c. Do the criteria include the definition of data protection responsibilities, procedures and processing covered by the scope of the certification mechanism?***	**GLOBAL CBPR FORUM - ACCOUNTABILITY AGENT RECOGNITION APPLICATION** ***Overview*** The purpose of this document is to guide the application process for an organization seeking recognition as an Accountability Agent ("Applicant Accountability Agent") under the Global Cross-Border Privacy Rules (CBPR) System or Global	🟢 The Accountability Agent Recognition Application expressly sets forth the necessary recognition criteria for Accountability Agents and how they are to complete the certification process.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	Privacy Recognition for Processors (PRP) System, or both. This document explains the necessary recognition criteria and provides the program requirements of the Global CBPR and Global PRP Systems ("Global CBPR System Program Requirements" and "Global PRP System Program Requirements"). Only Accountability Agents recognized by the Global CBPR Forum ("Forum") may participate in the Global CBPR and Global PRP Systems. Once recognized, Accountability Agents may publicize this recognition and certify organizations as Global CBPR- and/or Global PRP-compliant. A recognized Accountability Agent would only be able to certify as Global CBPR- and/or Global PRP-compliant those organizations that are subject to enforcement as described in the Policies, Rules and Guidelines. * * * **ANNEX A:** ***Accountability Agent Recognition Criteria*** **Program Requirements** 4) An Accountability Agent evaluates Applicant Organizations against the Global CBPR and/or Global PRP Program Requirements ("Program Requirements"). (NOTE: an Accountability Agent may charge a fee to a Certified Organization for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.) **Certification Process**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	5) An Accountability Agent has a comprehensive process to review an Applicant Organization's policies and practices with respect to the Applicant Organization's participation in the Global CBPR and/or Global PRP Systems and to verify its compliance with the Program Requirements. The certification process includes: a. An initial assessment of compliance, which will include verifying the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Applicant Organization against the Program Requirements, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools; b. A comprehensive report to the Applicant Organization outlining the Accountability Agent's findings regarding the Applicant Organization's level of compliance with the Program Requirements. Where non-fulfilment of any of the Program Requirements is found, the report must include a list of changes the Applicant Organization needs to complete for purposes of obtaining certification for participation in the Global CBPR and/or Global PRP Systems; c. Verification that any changes required under paragraph 5(b) have been properly completed by the Applicant Organization;	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	d. Certification that the Applicant Organization is in compliance with the Program Requirements; and e. Provision of the relevant details of the Certified Organization's certification for the Forum's Compliance Directory. The relevant details should include at least the following: the name of the Certified Organization, links to the Certified Organization's website and privacy policy, contact information, the name of the Accountability Agent that certified the Certified Organization and can handle consumer disputes, the name of the relevant PEA, the scope of the certification, the date that the Certified Organization was first certified, and the expiry date for the current certification.	
C. PROCESSING OPERATION, ARTICLE 42(1)		
EDPB_1-2018_11. Legal bases for processing **ANNEX 2, SEC. 4, PARA. A** ***a. Do criteria require identification of the valid legal bases of processing with respect to the ToE?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** Q12. Do you collect PI (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such PI? Where YES, describe.	🟡 Whereas the GDPR allows for six bases upon which personal data can be processed, the Global CBPR focuses only one: consent. That said, Program Requirement 12 requires that collection be by "lawful and fair means." As the for other legal bases available under the GDPR, the System's Policies, Rules And Guidelines are clear: "The Global CBPR and Global PRP Systems do not displace or change a Member's

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = **Aligned;** = **Similar;** = **Different**
	GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES* * * * **THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS** 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply. 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional	domestic laws and regulations. … Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	
EDPB_1-2018_12. Phases of processing **ANNEX 2, SEC. 4, PARA. B** ***b. With respect to the ToE, do the criteria recognize the relevant phases of processing and the whole life-cycle of data including the deletion and or anonymisation?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** * * * Q6. Do you provide clear and easily accessible statements about your practices and policies that govern the PI described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same. Q7. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?	🟢 The Global CBPR Program Requirements cover the whole lifecycle of processing.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Q8. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which PI is being collected? Q9. Subject to the Qualifications [listed here], at the time of collection of PI, do you notify individuals that their PI may be shared with third parties? * * * Q13. Do you limit the use of the PI you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below. * * * Q28. Do you take steps to verify that the PI held by you is up-to-date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe. Q29. Do you have a mechanism for correcting inaccurate, incomplete and outdated PI to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary. * * * Q33. Have you implemented an information security policy?	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses? * * * Q38. Have you implemented a policy for secure disposal of PI? Q39. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures? * * *	
EDPB_1-2018_13. Data portability **ANNEX 2, SEC. 4, PARA. C** ***c. With respect to the ToE, do the criteria require data portability?***	N/A	🔴 The Global CBPR Program Requirements cover a number of data subject rights, but not data portability.
EDPB_1-2018_14. Automated decision making **ANNEX 2, SEC. 4, PARA. D** ***d. With respect to the ToE, do the criteria allow identifying and reflecting special types of processing operations, e.g. automated decision making, profiling?***	N/A	🔴 The Global CBPR Program Requirements do not address automated decision making or profiling .

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
EDPB_1-2018_15. Special categories of data **ANNEX 2, SEC. 4, PARA. E** ***e. With respect to the ToE, do the criteria allow identifying special categories of data?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** Q1. Do you take steps to identify and provide appropriate additional safeguards for personal information that is **considered sensitive or categorized to require special protection** based on the laws governing your collection or processing of the personal information or where an organization transferring the personal information to you has identified it as such? If YES, describe. Q2. Do you take steps to assess whether you collect or process personal information that is **considered or categorized as children's personal information** based on the laws governing your collection or processing of the personal information? * * *	🟢 The newly updated Global CBPR Program Requirements cover sensitive data and children's data.
EDPB_1-2018_16. Assessment of risks – data subjects **ANNEX 2, SEC. 4, PARA. F** ***f. Do the criteria allow and require assessing the risk of the individual processing operations and the protection needs for the rights and freedoms of data subjects?***	**CBPR PROGRAM REQUIREMENT QUESTION** Q4. Do you have procedures/mechanisms in place to **identify and assess the risks** of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?	🟡 The newly updated Global CBPR Program Requirements cover the assessment of risk, which could be read to address rights and freedoms of data subjects.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_17. Assessment of risks – natural persons **ANNEX 2, SEC. 4, PARA. G** ***g. Do the criteria allow and require adequate account of the risks to the rights and freedoms of natural persons?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** Q4. Do you have procedures/mechanisms in place to **identify and assess the risks** of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?	🟡 The newly updated Global CBPR Program Requirements cover the assessment of risk, which could be read to address rights and freedoms of natural persons.
D. LAWFULNESS OF PROCESSING		
EDPB_1-2018_18. Purpose and necessity of processing. **ANNEX 2, SEC. 5, PARA. A** ***a. Do the criteria require checking the lawfulness of processing for individual processing operations with respect to purpose and necessity of processing?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** Q11. Do you limit your PI collection (whether directly or through the use of third parties acting on your behalf) to information that is **relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes**? Q12. Do you collect PI (whether directly or through the use of third parties acting on your behalf) by **lawful and fair means**, consistent with the requirements of the jurisdiction that governs the collection of such PI? Where YES, describe. Q13. Do you limit the use of the PI you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to **those purposes for which the information was**	🟢 The Global CBPR Program Requirements limit processing to lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection. Processing is also limited to the purposes for which the information was collected or for other compatible or related purposes.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	collected or for other compatible or related purposes? If necessary, provide a description in the space below. Q14. If you answered NO, do you use the PI you collect for unrelated purposes under one of the following circumstances? Describe below. Q14a. Based on express consent of the individual? Q14b. Compelled by applicable laws? * * * Q28. Do you take steps to verify that the PI held by you is up-to-date, accurate and complete, to the extent **necessary for the purposes of use**? If YES, describe. * * *	
EDPB_1-2018_19. Legal basis for processing **ANNEX 2, SEC. 5, PARA. B** ***b. Do the criteria require checking all the requirements of a legal basis for individual processing operations?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** Q11. Do you limit your PI collection (whether directly or through the use of third parties acting on your behalf) to information that is **relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes**? Q12. Do you collect PI (whether directly or through the use of third parties acting on your behalf) by **lawful and fair means**, consistent with the requirements of the jurisdiction that governs the collection of such PI? Where YES, describe. * * *	🟢 The Global CBPR Program Requirements limit processing to lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

E. PRINCIPLES, ARTICLE 5

EDPB_1-2018_20. Data protection principles

ANNEX 2, SEC. 6, PARA. A

a. Do the criteria adequately address all data protection principles pursuant to Article 5?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)

* * *

Part III. Global CBPR Privacy Principles

I. PREVENTING HARM

17. Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

II. NOTICE

18. Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:

a) the fact that personal information is being collected;

b) the purposes for which personal information is collected;

GDPR Art. 5 identifies six principles; the Global CBPR Framework identifies nine. That said, the six GDPR principles, listed below, are reflected the corresponding principles from the Framework:

- **Lawfulness, Fairness, Transparency:**
  - COLLECTION LIMITATION " any such information should be obtained by lawful and fair means"
  - NOTICE: "provide clear and easily accessible statements about … practices and policies"
- **Purpose Limitation:**
  - USES OF PERSONAL INFORMATION**:** "Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes"
- **Data Minimization:**
  - COLLECTION LIMITATION: "The collection of personal information should be limited to information that is relevant to the purposes of collection"
  - PREVENTING HARM: "Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information."
- **Accuracy:**

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information. 19. All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable. 20. It may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information. **III. COLLECTION LIMITATION** 21. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by **lawful and fair means**, and where appropriate, with notice to, or consent of, the individual concerned. **IV. USES OF PERSONAL INFORMATION**	○ INTEGRITY OF PERSONAL INFORMATION: "Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use" • **Storage Limitation:** ○ USES OF PERSONAL INFORMATION**:** "Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes" ○ SECURITY SAFEGUARDS: "Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information, or other misuses." • **Integrity and Confidentiality:** ○ INTEGRITY OF PERSONAL INFORMATION: "Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use" • **Accountability:** ○ ACCOUNTABILITY: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	22. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. **V. CHOICE** 23. Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information. **VI. INTEGRITY OF PERSONAL INFORMATION** 24. Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use. **VII. SECURITY SAFEGUARDS** 25. Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information, or other misuses. Such safeguards should be	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment. **VIII. ACCESS AND CORRECTION** 26. Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; (iv) in a form that is generally understandable; and, c) challenge the accuracy of personal information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted. 27. Such access and opportunity for correction should be provided except where: a) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's personal information and privacy in the case in question;	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	b) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or c) the personal information and privacy of persons other than the individual would be violated. 28. If a request under 25(a) or 25(b) or a challenge under 25(c) is denied, the individual should be provided with reasons why and be able to challenge such denial. **IX. ACCOUNTABILITY** 29. A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles. * * *	
EDPB_1-2018_21. Data minimisation **ANNEX 2, SEC. 6, PARA. B** ***b. Do the criteria require demonstration of data minimisation for the individual ToE?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **Part III. Global CBPR Privacy Principles** **I. PREVENTING HARM**	🟡 While the Global CBPR Framework does not use the term "data minimisation," the concept is implied, especially in the "COLLECTION LIMITATION" Principle. The Commentary on that Principle explains that the collection of personal information "should be **relevant** to such purposes, and **necessity**

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	17. Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information. * * * **III. COLLECTION LIMITATION** 21. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by **lawful and fair means**, and where appropriate, with notice to, or consent of, the individual concerned. *COMMENTARY* *21. This Principle limits collection of personal information by reference to the purposes for which it is collected. The collection of the personal information should be relevant to such purposes, and necessity and proportionality to the fulfillment of such purposes may be factors in determining what is relevant. This Principle also provides that collection methods must be lawful and fair. For example, obtaining personal information under false pretenses (e.g., where an organization uses phishing,*	**and proportionality** to the fulfillment of such purposes may be factors in determining what is relevant."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	telemarketing calls, or pretexting emails to fraudulently misrepresent itself as another company in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal information) may in many Members be considered unlawful. Therefore, even in those Members where there is no explicit law against these specific methods of collection, they may be considered to be unfair means of collection. . *The Principle also recognizes that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate. For example, in a situation where there is an outbreak of food poisoning, it would be appropriate for the relevant health authorities to collect the personal information of patrons from restaurants without providing notice to or obtaining the consent of individuals in order to inform them of the potential health risk.* **IV. USES OF PERSONAL INFORMATION** 22. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or,	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. * * *	
F. GENERAL OBLIGATIONS OF CONTROLLERS AND PROCESSORS		
EDPB_1-2018_22. Data Processing Agreement **ANNEX 2, SEC. 7, PARA. A** ***a. Do the criteria require proof of contractual agreements between processors and controllers?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.** • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Maintaining records of processing activities ___ • Other (describe) ___ ***Assessment Criteria*** *The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant*	🟡 While the Global CBPR and Global PRR Systems do not ***require*** the existence of a contract per se, they do require evidence of measures to ensure that any processing is done in accordance with the Privacy Principles and limited to the purposes specified by the controller. That said, the System's Policies, Rules And Guidelines are clear: "The Global CBPR and Global PRP Systems ***do not displace or change a Member's domestic laws*** and regulations. … Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	processing activities which are capable of being provided upon request. *Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.* * * * **Q53. Do you have mechanisms in place with PI processors, agents, contractors, or other service providers pertaining to PI they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?** • Internal guidelines or policies ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Others (describe) ___ ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of agreement described.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	agreements is required for compliance with this Privacy Principle. **Q54. Do these agreements generally require that PI processors, agents, contractors or other service providers:** • Abide by your Global CBPR-compliant privacy policies and practices as stated in your Privacy Statement? • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? • Follow instructions provided by you relating to the manner in which your PI must be handled? • Impose restrictions on subcontracting unless with your consent? • Be Global CBPR-certified by a Forum-recognized AA in their jurisdiction? • Notify the Applicant Organization in the case of a breach of the personal information of the Applicant Organization's customers? • Other (describe) ***Assessment Criteria*** *The AA must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.* * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

GLOBAL PRP PROGRAM REQUIREMENT QUESTIONS

* * *

Q9. Does your organization limit its processing of PI to the purposes specified by the controller?

Assessment Criteria

The AA must verify that the Applicant Organization has policies in place to limit its processing to the purposes specified by the controller.

* * *

Q11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of PI processing? Please describe.

Assessment Criteria

The AA must verify that the Applicant Organization indicates the measures it takes to ensure compliance with the controller's instructions.

* * *

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*

* * *

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply. 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	
EDPB_1-2018_23. Evaluation of data processing agreement **ANNEX 2, SEC. 7, PARA. B** ***b. Are controller processor agreements subject to evaluation?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.** • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Maintaining records of processing activities ___ • Other (describe) ___ ***Assessment Criteria***	🟢 The Framework requires an Accountability Agent to evaluate all measures taken, which would include the terms of a data processing agreement should one exist.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant processing activities which are capable of being provided upon request. *Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.* * * * **Q53. Do you have mechanisms in place with PI processors, agents, contractors, or other service providers pertaining to PI they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?** • Internal guidelines or policies ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Others (describe) ___ ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of agreement described.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	*Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.* **Q54. Do these agreements generally require that PI processors, agents, contractors or other service providers:** • Abide by your Global CBPR-compliant privacy policies and practices as stated in your Privacy Statement? • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? • Follow instructions provided by you relating to the manner in which your PI must be handled? • Impose restrictions on subcontracting unless with your consent? • Be Global CBPR-certified by a Forum-recognized AA in their jurisdiction? • Notify the Applicant Organization in the case of a breach of the personal information of the Applicant Organization's customers? • Other (describe) ***Assessment Criteria***	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	The AA must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met. * * * **GLOBAL PRP PROGRAM REQUIREMENT QUESTIONS** * * * **Q9. Does your organization limit its processing of PI to the purposes specified by the controller?** ***Assessment Criteria*** *The AA must verify that the Applicant Organization has policies in place to limit its processing to the purposes specified by the controller.* * * * **Q11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of PI processing? Please describe.** ***Assessment Criteria*** *The AA must verify that the Applicant Organization indicates the measures it takes to ensure compliance with the controller's instructions.* * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_24. Obligations of controller

ANNEX 2, SEC. 7, PARA. C

c. Do the criteria reflect the obligations of the controller pursuant to Chapter IV?

GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS

Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?

Assessment Criteria

The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.

Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.

* * *

While the Global CBPR Framework covers many of the obligations outlined in the GDPR—including the use of risk assessments, maintenance of records of processing, application of security measures, notification of data breaches, and appointment of a data protection officer—the Framework is silent on measures related to data protection by design and default. That said, such measures could be viewed as falling withing the scope of Global CBRP Program Requirement 4, which references measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	Q33. Have you implemented an information security policy? ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify the existence of this written policy.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.* **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?** ***Assessment Criteria*** *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • Authentication and access control (e.g., password protections) • Encryption • Boundary protection (e.g., firewalls, intrusion detection)	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	• Audit logging • Monitoring (e.g., external and internal audits, vulnerability scans) • Other (specify) *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.* *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.* *Where the Applicant Organization indicates that it has **NO** physical, technical and*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle. * * * **Q38. Have you implemented a policy for secure disposal of PI?** ***Assessment Criteria*** *Where the Applicant Organization answers YES, the AA must verify the implementation of a policy for the secure disposal of PI.* *Where the Applicant Organization answers NO, the AA must inform Applicant Organization that the existence of a policy for the secure disposal of PI is required for compliance with this Privacy Principle.* **Q39. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?** ***Assessment Criteria*** *Where the Applicant Organization answers YES, the AA must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures.* *Where the Applicant Organization answers NO, the AA must inform the Applicant Organization that the existence of measures*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this Privacy Principle. **Q40. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 39? Describe below.** ***Assessment Criteria*** *The AA must verify that such tests are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these tests.* * * * **Q47. Have you appointed a qualified individual(s) to be responsible for overall compliance with your data protection program and the Global CBPR Privacy Principles?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has appointed an individual(s) who is responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles. The Applicant Organization should describe the individual(s)' qualifications that are appropriate to the nature of the data processing activities.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	The Applicant Organization must appoint an individual or individuals to be responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that appointment of such an individual(s) is required for compliance with this Privacy Principle.* * * *	
EDPB_1-2018_25. Review of measures **ANNEX 2, SEC. 7, PARA. D** ***d. Do the criteria require proof of review and updating of technical and organisational measures implemented by the controller pursuant to Article 24(1)?***	**GLOBAL CBPR FORUM – *ACCOUNTABILITY AGENT RECOGNITION APPLICATION*** * * * ***Annex A*** **ACCOUNTABILITY AGENT RECOGNITION CRITERIA** * * * **On-going Monitoring and Compliance Review Processes** 6) An Accountability Agent has comprehensive written procedures designed to ensure the integrity of the certification process and to monitor Certified Organizations throughout	🟡 The requirement to review and update technical and organizational measures is implicit in the Accountability Agent's duty to ensure ongoing monitoring and compliance of an organization's technical and organisational measures. Moreover, certifications are subject to annual attestation and re-certification.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	their certification periods to ensure continued compliance with the Program Requirements. * * * **Re-Certification and Annual Attestation** 8) An Accountability Agent will require Certified Organizations to attest on an annual basis to their continued compliance to the Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-certification. Where there has been a material change to the Certified Organization's privacy policy (as reasonably determined by the Accountability Agent in good faith), the Accountability Agent will carry out an immediate review process. This re-certification review process includes: a. An assessment of compliance, which will include verification of the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Certified Organization, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools; b. A report to the Certified Organization outlining the Accountability Agent's findings regarding the Certified Organization's level of compliance with the Program Requirements. The report must also list any corrections the Certified Organization needs to make to correct areas of non-compliance and the timeframe within which the	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
	corrections must be completed for purposes of obtaining re-certification; c. Verification that required corrections have been properly completed by the Certified Organization; and d. Notice to the Certified Organization that the Certified Organization is in compliance with the Program Requirements and has been re-certified. **GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to*	

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	document the risk assessment and that they have been or will be implemented where necessary. *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?** *Assessment Criteria* *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • *Authentication and access control (e.g., password protections)* • *Encryption* • *Boundary protection (e.g., firewalls, intrusion detection)* • *Audit logging* • ***Monitoring (e.g., external and internal audits, vulnerability scans)***	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	• *Other (specify)* *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.* *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.* *Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	required for compliance with this Privacy Principle.	
EDPB_1-2018_26. Appointment of DPO **ANNEX 2, SEC. 7, PARA. E** ***e. Do the criteria check that the organisation has assessed if a Data Protection Officer (DPO) should be appointed as required by Article 37? Where relevant does the DPO meet the requirements under Articles 37 to 39?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q47. Have you appointed a qualified individual(s) to be responsible for overall compliance with your data protection program and the Global CBPR Privacy Principles?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has appointed an individual(s) who is responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles. The Applicant Organization should describe the individual(s)' qualifications that are appropriate to the nature of the data processing activities.* *The Applicant Organization must appoint an individual or individuals to be responsible for the Applicant Organization's overall compliance with data protection and these Privacy Principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that appointment of such an*	🟢 Global CBPR Program Requirement 47 mirrors the EBPB's criterion.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	individual(s) is required for compliance with this Privacy Principle.	
EDPB_1-2018_27. Records of processing activities **ANNEX 2, SEC. 7, PARA. F** ***f. Do the criteria check that records of processing of activities are required in accordance with Article 30(5) and appropriately address Article 30 requirements?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.** • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • **Maintaining records of processing activities ___** • Other (describe) ___ *Assessment Criteria* *The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant processing activities which are capable of being provided upon request.* *Where the Applicant Organization answers it does not maintain records of processing*	🟢 Global CBPR Program Requirement 46 specifically references records of processing activities.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.	
G. RIGHTS OF THE DATA SUBJECTS		
EDPB_1-2018_28. Right to information **ANNEX 2, SEC. 8, PARA. A** ***a. Do the criteria adequately address data subject's right to information and require respective measures to be put in place?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q43. Upon request, do you provide confirmation of whether or not you hold PI about the requesting individual? Describe below.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to respond to such requests.* *The Applicant Organization must grant access to any individual, to PI collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.* *The Applicant Organization's processes or mechanisms for access by individuals to PI must be reasonable having regard to the manner of request and the nature of the PI.* *The PI must be provided to individuals in an easily comprehensible way.* *The Applicant Organization must provide the individual with a time frame indicating when the requested access will be granted.*	🟢 Global CBPR Program Requirements 43-44 specifically address the right to information.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	*Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q44. Upon request, do you provide individuals access to the PI that you hold about them? Where YES, answer questions 44(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 45.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES** the AA must verify each answer provided.* *The Applicant Organization must implement reasonable and suitable processes or mechanisms to enable the individuals to access their PI, such as account or contact information.* *If the Applicant Organization denies access to PI, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	*Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that it may be required to permit access by individuals to their PI. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.*	
EDPB_1-2018_29. Right to access **ANNEX 2, SEC. 8, PARA. B** ***b. Do the criteria require that data subjects are granted adequate or even greater access and control of their data including data portability?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q43. Upon request, do you provide confirmation of whether or not you hold PI about the requesting individual? Describe below.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to respond to such requests.* *The Applicant Organization must grant access to any individual, to PI collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.* *The Applicant Organization's processes or mechanisms for access by individuals to PI must be reasonable having regard to the manner of request and the nature of the PI.* *The PI must be provided to individuals in an easily comprehensible way.*	🟡 While the Global CBPR Program Requirements specifically provide a right to access information, they does not include the right to data portability.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	The Applicant Organization must provide the individual with a time frame indicating when the requested access will be granted. *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q44. Upon request, do you provide individuals access to the PI that you hold about them? Where YES, answer questions 44(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 45.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES** the AA must verify each answer provided.* *The Applicant Organization must implement reasonable and suitable processes or mechanisms to enable the individuals to access their PI, such as account or contact information.* *If the Applicant Organization denies access to PI, it must explain to the individual why access was denied, and provide the*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	appropriate contact information for challenging the denial of access where appropriate. *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that it may be required to permit access by individuals to their PI. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.*	
EDPB_1-2018_30. Right to correction/erasure **ANNEX 2, SEC. 8, PARA. C** ***c. Do criteria require measures put in place providing for the possibility to intervene in the processing operation in order to guarantee data subjects' rights and allow corrections, erasure or restrictions?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q45. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your policies/procedures in this regard below and answer questions 38 (a) – (e).** ***Assessment Criteria*** *Where the Applicant Organization answers YES to questions 45(a) – (e), the AA must verify that such policies are available and understandable in the primarily targeted economy.* *If the Applicant Organization denies correction to the individual's PI, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for*	🟢 Global CBPR Program Requirement 45 (including Q45a – Q45e) specifically addresses the right to correction, etc.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	challenging the denial of correction where appropriate. *All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual.* *Where the Applicant Organization answers **NO** to questions 45(a) – (e) and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q45.a. Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Q45.b. If an individual demonstrates that PI about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? **Q45.c. Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?** **Q45.d. Do you provide a copy to the individual of the corrected PI or provide confirmation that the data has been corrected or deleted?** **Q45.e. If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?**	
H. RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS		
EDPB_1-2018_31. Risk assessment **ANNEX 2, SEC. 9, PARA. A** ***a. Do the criteria allow and require assessing the risk to the rights and freedoms of natural persons?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?**	🟢 Global CBPR Program Requirement 4 specifically addresses risk assessments.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Assessment Criteria *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.*	
EDPB_1-2018_32. Risk assessment methodology **ANNEX 2, SEC. 9, PARA. B** ***b. Do the criteria provide or require a recognized risk assessment methodology? If appropriate, is it commensurate?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?**	🟡 The Global CBPR does not provide or require a particular risk assessment methodology, but since the Global CBPR would not override the terms of the GDPR, the GDPR's methodology could apply.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Assessment Criteria *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q41. Do you use third-party certifications or other risk assessments? Describe below.** ***Assessment Criteria*** *The AA must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these certifications or risk assessments. One*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	example is whether privacy compliance audits are carried out by the Applicant Organization and if audits are carried out, the AA must verify whether recommendations made in the audits are implemented.	
EDPB_1-2018_33. Impact assessment **ANNEX 2, SEC. 9, PARA. C** ***c. Do the criteria allow and require assessing the impact of the envisaged processing operations for the rights and freedoms of natural persons?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.*	🟢 Inasmuch as Global CBPR Program Requirement 4 requires an assessment of the "potential harm to individuals," it appears to satisfy this criterion.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle. * * * **Q41. Do you use third-party certifications or other risk assessments? Describe below.** ***Assessment Criteria*** *The AA must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant Organization and if audits are carried out, the AA must verify whether recommendations made in the audits are implemented.*	
EDPB_1-2018_34. DPIA consultation **ANNEX 2, SEC. 9, PARA. D** ***d. Do the criteria, [sic] require prior consultation concerning the remaining risks that could not be mitigated, based on the results of the Data Protection Impact Assessment (DPIA)?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?**	🟡 Given the role of the Accountability Agent in the Global CBPR Framework, the AA's review of "procedures or mechanisms implemented to identify and assess risks to the individual of harm …" could arguably encompass the "prior consultation" envisaged by this criterion.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Assessment Criteria *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q41. Do you use third-party certifications or other risk assessments? Describe below.** ***Assessment Criteria*** *The AA must verify that such **risk assessments or certifications** are undertaken at appropriate intervals, and that the Applicant Organization adjusts their security safeguards to reflect the results of these certifications or risk assessments. One*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	example is whether privacy compliance audits are carried out by the Applicant Organization and if audits are carried out, the AA must verify whether recommendations made in the audits are implemented.	
I. TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION		
EDPB_1-2018_35. Confidentiality **ANNEX 2, SEC. 10, PARA. A** ***a. Do criteria require the application of technical and organisational measures providing for confidentiality of processing operations?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they*	🟡 While the Global CBPR does not specifically address the confidentiality of the processing operations themselves, confidentiality measures regarding processing operations could arguably constitute "measures to mitigate the risk of harm" pursuant to Program Requirement 4.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	have been or will be implemented where necessary. *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.** • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Maintaining records of processing activities ___ • Other (describe) ___ ***Assessment Criteria*** *The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	processing activities which are capable of being provided upon request. *Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.* * * * **GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS** 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply. 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_36. Integrity

ANNEX 2, SEC. 10, PARA. B

b. Do criteria require the application of technical and organisational measures providing for integrity of processing operations?

GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS

Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?

Assessment Criteria

The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.

Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.

* * *

While the Global CBPR does not specifically address the integrity of the processing operations themselves, integrity measures regarding processing operations could arguably constitute "measures to mitigate the risk of harm" pursuant to Program Requirement 4.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Maintaining records of processing activities ___ • Other (describe) ___ ***Assessment Criteria*** *The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant processing activities which are capable of being provided upon request.* *Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.* * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

	GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*	
	* * *	
	THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS	
	62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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.	
	63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply.	
	64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	
EDPB_1-2018_37. Availability **ANNEX 2, SEC. 10, PARA. C** ***c. Do criteria require the application of technical and organisational measures providing for availability of processing operations?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and*	🟡 While the Global CBPR does not specifically address the "availability" of processing operations themselves (and while there is some confusion regarding what "availability" would mean in such a context), the availability of measures regarding processing operations could arguably constitute "measures to mitigate the risk of harm" pursuant to Program Requirement 4.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary. *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.** • Internal guidelines or policies (if applicable, describe how implemented) ___ • Contracts ___ • Compliance with applicable industry or sector laws and regulations ___ • Compliance with self-regulatory Applicant Organization code and/or rules ___ • Maintaining records of processing activities ___	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	• Other (describe) ___ ***Assessment Criteria*** *The AA has to verify that the Applicant Organization indicates the measures it takes to ensure compliance with the Global CBPR Privacy Principles, including that it maintains records to demonstrate compliant processing activities which are capable of being provided upon request.* *Where the Applicant Organization answers it does not maintain records of processing activities, the Accountability Agent must inform the Applicant Organization that it must have procedures in place to maintain records of processing activities.* * * *	
EDPB_1-2018_38. Transparency with respect to accountability **ANNEX 2, SEC. 10, PARA. E**[1] ***e. Do criteria require the application of measures providing for transparency of processing operations with respect to accountability?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** * * * Q6. Do you provide clear and easily accessible statements about your practices and policies that govern the PI described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	🟢 A number of Program Requirements address transparency in operations.

[1] Subparagraph (d) lacks substantive content, as it encompasses on the first part of the question: "Do criteria require the application of measures providing for transparency of processing operations with respect to [sic]." Subparagraph (e) states simply: "Accountability?"

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
	Q7. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected? Q8. Subject to the Qualifications [listed here], at the time of collection of PI, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which PI is being collected? Q9. Subject to the Qualifications [listed here], at the time of collection of PI, do you notify individuals that their PI may be shared with third parties? * * * Q13. Do you limit the use of the PI you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below. * * * Q28. Do you take steps to verify that the PI held by you is up-to-date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe. Q29. Do you have a mechanism for correcting inaccurate, incomplete and outdated PI to the extent necessary for purposes of use? Provide a	

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	description in the space below or in an attachment if necessary. * * * Q33. Have you implemented an information security policy? Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses? * * * Q38. Have you implemented a policy for secure disposal of PI? Q39. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures? * * *	
EDPB_1-2018_39. Transparency with respect to data subject rights **ANNEX 2, SEC. 10, PARA. F** ***f. Do criteria require the application of measures providing for transparency of processing operations with respect to data subject rights?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q43. Upon request, do you provide confirmation of whether or not you hold PI about the requesting individual? Describe below.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to respond to such requests.* *The Applicant Organization must grant access to any individual, to PI collected or*	🟢 Global CBPR Program Requirements 43-45 specifically address transparency obligations regarding the rights to access and correction/deletion.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	gathered about that individual, upon receipt of sufficient information confirming the individual's identity. *The Applicant Organization's processes or mechanisms for access by individuals to PI must be reasonable having regard to the manner of request and the nature of the PI.* *The PI must be provided to individuals in an easily comprehensible way.* *The Applicant Organization must provide the individual with a time frame indicating when the requested access will be granted.* *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q44. Upon request, do you provide individuals access to the PI that you hold about them? Where YES, answer questions 44(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 45.** ***Assessment Criteria***	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	*Where the Applicant Organization answers **YES** the AA must verify each answer provided.* *The Applicant Organization must implement reasonable and suitable processes or mechanisms to enable the individuals to access their PI, such as account or contact information.* *If the Applicant Organization denies access to PI, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate.* *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that it may be required to permit access by individuals to their PI. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q45. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your policies/procedures in this regard below and answer questions 38 (a) – (e).** ***Assessment Criteria***	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	Where the Applicant Organization answers YES to questions 45(a) – (e), the AA must verify that such policies are available and understandable in the primarily targeted economy. *If the Applicant Organization denies correction to the individual's PI, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.* *All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual.* *Where the Applicant Organization answers **NO** to questions 45(a) – (e) and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	verify whether the applicable Qualification is justified. **Q45.a. Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.** **Q45.b. If an individual demonstrates that PI about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?** **Q45.c. Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?** **Q45.d. Do you provide a copy to the individual of the corrected PI or provide confirmation that the data has been corrected or deleted?** **Q45.e. If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_40. Transparency with respect to assessment of individual processing operations **ANNEX 2, SEC. 10, PARA. G** ***g. Do criteria require the application of measures providing for transparency of processing operations with respect to assessment of individual processing operations, e.g. for algorithmic transparency?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** * * * Q6. Do you provide clear and easily accessible statements about your practices and policies that govern the PI described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same. * * *	🟡 While the Global CBPR does not specifically address "algorithmic transparency," such an obligation could be inferred by Program Requirement 6, which requires clear and easily accessible statements about your practices and policies …."
EDPB_1-2018_41. Measures guaranteeing data subject rights **ANNEX 2, SEC. 10, PARA. H** ***h. Do criteria require the application of technical and organisational measures guaranteeing data subjects' rights, e.g. the ability to provide information, or to data portability?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q43. Upon request, do you provide confirmation of whether or not you hold PI about the requesting individual? Describe below.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to respond to such requests.* *The Applicant Organization must grant access to any individual, to PI collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.* *The Applicant Organization's processes or mechanisms for access by individuals to PI must be reasonable having regard to the manner of request and the nature of the PI.*	🟡 While Global CBPR Program Requirements 43-45 specifically address measures relating to data subject rights, there is no provision addressing the right to data portability.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	The PI must be provided to individuals in an easily comprehensible way. *The Applicant Organization must provide the individual with a time frame indicating when the requested access will be granted.* *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q44. Upon request, do you provide individuals access to the PI that you hold about them? Where YES, answer questions 44(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 45.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES** the AA must verify each answer provided.* *The Applicant Organization must implement reasonable and suitable processes or mechanisms to enable the individuals to access their PI, such as account or contact information.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	If the Applicant Organization denies access to PI, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. *Where the Applicant Organization answers **NO** and does not identify an applicable Qualification, the AA must inform the Applicant Organization that it may be required to permit access by individuals to their PI. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q45. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your policies/procedures in this regard below and answer questions 38 (a) – (e).** ***Assessment Criteria*** *Where the Applicant Organization answers YES to questions 45(a) – (e), the AA must verify that such policies are available and understandable in the primarily targeted economy.* *If the Applicant Organization denies correction to the individual's PI, it must explain to the individual why the correction request was denied, and provide the*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	appropriate contact information for challenging the denial of correction where appropriate. *All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual.* *Where the Applicant Organization answers **NO** to questions 45(a) – (e) and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.* **Q45.a. Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Q45.b. If an individual demonstrates that PI about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? **Q45.c. Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion?** **Q45.d. Do you provide a copy to the individual of the corrected PI or provide confirmation that the data has been corrected or deleted?** **Q45.e. If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?**	
EDPB_1-2018_42. Measures guaranteeing rights of correction, erasure, restriction **ANNEX 2, SEC. 10, PARA. I** ***i. Do criteria require the application of technical and organisational measures providing for the ability to intervene into the processing operation in order to guarantee data subjects right and allow corrections, erasure or restrictions?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q45. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your policies/procedures in this regard below and answer questions 38 (a) – (e).** ***Assessment Criteria*** *Where the Applicant Organization answers YES to questions 45(a) – (e), the AA must verify that such policies are available and*	🟢 Global CBPR Program Requirements 45 et seq specifically address measures regarding the rights to correction/deletion.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	understandable in the primarily targeted economy. *If the Applicant Organization denies correction to the individual's PI, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.* *All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual.* *Where the Applicant Organization answers **NO** to questions 45(a) – (e) and does not identify an applicable Qualification, the AA must inform the Applicant Organization that the existence of written procedures to respond to such requests is required for compliance with this Privacy Principle. Where the Applicant Organization identifies an applicable Qualification, the AA must verify whether the applicable Qualification is justified.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	Q45.a. Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. **Q45.b.** If an individual demonstrates that PI about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? **Q45.c.** Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? **Q45.d.** Do you provide a copy to the individual of the corrected PI or provide confirmation that the data has been corrected or deleted? **Q45.e.** If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_43. Measures providing ability to patch or check **ANNEX 2, SEC. 10, PARA. J** ***j. Do criteria require the application of measures providing for the ability to intervene into the processing operation in order to patch or check the system or the process?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.*	🟡 Given the role of the Accountability Agent in the Global CBPR Framework, the AA's review of "procedures or mechanisms implemented to identify and assess risks to the individual of harm …" could arguably provide for the ability to intervene into the processing operation in order to patch or check the system or the process.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different

EDPB_1-2018_44. Measures to ensure data minimisation

ANNEX 2, SEC. 10, PARA. K

k. Do criteria require the application of technical and organisational measures to ensure data minimisation, for example, unlinking or separation of the data from the data subject, anonymisation or pseudonymisation or isolation of data systems?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)

* * *

Part III. Global CBPR Privacy Principles

I. PREVENTING HARM

17. Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

* * *

III. COLLECTION LIMITATION

21. The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by **lawful and fair means**, and where appropriate, with notice to, or consent of, the individual concerned.

COMMENTARY

21. This Principle limits collection of personal information by reference to the purposes for which it is collected. The collection of the personal information should be relevant to such purposes, and necessity and

🟡

While the Global CBPR Framework does not use the term "data minimisation," the concept is implied, especially in the "COLLECTION LIMITATION" Principle. Moreover,

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	proportionality to the fulfillment of such purposes may be factors in determining what is relevant. This Principle also provides that collection methods must be lawful and fair. For example, obtaining personal information under false pretenses (e.g., where an organization uses phishing, telemarketing calls, or pretexting emails to fraudulently misrepresent itself as another company in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal information) may in many Members be considered unlawful. Therefore, even in those Members where there is no explicit law against these specific methods of collection, they may be considered to be unfair means of collection. . *The Principle also recognizes that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate. For example, in a situation where there is an outbreak of food poisoning, it would be appropriate for the relevant health authorities to collect the personal information of patrons from restaurants without providing notice to or obtaining the consent of individuals in order to inform them of the potential health risk.* **IV. USES OF PERSONAL INFORMATION**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	22. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect. * * *	
EDPB_1-2018_45. Measures to implement data protection by default **ANNEX 2, SEC. 10, PARA. L** ***l. Do criteria require technical measures to implement data protection by default?***	**N/A**	🔴 The Global CBPR Framework does not address data protection by default.
EDPB_1-2018_46. Measures to implement data protection by design **ANNEX 2, SEC. 10, PARA. M** ***m. Do criteria require technical and organisational measures implementing data protection by design, e.g. a data protection management system to demonstrate, inform, control and enforce data protection requirements?***	**N/A**	🔴 The Global CBPR Framework does not address data protection by design.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_47. Measures to implement personnel training **ANNEX 2, SEC. 10, PARA. N** ***n. Do criteria require technical and organisational measures implementing appropriate periodic training and education for the personnel having permanent or regular access to personal data?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q36. Describe how you make your employees aware of the importance of maintaining the security of PI (e.g., through regular training and oversight).** ***Assessment Criteria*** *The AA must verify that the Applicant Organization's employees are aware of the importance of, and obligations respecting, maintaining the security of PI through regular training and oversight as demonstrated by procedures, which may include:* • ***Training program for employees,*** • *Regular staff meetings or other communications,* • *Security policy signed by employees, or* • *Other (specify)* *Where the Applicant Organization answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of PI through regular training and oversight, the AA has to inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.*	🟢 Several Program Requirements mandate the appropriate training and education of employees.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	Q37. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: • **Employee training and management or other organizational safeguards?** • **Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?** • **Detecting, preventing, and responding to attacks, intrusions, or other security failures?** • **Physical security?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES** (to questions 37.a. to 37.d.), the AA has to verify the existence of each of the safeguards.* *The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant Organization must employ suitable and reasonable means, such as encryption, to protect all PI.* *Where the Applicant Organization answers **NO** (to questions 37.a. to 37.d.), the AA must inform the Applicant Organization that the existence of safeguards on each*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	category is required for compliance with this Privacy Principle. * * * **Q48. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to receive, investigate and respond to privacy-related complaints, such as:* • *A description of how individuals may submit complaints to the Applicant Organization (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR* • *A designated employee(s) to handle complaints related to the Applicant Organization's compliance with the Global CBPR Framework and/or requests from individuals for access to PI; AND/OR* • *A formal complaint-resolution process; AND/OR* • *Other (must specify).* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	procedures is required for compliance with this Privacy Principle. * * * **Q51. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints.* *Where the Applicant Organization answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the AA must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_48. Measures requiring review

ANNEX 2, SEC. 10, PARA. O

o. Do criteria require reviewing measures?

GLOBAL CBPR FORUM – *ACCOUNTABILITY AGENT RECOGNITION APPLICATION*

* * *

Annex A

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

* * *

Program Requirements

4) An Accountability Agent evaluates Applicant Organizations against the Global CBPR and/or Global PRP Program Requirements ("Program Requirements"). (*NOTE*: an Accountability Agent may charge a fee to a Certified Organization for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.)

Certification Process

5) An Accountability Agent has a comprehensive process to review an Applicant Organization's policies and practices with respect to the Applicant Organization's participation in the Global CBPR and/or Global PRP Systems and to verify its compliance with the Program Requirements. The certification process includes:

   a. An initial assessment of compliance, which will include verifying the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Applicant Organization against the Program Requirements, and which may also include

The role of the Accountability Agent is to review measures that have been put in place. Moreover, the Accountability Agent has a duty to ensure ongoing monitoring and compliance of an organization's technical and organisational measures.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools; b. A comprehensive report to the Applicant Organization outlining the Accountability Agent's findings regarding the Applicant Organization's level of compliance with the Program Requirements. Where non-fulfilment of any of the Program Requirements is found, the report must include a list of changes the Applicant Organization needs to complete for purposes of obtaining certification for participation in the Global CBPR and/or Global PRP Systems; c. Verification that any changes required under paragraph 5(b) have been properly completed by the Applicant Organization; d. Certification that the Applicant Organization is in compliance with the Program Requirements; and e. Provision of the relevant details of the Certified Organization's certification for the Forum's Compliance Directory. The relevant details should include at least the following: the name of the Certified Organization, links to the Certified Organization's website and privacy policy, contact information, the name of the Accountability Agent that certified the Certified Organization and can handle consumer disputes, the name of the relevant PEA, the scope of the certification, the date that the Certified Organization was	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	first certified, and the expiry date for the current certification. **On-going Monitoring and Compliance Review Processes** 6) An Accountability Agent has 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 Program Requirements. * * * **Re-Certification and Annual Attestation** 8) An Accountability Agent will require Certified Organizations to attest on an annual basis to their continued compliance to the Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-certification. Where there has been a material change to the Certified Organization's privacy policy (as reasonably determined by the Accountability Agent in good faith), the Accountability Agent will carry out an immediate review process. This re-certification review process includes: a. An assessment of compliance, which will include verification of the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Certified Organization, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools;	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

b. A report to the Certified Organization outlining the Accountability Agent's findings regarding the Certified Organization's level of compliance with the Program Requirements. The report must also list any corrections the Certified Organization needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification;

c. Verification that required corrections have been properly completed by the Certified Organization; and

d. Notice to the Certified Organization that the Certified Organization is in compliance with the Program Requirements and has been re-certified.

GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS

Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?

Assessment Criteria

The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary. *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?** *Assessment Criteria* *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • *Authentication and access control (e.g., password protections)*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	• *Encryption* • *Boundary protection (e.g., firewalls, intrusion detection)* • *Audit logging* • ***Monitoring (e.g., external and internal audits, vulnerability scans)*** • *Other (specify)* *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.* *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	reassess its security measures to evaluate their relevance and effectiveness. *Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.*	
EDPB_1-2018_49. Measures requiring self-assessment/ internal audit **ANNEX 2, SEC. 10, PARA. P** ***p. Do criteria require self-assessment/ internal audit?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in*	🟢 The Global CBPR Program Requirements make implicit and explicit references to internal audits.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary. *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?** *Assessment Criteria* *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • *Authentication and access control (e.g., password protections)* • *Encryption* • *Boundary protection (e.g., firewalls, intrusion detection)* • *Audit logging* • ***Monitoring (e.g., external and internal audits, vulnerability scans)***	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	• *Other (specify)* *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.* *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.* *Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	required for compliance with this Privacy Principle.	
EDPB_1-2018_50. Measures requiring data breach notification **ANNEX 2, SEC. 10, PARA. Q** ***q. Do criteria require measure to ensure that personal data breach notification duties are carried out in due time and scope?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q5. Do you have a process in place to notify affected individuals without unreasonable delay if a breach is likely to result in significant harm to the affected individuals after confirming the loss, unauthorized access, destruction, use, modification or disclosure of information or other misuses of personal information? If YES, describe.** ***Assessment Criteria*** *Where the Applicant Organization answers YES, the Accountability Agent must verify that the Applicant Organization has written policies and procedures to notify affected individuals without unreasonable delay.* *Notifications to affected individuals should include information about the nature and extent of the breach and the types of information involved; steps affected individuals may take to protect themselves from potential harm; a brief description of what the Applicant Organization is doing to investigate the breach, mitigate the harm, and prevent further breaches; and contact information for the privacy personnel at the Applicant Organization.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that*	🟢 Program Requirement 5 addresses breach notification obligations.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	implementation of such policies and procedures is required for compliance with this Privacy Principle.	
EDPB_1-2018_51. Measures requiring incident management procedures **ANNEX 2, SEC. 10, PARA. R** ***r. Do criteria require incident management procedures to be in place and verified?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q37. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:** **Q37a. Employee training and management or other organizational safeguards?** **Q37b. Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?** **Q37c. Detecting, preventing, and responding to attacks, intrusions, or other security failures?** **Q37d. Physical security?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES** (to questions 37.a. to 37.d.), the AA has to verify the existence of each of the safeguards.* *The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant Organization must employ suitable and*	🟢 Incident management procedures are addressed in Program Requirement 37c., i.e., "detecting, preventing, and responding to attacks, intrusions, or other security failures."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	reasonable means, such as encryption, to protect all PI. *Where the Applicant Organization answers **NO** (to questions 37.a. to 37.d.), the AA must inform the Applicant Organization that the existence of safeguards on each category is required for compliance with this Privacy Principle.*	
EDPB_1-2018_52. Monitoring updates **ANNEX 2, SEC. 10, PARA. S** ***s. Do criteria require monitoring of evolving privacy and technology issues and updating of the scheme as required?***	**GLOBAL CBPR FORUM – *ACCOUNTABILITY AGENT RECOGNITION APPLICATION*** * * * ***Annex A*** **ACCOUNTABILITY AGENT RECOGNITION CRITERIA** * * * **On-going Monitoring and Compliance Review Processes** 6) An Accountability Agent has 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 Program Requirements. * * * **Re-Certification and Annual Attestation** 8) An Accountability Agent will require Certified Organizations to attest on an annual basis to their continued compliance to the Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the	🟡 The requirement to monitor evolving privacy and technology issues is implicit in the Accountability Agent's duty to ensure ongoing monitoring and compliance of an organization's technical and organisational measures. Moreover, certifications are subject to annual attestation and re-certification.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	re-certification. Where there has been a material change to the Certified Organization's privacy policy (as reasonably determined by the Accountability Agent in good faith), the Accountability Agent will carry out an immediate review process. This re-certification review process includes: a. An assessment of compliance, which will include verification of the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Certified Organization, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools; b. A report to the Certified Organization outlining the Accountability Agent's findings regarding the Certified Organization's level of compliance with the Program Requirements. The report must also list any corrections the Certified Organization needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification; c. Verification that required corrections have been properly completed by the Certified Organization; and d. Notice to the Certified Organization that the Certified Organization is in compliance with the Program Requirements and has been re-certified.	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

	GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	* * *	
	Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses? *Assessment Criteria* *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • *Authentication and access control (e.g., password protections)* • *Encryption* • *Boundary protection (e.g., firewalls, intrusion detection)* • *Audit logging* • ***Monitoring (e.g., external and internal audits, vulnerability scans)*** • *Other (specify)* *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	unauthorized use, alteration, disclosure, distribution, or access. *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.* *Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

J. OTHER SPECIAL DATA PROTECTION FRIENDLY FEATURES

EDPB_1-2018_53. Implementation of data protection enhancing techniques

ANNEX 2, SEC. 11, PARA. A

a. Do the criteria require the implementation of data protection enhancing techniques? This could include criteria that require enhanced data protection by eliminating or reducing personal data and/or the data protection risk.

GLOBAL CBPR FORUM – *ACCOUNTABILITY AGENT RECOGNITION APPLICATION*

* * *

Annex A

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

* * *

On-going Monitoring and Compliance Review Processes

6) An Accountability Agent has 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 Program Requirements.

* * *

Re-Certification and Annual Attestation

8) An Accountability Agent will require Certified Organizations to attest on an annual basis to their continued compliance to the Program Requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-certification. Where there has been a material change to the Certified Organization's privacy policy (as reasonably determined by the Accountability Agent in good faith), the Accountability Agent will carry out an immediate review process. This re-certification review process includes:

Although the Global CBPR Framework does not specifically refer to the use of privacy enhancing technologies, such a requirement could be implied from Accountability Agent's duty to ensure ongoing monitoring and compliance of an organization's technical and organisational measures.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	a. An assessment of compliance, which will include verification of the contents of the Global CBPR and/or Global PRP Intake Questionnaires completed by the Certified Organization, and which may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools; b. A report to the Certified Organization outlining the Accountability Agent's findings regarding the Certified Organization's level of compliance with the Program Requirements. The report must also list any corrections the Certified Organization needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification; c. Verification that required corrections have been properly completed by the Certified Organization; and d. Notice to the Certified Organization that the Certified Organization is in compliance with the Program Requirements and has been re-certified. **GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm? ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that implementation of such procedures or mechanisms is required for compliance with this Privacy Principle.* * * * **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?**	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	Assessment Criteria *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • *Authentication and access control (e.g., password protections)* • *Encryption* • *Boundary protection (e.g., firewalls, intrusion detection)* • *Audit logging* • ***Monitoring (e.g., external and internal audits, vulnerability scans)*** • *Other (specify)* *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access.* *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.	
EDPB_1-2018_54. Implementation of enhanced data subjects controls **ANNEX 2, SEC. 11, PARA. B** ***b. Do the criteria require the implementation of enhanced data subjects controls to facilitate self-determination and choice?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **Part III. Global CBPR Privacy Principles** * * * **V. CHOICE** 23. Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide	🟢 Choice is one of the key principles of the Global CBPR Framework, and Program Requirements 19 - 27 ensure the facilitation of choice.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	these mechanisms when collecting publicly available information. * * * **GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** Q19. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the collection of their PI? Where YES describe such mechanisms below. Q20. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the use of their PI? Where YES describe such mechanisms below. Q21. Subject to the Qualifications [listed here], do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their PI? Where YES describe such mechanisms below. Q22. As applicable, do you permit individuals to exercise choice in relation to receiving direct marketing at any time? If YES, describe. Q23. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or disclosure (question 21) of their PI, are they displayed or provided in a clear and conspicuous manner? Q24. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	disclosure (question 21) of their PI, are they clearly worded and easily understandable? Q25. When choices are provided to the individual offering the ability to limit the collection (question 19), use (question 20) and/or disclosure (question 21) of their PI, are these choices easily accessible and affordable? Where YES, describe. Q26. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below. Q27. Subject to the Qualifications described below, do you permit individuals to withdraw consent where the information is no longer needed by the organization for the purposes for which consent was provided, and do you have procedures to respond to individuals' requests to cease the use or disclosure of their personal information?	
K. ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL		
EDPB_1-2018_55. Covers all member states **ANNEX 2, SEC. 13, PARA. A** ***a. Do the criteria envisage covering all Member States?***	**GLOBAL CBPR FORUM TERMS OF REFERENCE (2023)** * * * **ANNEX A** **Admission of Members and Associates to the Global CBPR Forum** 1. A jurisdiction interested in participating in the Global CBPR Forum ("Applicant") should contact	🟢 Participation in the Global CBPR Forum is open to all Member States and to the EU as a whole.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	the Chair of the Membership Committee in writing to indicate which form of participation it seeks and to initiate preparations for its application. Upon receipt of a request to initiate consultations, the Chair of the Membership Committee should promptly notify the Global Forum Assembly ("GFA") of the Applicant's interest. 2. As part of the consultations, the Chair of the Membership Committee should confirm with the Applicant the applicable form of participation. *Criteria for Membership* 3. After consulting with the Chair of the Membership Committee, the Applicant should provide an application that includes a letter of intent confirming that the Applicant: (a) Concurs with the principles and objectives of the Global CBPR Forum ("Forum") set forth in the 2022 Global CBPR Declaration and the Global CBPR Framework, and demonstrates alignment of its domestic legal system with the Global CBPR Framework; (b) Has at least one Privacy Enforcement Authority as a participant in the Global Cooperation Arrangement for Privacy Enforcement ("Global CAPE"); and (c) Either: (i) Intends to make use of at least one Forum-recognized Accountability Agent ("AA"), and submits an explanation of	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	how the Global CBPR and/or Global PRP program requirements may be enforced in its jurisdiction; Or (ii) Demonstrates 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 Forum-recognized AA. * * *	
EDPB_1-2018_56. Takes into account Member State law **ANNEX 2, SEC. 13, PARA. B** ***b. Are the criteria able to take into account Member State data protection law or scenarios?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS** 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified	🟢 The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations, and participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply. 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
EDPB_1-2018_57. Takes into account sector specific Member State data protection law **ANNEX 2, SEC. 13, PARA. C** ***c. Do the criteria require an evaluation of the individual ToE with respect to sector specific Member State data protection law?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **Part II. Scope** 5. The purpose of Part II of the Global CBPR Framework is to make clear the extent of coverage of the Global CBPR Privacy Principles contained in Part III of this Framework. * * * ADDITIONAL DEFINITIONS 9. **Data Protection and Privacy Laws** means laws and regulations of a Member, the enforcement of which have the effect of protecting personal information consistent with the Global CBPR Framework. *COMMENTARY* *9. Data Protection and Privacy Laws come in a variety of forms. Some are general privacy or data protection statutes while others take a sectoral approach covering particular areas such as credit reporting or health information. In some cases, the relevant legal provisions are contained within broader laws dealing with such issues as telecommunications or consumer protection. It is not important for the purposes of the definition what the laws are called: it is the effect of the laws that matters.*	🟢 The Global CBPR Framework recognizes that "Data Protection and Privacy Laws come in a variety of forms. Some are general privacy or data protection statutes while others take a sectoral approach covering particular areas such as credit reporting or health information…. It is not important for the purposes of the definition what the laws are called: it is the effect of the laws that matters."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_58. Provide processing information in local languages

ANNEX 2, SEC. 13, PARA. E

e. Do the criteria require the controller or processor to provide information to data subjects and interested parties in the languages of Member States on the processing/ToE?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*

* * *

THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS

62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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.
63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply.
64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional

The Global CBPR does not specifically address language requirements, but since the Global CBPR would not override the terms of the domestic laws and the language requirements contained therein, compliance with this criterion can be implied.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	
EDPB_1-2018_59. Provide documentation in local languages **ANNEX 2, SEC. 13, PARA. F** ***f. Do the criteria require the controller or processor to provide information to data subjects and interested parties in the languages of Member States [on] documentation of the processing/ToE?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS** 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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	🟡 The Global CBPR does not specifically address language requirements, but since the Global CBPR would not override the terms of the domestic laws and the language requirements contained therein, compliance with this criterion can be implied.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	necessary elements for the Global CBPR and/or PRP Systems are in place. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply. 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	compliance with applicable domestic legal requirements.	
EDPB_1-2018_60. Provide results of evaluation in local languages **ANNEX 2, SEC. 13, PARA. G** ***g. Do the criteria require the controller or processor to provide information to data subjects and interested parties in the languages of Member States [on] the results of the evaluation?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS** 62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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. 63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply.	🟡 The Global CBPR does not specifically address language requirements, but since the Global CBPR would not override the terms of the domestic laws and the language requirements contained therein, compliance with this criterion can be implied.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.	
L. OVERALL EVALUATION OF CRITERIA		
EDPB_1-2018_61. Certification can be trusted **ANNEX 2, SEC. 14, PARA. A** ***a. Do the criteria fully cover the scope of the certification mechanism (i.e. comprehensive criteria) to provide sufficient guarantees so that the certification can be trusted?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** **Part I. Preamble** *Recognising* that growing Internet connectivity and the digitisation of the global economy have resulted in the rapid increase in the collection, use, and transfer of data across borders, a trend that continues to accelerate;	🟢 The purpose of the Global CBPR is to facilitate "trusted cross border data flows."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY*: = Aligned; = Similar; = Different**
	***Conscious* that trusted cross-border data flows are indispensable** – not just for big, multinational technology companies, but for companies across all sectors of the economy, and for micro, small- and medium-sized businesses, workers, and consumers as well; *Believing* that cross-border data flows increase living standards, create jobs, connect people in meaningful ways, facilitate vital research and development in support of public health, foster innovation and entrepreneurship, and allow for greater international engagement; *Acknowledging* that regulatory barriers threaten to undermine opportunities created by the digital economy at a time when companies are relying increasingly on digital technologies and innovations to continue business operations and recover economically; *Recognising* the importance of strong and effective data protection and privacy in **strengthening consumer and business trust in digital transactions**; *Acknowledging* the important contribution made by the Asia-Pacific Economic Cooperation (APEC) in developing the APEC CBPR System to foster cross-border data flows and interoperability; * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_62. Certification criteria commensurate to size, sensitivity, risk **ANNEX 2, SEC. 14, PARA. B** ***b. Are the criteria commensurate with the size of the processing operation being addressed by the scope of the certification mechanism, the sensitivity of information and the risk of processing?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q1. Do you take steps to identify and provide appropriate additional safeguards for personal information that is considered sensitive or categorized to require special protection based on the laws governing your collection or processing of the personal information or where an organization transferring the personal information to you has identified it as such? If YES, describe.** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization has written policies and procedures that demonstrate that the Applicant Organization has taken steps to determine whether all or some of the information it collects or receives is considered sensitive or categorized to require special protection under the law governing the collection, processing or disclosure or whether it processes information transferred from an organization that has identified it as such and to apply the appropriate safeguards to the processing of such information as required. Due to its sensitive nature the safeguards should be applied to information in this category with more care compared to the safeguards applied to other types of personal information.* *Where an Applicant Organization answers NO, the Accountability Agent must inform*	The Global CBPR takes into account issues of sensitivity and proportionality.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle if the Applicant Organization processes sensitive personal information. * * * **Q4. Do you have procedures/mechanisms in place to identify and assess the risks of misuse of personal information, and therefore potential harm to individuals, that may result from your data processing operations and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of potential harm?** ***Assessment Criteria*** *The Accountability Agent must verify that the Applicant Organization provides a description of the procedures or mechanisms implemented to identify and assess risks to the individual of harm that may result from misuse of personal information and to implement measures to mitigate the risk of harm, proportionate to the likelihood and severity of harm threatened. The Accountability Agent will verify that procedures or mechanisms are in place to allow the Applicant Organization to document the risk assessment and that they have been or will be implemented where necessary.* *Where an Applicant Organization answers NO, the Accountability Agent must inform the Applicant Organization that*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	implementation of such procedures or mechanisms is required for compliance with this Privacy Principle. * * * **Q34. Describe the physical, technical and administrative safeguards you have implemented to protect PI against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?** ***Assessment Criteria*** *Where the Applicant Organization provides a description of the physical, technical and administrative safeguards used to protect PI, the AA must verify the existence of such safeguards, which may include:* • Authentication and access control (e.g., password protections) • Encryption • Boundary protection (e.g., firewalls, intrusion detection) • Audit logging • Monitoring (e.g., external and internal audits, vulnerability scans) • Other (specify) *The Applicant Organization must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant Organization's size and*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	complexity, the nature and scope of its activities, and the sensitivity of the PI and/or Third Party PI it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. *Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held.* *The Applicant Organization must take reasonable measures to require information processors, agents, contractors, or other service providers to whom PI is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant Organization must periodically review and reassess its security measures to evaluate their relevance and effectiveness.* *Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect PI, the AA must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy Principle.* * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB_1-2018_63. Certification likely to improve compliance

ANNEX 2, SEC. 14, PARA. C

c. Are the criteria likely to improve data protection compliance of controllers and processors?

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*

* * *

THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS

62. The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. 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.
63. Participation in the Global CBPR and/or Global PRP System does not replace a certified organization's domestic legal obligations. The commitments which a certified organization carries out in order to participate in the Global CBPR and/or Global PRP Systems are separate from any domestic legal obligations that may be applicable. Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply.
64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional

An Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements.

That said, it can simplify compliance for personal information controllers and processors.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
	requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. 65. For the purposes of participation in the Global CBPR and/or Global PRP Systems, an Accountability Agent's verification only applies to a certified organization's compliance with the Global CBPR and/or Global PRP Systems, not its compliance with applicable domestic legal requirements. **GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **V. Interoperability with data protection and privacy frameworks** 68. Members should promote interoperability of the Global CBPR System and PRP System with other data protection and privacy frameworks that give practical effect to this Framework. 69. Improving the global interoperability of data protection and privacy frameworks can bring benefits in improved personal information flows, help ensure that data protection and privacy requirements are maintained when	

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	personal information flows beyond Members and can **simplify compliance for personal information controllers and processors**. Global interoperability can also assist individuals to assert their personal information and privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.	
EDPB_1-2018_64. Certification benefits data subjects **ANNEX 2, SEC. 14, PARA. D** ***d. Will data subjects benefit in respect of their information rights, including explaining desired outcomes to data subjects?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS** **Q48. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to receive, investigate and respond to privacy-related complaints, such as:* • *A description of how individuals may submit complaints to the Applicant Organization (e.g., Email/Phone/Fax/Postal Mail/Online Form); AND/OR* • *A designated employee(s) to handle complaints related to the Applicant Organization's compliance with the Global CBPR Framework and/or requests from individuals for access to PI; AND/OR*	🟢 The series of Program Requirement questions pertaining to accountability ensure that data subjects have access to **complaint and dispute resolution** mechanisms.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	• *A formal complaint-resolution process; AND/OR* • *Other (must specify).* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.* **Q49. Do you have procedures in place to ensure individuals receive a timely response to their complaints?** *Assessment Criteria* *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place to ensure individuals receive a timely response to their complaints.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy Principle.* **Q50. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.** ***Assessment Criteria*** *The AA must verify that the Applicant Organization indicates what remedial action is considered.*	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
	51. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe. ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints.* *Where the Applicant Organization answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the AA must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.*	

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

II. EDPB GUIDELINES 07/2022

The following criteria are taken from Section 3.2 of Guidelines 07/2022.

A. ASSESSMENT OF THE THIRD COUNTRY LEGISLATION

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
EDPB_7-2022_1. Assessment of third country rules **GUIDELINES, SEC. 3.2, SUBTITLE. 1** ***a) Do the criteria require the importer to have assessed the rules and practices of the third country where it operates and whether they prevent the importer from complying with its commitments under the certification?***	N/A	**- NOT RELEVANT** The Global CBPR System does not envisage an assessment of jurisdictions' rules and practices, as jurisdictions participating in the System are agreeing to a certification that promotes interoperability and helps bridge different regulatory approaches to data protection and privacy.
EDPB_7-2022_2. Documentation of third country assessment **GUIDELINES, SEC. 3.2, SUBTITLE. 1** ***b) Do the criteria require the importer to document the assessment of the rules and practices of the third country where it operates and keep the documentation available to the certification body and upon request to the SA in the EEA competent for the data exporter and to the data exporter?***	N/A	**- NOT RELEVANT** The Global CBPR System does not need documentation of country-by-country assessments, as jurisdictions participating in the System are agreeing to a certification that promotes interoperability and helps bridge different regulatory approaches to data protection and privacy.
EDPB_7-2022_3. Appropriate safeguards	N/A	**- NOT RELEVANT**

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
GUIDELINES, SEC. 3.2, SUBTITLE. 1 ***c) Do the criteria require the importer to have identified and implemented the organisational and technical measures to provide the appropriate safeguards under Article 46 GDPR taking into account the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data?***		The Global CBPR System itself would constitute an "appropriate safeguard" pursuant to GDPR Art. 46, para. 2(f), i.e., an approved certification mechanism.
EDPB_7-2022_4. Documentation of safeguards **GUIDELINES, SEC. 3.2, SUBTITLE. 1** ***d) Do the criteria require the importer to document the organisational and technical measures effectively implemented to provide the appropriate safeguards under Article 46 GDPR and keep the documentation available to the certification body and upon request to the competent data protection authorities and to the data exporter?***	N/A	⚪ **- NOT RELEVANT** The Global CBPR System itself would constitute an "appropriate safeguard" pursuant to GDPR Art. 46, para. 2(f); no separate documentation would be required.
EDPB_7-2022_5. Security measures **GUIDELINES, SEC. 3.2, SUBTITLE. 1** ***e) Do the criteria require the importer to have identified and implemented the organisational and technical measures to ensure the security of the personal data transferred, taking into account the "Recommendations 01/2020 on***	N/A	⚪ **- NOT RELEVANT** The Global CBPR System itself already identifies and requires the implementation of organisational and technical measures to ensure the security of the personal data transferred.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" if the transit is included in the scope of certification as a tool for transfers?		
EDPB_7-2022_6. Warranty **GUIDELINES, SEC. 3.2, SUBTITLE. 1** ***f) Do the criteria require a warranty to the certification body and the exporter that the importer has no reason to believe that the legislation and practices applicable to it may prevent it from fulfilling its obligations under the certification?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **IV. Cross-border transfers** 66. A Member should refrain* from restricting cross border flows of personal information between itself and another Member where (a) the other Member has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the Global CBPR System) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it. * *Cross border data flows remain subject to members' applicable domestic laws, regulations, and international agreements and commitments.* 67. Any restrictions to cross-border flows of personal information should be proportionate	⚪ **- NOT RELEVANT** Under the Global CBPR System, the importer would be located in a member jurisdiction that has already agreed to the terms and principles of Global CBPR Framework.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross-border transfer. * * *	
B. GENERAL OBLIGATIONS OF EXPORTERS AND IMPORTERS		
EDPB_7-2022_7. Contract with description of specific transfer **GUIDELINES, SEC. 3.2, SUBTITLE. 2** ***a) Do the criteria require to lay down in contractual agreements (e.g. in an existing service contract) between exporters and importers a description of the specific transfer to which the certification applies and that third-party beneficiary rights are recognised to the concerned data subjects?***	N/A	⚪ **- NOT RELEVANT** Under the Global CBPR System, certification ensures that practices are in place to ensure that all transfers abide by the System's Program Requirements.
EDPB_7-2022_8. Contract subject to evaluation **GUIDELINES, SEC. 3.2, SUBTITLE. 2** ***b) Insofar as the criteria require a specific content for these contractual agreements or instruments and a template is provided, do the criteria require that they also be the subject of the evaluation?***	N/A	⚪ **- NOT RELEVANT** Under the Global CBPR System, certification ensures that practices have been evaluated by an Accountability Agent and are compliant with System's Program Requirements.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

C. RULES ON ONWARD TRANSFERS

EDPB_7-2022_9. Onward transfers

GUIDELINES, SEC. 3.2, SUBTITLE. 3

a) Do the criteria require that onward transfers are subject to specific safeguards in line with Chapter V GDPR requirements so as to ensure that the level of protection ensured in the EEA will not be undermined and do the criteria require that appropriate documentation is kept available to the certification body and the SA in the EEA competent for the data exporter(s) and to the data exporter upon request?

GLOBAL CBPR PROGRAM REQUIREMENT QUESTIONS

Q46. What measures do you take to ensure compliance with the Global CBPR Privacy Principles? Please check all that apply and describe.

- Internal guidelines or policies (if applicable, describe how implemented) ___
- Contracts ___
- Compliance with applicable industry or sector laws and regulations ___
- Compliance with self-regulatory Applicant Organization code and/or rules ___
- Maintaining records of processing activities ___
- Other (describe) ___

GLOBAL CBPR PROGRAM REQUIREMENT QUESTION

Q53. Do you have mechanisms in place with PI processors, agents, contractors, or other service providers pertaining to PI they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?

- **Internal guidelines or policies ___**
- **Contracts ___**

While Global CBPR Program Requirement 53 requires mechanisms to be in place to ensure that obligations are assumed by "agents, contractors, or other service providers," nothing specifically addresses onward transfers of personal data to another third country.

That said, Program Requirement 46 addresses the maintenance of records of processing activities.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	• **Compliance with applicable industry or sector laws and regulations ___** • **Compliance with self-regulatory Applicant Organization code and/or rules ___** • **Others (describe) ___** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify the existence of each type of agreement described.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that implementation of such agreements is required for compliance with this Privacy Principle.*	
D. REDRESS AND ENFORCEMENT		
EDPB_7-2022_10. Redress in EEA court or international organisation **GUIDELINES, SEC. 3.2, SUBTITLE. 4** ***a) Do the criteria provide that data subjects can enforce their rights as third-party beneficiaries against the data importer before the EEA court of the data subject's habitual residence, or with an international organisation, including for compensation for damage suffered by the data subject in case of non-compliance by the importer with the relevant Certification scheme?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **OPERATION OF THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS** * * * **ELEMENT 4 – ENFORCEMENT** 25. PEAs should be able to (a) review a Global CBPR complaint/issue and, as appropriate, a Global PRP complaint/issue, if it cannot be resolved by	🟡 Generally speaking, the Global CBPR System is enforceable by Accountability Agents and Privacy Enforcement Authorities (PEAs)—which in the case of the EU would be supervisory authorities. That said, redress is first available from the certified organization, as Program Requirement 48 requires organizations to have procedures in place to receive, investigate, and respond to privacy-related complaints. The Global CBPR's *POLICIES, RULES AND GUIDELINES clarifies that:*

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	the certified organization in the first instance or by the Accountability Agent and (b) when appropriate, investigate and take enforcement action. ***Global CAPE*** 26. The Global CAPE aims to: • facilitate information sharing among PEAs globally; • provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of Global CBPR System Program Requirements, Global PRP System Program Requirements (where applicable), and Data Protection and Privacy Laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions; and • encourage information sharing and cooperation on data protection and privacy investigation and enforcement with PEAs globally, including by ensuring that the Global CAPE can work seamlessly with similar arrangements at the global level. 27. The Global CAPE creates a framework for the voluntary sharing of information and provision of assistance for data protection and privacy enforcement related activities. Any PEA may participate. Participating PEAs may contact each other for assistance or to make referrals regarding information privacy investigations	• Accountability Agents should be able to enforce the Global CBPR System Program Requirements through law or contract; and • The PEAs should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements. As for specific remedies, the Framework provides that " appropriate remedies … could include redress, the ability to stop a violation from continuing, and other remedies." Furthermore, in determining the range of remedies, member jurisdictions should take a number of factors into account including: a) the particular system in that Member that provides data protection and privacy (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems); and b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	and enforcement matters that involve each other's jurisdictions. For example, during an investigation, a PEA in jurisdiction X may seek the assistance of a PEA in jurisdiction Y, if certain evidence of the alleged data protection and privacy violation (or the entity being investigated or a controller on whose behalf a processor under investigation is acting) is located in jurisdiction Y. In that case, the PEA in jurisdiction X may send a Request for Assistance to the point of contact in the PEA in jurisdiction Y. The PEA in jurisdiction Y may then consider the matter and provide assistance on a discretionary basis. ***Global CBPR System Enforcement*** 28. The Global CBPR System should be enforceable by Accountability Agents and PEAs: • Accountability Agents should be able to enforce the Global CBPR System Program Requirements through law or contract; and • The PEAs should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements. ***Global PRP System Enforcement*** 29. While the Global PRP System provides a mechanism for cross-border data transfers that may satisfy the data transfer restrictions and limitations of applicable Data Protection and	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	Privacy Laws, nothing in the Global PRP System changes the allocation of responsibility in the controller-processor relationship under applicable laws, the Global CBPR Framework or the Global CBPR System. 30. Under the Accountability principle in the Global CBPR Framework and the Global CBPR System, controllers are responsible for the activities processors perform on their behalf and they will remain so even when contracting with a Global PRP-recognized Processor. Thus, Processors' activities remain subject to enforcement through enforcement against the controllers. This means that Global CBPR-certified Controllers must apply due diligence in selecting their processors and engage in appropriate oversight over their processors, regardless of whether the processors are Global PRP-recognized. 30. Under the Data Protection and Privacy Laws of some Members, due to differences in scope and controller and processor liability regimes, Processors recognized under the Global PRP System may not be subject to direct government backstop enforcement in the same way that all Global CBPR-certified Controllers are subject to such enforcement. However, the Global PRP System is still subject to other means of enforcement as set forth in Paragraph 31. 31. There are a number of oversight and enforcement mechanisms, either through contract or by law, available across the	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	Members to ensure the effective oversight of Processors recognized under the Global PRP System. These may include: • Where applicable, direct PEA backstop enforcement of the processor's compliance with the Global PRP System Program Requirements; • Enforcement by contract between the Accountability Agent and the Processor, whereby the Accountability Agent assumes primary responsibility for enforcing the Processor's compliance with the Global PRP System Program Requirements; • Government oversight of an Accountability Agent, and enforcement by the GFA via the Accountability Agent Oversight and Engagement Committee's ("**AA Committee**") authority to recommend to the GFA the suspension of an Accountability Agent in the event the Accountability Agent fails to perform its obligations under the Accountability Agent Recognition Criteria; and • **Mechanisms that can have the effect of enforcing data protection and privacy, such as private rights of action, and third-party beneficiary rights for enforcement authorities under the contracts between the Accountability Agents and the processors.** * * *	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: = Aligned; = Similar; = Different
	THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS AND DOMESTIC LAWS AND REGULATIONS * * * 64. Where requirements of the Global CBPR and/or Global PRP Systems exceed the requirements of domestic laws and regulations, a certified organization needs to carry out such additional requirements in order to participate in the Global CBPR and/or Global PRP Systems. Nonetheless, **PEA(s) of that Member should have the ability to take enforcement actions under applicable domestic laws and regulations** that have the effect of protecting personal information consistent with the Global CBPR System Program Requirements and where possible, the Global PRP System Program Requirements. * * * **GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **II. Giving Effect to the Global CBPR Framework** 34. There are several options for giving effect to the Framework and securing data protection and privacy for individuals, including legislative, administrative, industry self-regulatory or a combination of these policy instruments. In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various models of enforcement,	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	including through Privacy Enforcement Authorities, multi-agency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as Members deem appropriate. 35. The means of giving effect to the Framework will often differ between Members. A Member may determine that different Global CBPR Privacy Principles call for different means of domestic implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatible data protection and privacy approaches among Members that are respectful of individual Members' requirements. 36. Members should adopt non-discriminatory practices in giving effect to the Framework's principles and in protecting individuals from data protection and privacy violations occurring in that Member's jurisdiction. For example, Members should ensure that laws or other approaches that give effect to the protections in the Framework do not impede individuals living in other jurisdictions from benefitting from those protections. 37. Coordination across government agencies and other stakeholders is important to identify ways to strengthen data protection and privacy without creating obstacles to national security, public safety, and other public policy objectives. 38. Members should maintain Privacy Enforcement Authorities. These Privacy Enforcement Authorities should be provided with the	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions in an objective, impartial and consistent basis.

39. Privacy Enforcement Authorities may find it useful to apply a risk-based approach to selected oversight efforts and, where permitted, to prioritize their enforcement efforts according to the likelihood and severity of harm that might result from data protection and privacy violations or from an action taken or proposed.

* * *

Part IV. Implementation

* * *

VII. Providing for appropriate remedies in situations where data protection and privacy are violated

50. A Member's system of data protection and privacy should include appropriate remedies for data protection and privacy violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for data protection and privacy violations, Members should take a number of factors into account including:

    a) the particular system in that Member that provides data protection and privacy (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

	action, industry self-regulation, or a combination of systems); and b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations. 51. A Member should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable. **GLOBAL CBPR FORUM - ACCOUNTABILITY AGENT RECOGNITION APPLICATION** * * * **ANNEX A: *Accountability Agent Recognition Criteria*** * * * ***Mechanism for Enforcing Program Requirements*** 11) An Accountability Agent has the authority to enforce its program requirements against Certified Organizations, either through contract or by law. 12) An Accountability Agent has a process in place for notifying Certified Organizations	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	immediately of non-compliance with the Program Requirements and for requiring Certified Organizations to remedy the non-compliance within a specified time period. 13) An Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Certified Organization has not complied with the Program Requirements and has failed to remedy the non-compliance within a specified time period. [*NOTE*: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.] a. Requiring Certified Organizations to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall terminate the Certified Organization's certification. b. Temporarily suspending the Certified Organization's right to display the Accountability Agent's seal. c. Naming the Certified Organization and publicizing the non-compliance. d. Referring the violation to the relevant PEA(s). [*NOTE*: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]	

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	e. Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent. 14) An Accountability Agent will 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 Organization's failure to remedy a non-compliance with the Program Requirements within a reasonable time (under the procedures established by the Accountability Agent pursuant to paragraph 12) can be a violation of applicable law. 15) Where possible, an Accountability Agent will respond to requests from PEAs and other relevant government entities of a Member that reasonably relate to that Member and to the Global CBPR or Global PRP Systems-related activities of the Accountability Agent. * * *	
EDPB_7-2022_11. Liability in EEA **GUIDELINES, SEC. 3.2, SUBTITLE. 4** ***b) Do the criteria enable adequately assessing that an importer is liable in the EEA for the harm suffered by the data subject in case of non-compliance with the relevant Certification scheme?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **Part IV. Implementation** * * * **VII. Providing for appropriate remedies in situations where data protection and privacy are violated**	🟢 The Framework provides flexibility for Member jurisdictions, permitting them to take into account "the particular system in that Member that provides data protection and privacy (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems)."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	50. A Member's system of data protection and privacy should include appropriate remedies for data protection and privacy violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for data protection and privacy violations, Members should take a number of factors into account including: a) the particular system in that Member that provides data protection and privacy (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems); and b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.	
EDPB_7-2022_12. Lodge complaint with supervisory authority **GUIDELINES, SEC. 3.2, SUBTITLE. 4** ***c) Do the criteria require that data subjects can lodge a complaint against the importer with a supervisory authority in the EEA, in particular in the EEA State of his or her habitual residence, place of work or competent for the data exporter(s)?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **OPERATION OF THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS** * * * **ELEMENT 4 – ENFORCEMENT** 25. PEAs should be able to (a) review a Global CBPR complaint/issue and, as appropriate, a Global	🟡 Data subjects may lodge a complaint with a supervisory authority, but only after seeking recourse from the certified organization in the first instance and the Accountability Agent thereafter. That said, the System's Policies, Rules And Guidelines are clear: "The Global CBPR and Global PRP Systems do not displace or change a Member's domestic laws and regulations. … Where domestic legal obligations exceed what is expected in the Global CBPR and/or Global PRP System, the full extent of such domestic laws and regulations continues to apply."

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	PRP complaint/issue, if it cannot be resolved by the certified organization in the first instance or by the Accountability Agent and (b) when appropriate, investigate and take enforcement action.	
EDPB_7-2022_13. Cooperation with supervisory authority **GUIDELINES, SEC. 3.2, SUBTITLE. 4** ***d) Do the criteria require that the importer will cooperate with the supervisory authority in the EEA competent for the data exporter(s) and accept to be audited and to be inspected by it (them), take into account its (their) advice and abide by its (their) decisions?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) AND GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEMS - *POLICIES, RULES AND GUIDELINES*** * * * **OPERATION OF THE GLOBAL CBPR AND GLOBAL PRP SYSTEMS** * * * **ELEMENT 4 – ENFORCEMENT** 25. PEAs should be able to (a) review a Global CBPR complaint/issue and, as appropriate, a Global PRP complaint/issue, if it cannot be resolved by the certified organization in the first instance or by the Accountability Agent and (b) when appropriate, investigate and take enforcement action. * * * **GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **II. Giving Effect to the Global CBPR Framework** * * *	🟡 Given that supervisory authorities retain investigatory and enforcement powers, cooperation with them is implied.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
	42. Personal information controllers should be prepared to demonstrate their data protection and privacy management programmes at the request of a competent Privacy Enforcement Authority of that Member or in response to a valid request by another appropriate entity, such as an Accountability Agent designated under the Global CBPR Forum or under an industry code of conduct giving effect to the Framework.	
E. PROCESS AND ACTIONS FOR SITUATIONS IN WHICH NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH COMMITMENTS TAKEN AS PART OF CERTIFICATION		
EDPB_7-2022_14. Effect of changes in legislation **GUIDELINES, SEC. 3.2, SUBTITLE. 5** ***a) Do the criteria require a commitment that where the data importer in a third country or an international organisation has reasons to believe that changes in the legislation and practices applicable to it may prevent it from fulfilling its obligations under the certification, it will promptly notify this to the certification body and to the data exporter, so that the latter can evaluate whether to immediately stop the transfers?***	**GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK (2023)** * * * **VIII. Reporting Domestic Implementation of the Global CBPR Framework** 52. Members should provide timely notice to the Global Forum Assembly on their domestic implementation of the Framework**, including any new laws or regulations and any amendments to existing laws or regulations**, as well as all other developments that may affect the operation and enforcement of the Global CBPR System and/or Global PRP System.	⚪ **- NOT RELEVANT** The obligation to notify about changes to legislation rests with the member jurisdiction, not with the data importer.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 = Aligned; 🟡 = Similar; 🔴 = Different
EDPB_7-2022_15. Requests for information from third country authorities **GUIDELINES, SEC. 3.2, SUBTITLE. 5** ***b) Do the criteria require a description of the steps to be taken (including notifying the exporter in the EEA and taking appropriate additional measures) if the data importer becomes aware of legislation or practises of a third country that prevents compliance with the obligations under the certification, as well as the measures to be taken in case of requests for information from third country authorities (including the obligation to review and, when necessary, challenge the legality of the request and to minimise any information disclosed)?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q52. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI, as well as provide the necessary training to employees regarding this subject.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.*	🟡 Global CBPR Program Requirement 52 ensures that procedures are in place for responding to judicial or other government subpoenas, warrants or orders, which arguably covers the intent of this criterion.
F. DEALING WITH REQUESTS FOR DATA ACCESS BY THIRD COUNTRY AUTHORITIES		
EDPB_7-2022_16. Duty to inform of requests for information from third country authorities **GUIDELINES, SEC. 3.2, SUBTITLE. 6** ***a) Do the criteria require that the data importer will promptly inform the data exporter in case of requests for access by third country authorities and take appropriate additional measures?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q52. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant*	🟡 Global CBPR Program Requirement 52 ensures that procedures are in place for responding to judicial or other government subpoenas, warrants or orders, but it doesn't specifically mention a duty to inform. That said, such a requirement could be inferred.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS
*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information		**KEY***: 🟢 **= Aligned;** 🟡 **= Similar;** 🔴 **= Different**
	Organization has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI, as well as provide the necessary training to employees regarding this subject. *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.*	
EDPB_7-2022_17. Response to access requests from third country authorities **GUIDELINES, SEC. 3.2, SUBTITLE. 6** ***b) Do the criteria require that transfers as a result of disproportionate access requests by third country public authorities, in particular requests that require massive and indiscriminate transfers of personal data, should not take place?***	**GLOBAL CBPR PROGRAM REQUIREMENT QUESTION** **Q52. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI?** ***Assessment Criteria*** *Where the Applicant Organization answers **YES**, the AA must verify that the Applicant Organization has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of PI, as well as provide the necessary training to employees regarding this subject.* *Where the Applicant Organization answers **NO**, the AA must inform the Applicant Organization that such procedures are required for compliance with this Privacy Principle.*	🟡 Global CBPR Program Requirement 52 ensures that procedures are in place for responding to judicial or other government subpoenas, warrants or orders, but it doesn't specifically mention under what circumstances a government access request should be denied. That said, such a requirement could be inferred.

EDPB GUIDELINES	GLOBAL CBPR/PRP	COMMENTS

*ABBREVIATIONS: **AA** = Accountability Agent; **PI** = Personal Information

KEY*: = Aligned; = Similar; = Different

G. ADDITIONAL SAFEGUARDS CONCERNING THE EXPORTER

EDPB_7-2022_18. Supplementary measures

GUIDELINES, SEC. 3.2, SUBTITLE. 7

a) Do the criteria require that, where so envisaged, the data importer ensures, also by way of binding requirements in this respect for the data exporter, that the supplementary measures it has identified are matched by corresponding supplementary measures on the part of the data exporter, taking into account the EDPB Recommendations 01/2020 and the use cases, in order to ensure an effective implementation of the importer's supplementary measures?

N/A

- NOT RELEVANT

The obligation to ensure "supplementary measures" would not apply in the context of transfers pursuant to the Global CBPR System, as the need to identify supplementary measures only arises when an exporter must undertake "the complex task of assessing third countries." See EDPB Recommendations 01/2020. No such assessment needs to take place under the System, since the "third country" would already be a member of the Global CBPR Forum.