

Roundtable of G7 Data Protection and Privacy Authorities

Comparative analysis of core elements of GDPR certification as a tool for transfers and the Global CBPR System

11 October 2024

Purpose of this document:

This comparative analysis has been developed by G7 Data Protection and Privacy Authorities (DPAs) as part of the work of the Data Free Flow with Trust (DFFT) working group and assesses differences as well as commonalities between EU certification criteria to be used as a tool for transfers from Controllers to Controllers (GDPR Certification, based upon European Data Protection Board (EDPB) Guidelines¹) and the Global Cross-Border Privacy Rules System² (Global CBPR System). The aim of the document is to contribute to the current dialogue on elements of convergence and future interoperability of global and regional instruments for cross-border data transfers in various international fora. A similar work is also being carried out with respect to model contractual clauses within the Global Frameworks and Standards Working Group (GFSWG) of the Global Privacy Assembly (GPA).

This comparative analysis is without prejudice to the individual approval of GDPR Certification mechanisms by accredited certification bodies or by national DPAs in line with EU data protection law or the certification of organizations by Global CBPR Forum recognized Accountability Agents. It is also without prejudice to enforcement actions by the relevant supervisory authorities. This comparative analysis has a descriptive aim and does not provide an exhaustive list of requirements applicable to the systems and should not be taken as legal advice and it does not reflect the official position of any organization that participated in its development.

¹ EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation; EDPB Guidelines 07/2022 on certification as a tool for transfers

² The Global CBPR Forum established a related Privacy Recognition for Processors (PRP) certification that is not included for the purpose of this comparison.

Structure:

The comparative tables below provide a summary of the main elements outlined in the current documents on GDPR Certification and the Global CBPR System. It is structured as follows: for each key requirement identified, the table puts side by side a summarized description of requirements in the two systems. This document does not aim at achieving mutual recognition between the two systems, nor to permit organizations to obtain a double certification. The GDPR, EDPB Guidelines, Global CBPR Framework and Global CBPR System documents include additional relevant details and obligations.

Resources:

At the time this comparative analysis was conducted (S1 2024), no EU certification scheme for data transfers had yet been approved. The GDPR part of the analysis is based on existing Guidelines issued by the EDPB which provide a general list of the main elements for certification schemes to be tailored to specific transfer scenarios³ when they are used for international transfers. EU certification schemes will be designed by scheme owners on the basis of the GDPR and these Guidelines. Once EEA DPAs and the EDPB will have more practical experience on the GDPR certification as a tool for transfers, further guidance could be provided if needed. The Global CBPR System analysis is based on the Global CBPR System documents established by the Global CBPR Forum⁴, and which, to date, are not yet operational.

Executive Summary:

The general objective of rules on transfers is to ensure data protection standards continue to be met when data moves across borders. In this context, both the GDPR as well as the Global CBPR System provide for certification schemes as an instrument for cross-border transfers of personal data.

In conducting this analysis, we observe that both schemes subscribe to various similar key principles (such as lawfulness, purpose limitation, security of data processing and transparency). That said, there are notable differences in their legal foundations, structure and purpose as well as specific provisions (including enforceability and legal redress, rules regarding independent oversight and government access).

³ Guidelines 01/2018 on certification and identifying certification criteria in accordance with Art. 42 and 43 of the Regulation (EDPB Guidelines 01/2018) and Guidelines 07/2022 on certification as a tool for transfers (EDPB Guidelines 07/2022).

⁴ <https://www.globalcbpr.org/documents/>

The following paragraphs summarize the key differences between the two systems while also highlighting some notable similarities.

Legal foundation:

GDPR certification schemes will be developed on the basis of and in accordance with the GDPR, i.e. EU legislation that is legally binding and directly applicable in the EU and in the European Economic Area (EEA) and which provides for enforceable rights and effective legal remedies for data subjects. The GDPR establishes the conditions under which international personal data transfers can be carried out. Data transfers are subject to appropriate safeguards, which, among other mechanisms, can be provided for by an approved GDPR Certification.

The Global CBPR System is a voluntary, multilateral framework with principles, requirements and a governance structure agreed among the Members of the Global CBPR Forum and implemented and enforced based on the domestic law of the Members. The Global CBPR Forum, which oversees and administers the Global CBPR System, has nine Members: Australia, Canada, Mexico, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States. The Global CBPR Forum established the Global CBPR System in 2024 based on the APEC CBPR System, which was established in 2011 and currently has eight approved Accountability Agents and over 70 certified companies. At the time of its establishment, the Global CBPR System requirements are the same as the APEC CBPR System requirements.

Structure and purpose of the schemes:

Under the GDPR, data exporters whose processing activities are subject to the GDPR (GDPR exporter(s)) cannot transfer personal data to another controller or processor outside the EEA (data importer) without ensuring an equivalent level of protection of individuals. Such protection can be ensured by appropriate safeguards that can be provided for by different tools, including a GDPR approved certification mechanism. The data importer (non-EEA controllers or processors not subject to the GDPR) can therefore be certified with regard to its processing activities of personal data received from the GDPR exporter. The GDPR certification scheme must guarantee a level of protection “essentially equivalent” to the one offered by the GDPR. This includes the respect of core data protection principles, ensuring independent oversight, and that data subjects can effectively enforce their rights, as well as providing for obligations of the data importer and the GDPR exporter to monitor and to take action when national legislation or practice in the data importer’s country prevent compliance with commitments under the

certification. In addition to the certification, the data importer outside the EEA must take binding and enforceable commitments (e.g. via contract) to ensure that individuals having their personal data being processed, can enforce, as third-party beneficiaries, the commitments taken, including in front of EEA courts. GDPR Certifications are issued by an accredited certification body or by an EEA DPA, on the basis of certification criteria set up by either a DPA or by a third-party scheme owner, and approved by the EDPB⁵ or national EEA DPAs, on the basis of an Opinion issued by the EDPB. This ensures consistency of the criteria in the EEA.

The Global CBPR System, on the other hand, is not established exclusively as a transfer tool but is a certification to core data privacy and protection principles applicable across jurisdictions. The Global CBPR Program Requirements⁶ which underpin a certification are common to all Members; as such, they are the same for certified organizations operating in any participating jurisdiction and certifications can only be issued by independent third-parties approved by all Members (Accountability Agents). In order to become a Member of the Global CBPR Forum and therefore to participate in the Global CBPR System, a jurisdiction must demonstrate that the Global CBPR Program Requirements are enforceable under its domestic laws. In addition to complying with the Global CBPR System requirements, certified organizations must comply with any additional requirements in jurisdictions in which they operate, as applicable. Further, the certified organisation needs to provide an internal complaint resolution procedure, and the Global CBPR System requires Accountability Agents to provide dispute resolution services for certified organizations. The availability of legal⁷ remedies is subject to domestic laws. The Global CBPR System allows for various models of enforcement in the Members' jurisdictions (including through Privacy Enforcement Authorities (PEAs), multi-agency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as Members deem appropriate)⁸, so that Global CBPR certifications are binding and enforceable within the jurisdiction in which an organization is certified. The Global CBPR System also facilitates cross-border enforcement cooperation through requiring PEAs from all Members participating in the Global CBPR Forum to participate in the Global Cooperation Arrangement on Privacy Enforcement (Global CAPE).

Key differences:

While both the Global CBPR and GDPR certification require the certified entity to ensure certain data protection principles and obligations are upheld when

⁵ When criteria are approved by the EDPB, they may result in a common certification, the European Data Protection Seal (Art. 45(5) and 70(1)(o) GDPR).

⁶ https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Program-Requirements_Final.pdf

⁷ Global CBPR Framework, pt. 50 (a)

⁸ Global CBPR Framework, pt. 34.

transferring data, a number of key differences exist between the two frameworks.

Enforceability of data subjects' rights and legal redress

As noted above, one focus of GDPR Certification is ensuring enforceable rights and effective legal remedies for data subjects when personal data is transferred outside of the EEA. To this end, GDPR Certification enables data subjects to file complaints against the data importer with an EEA DPA and enforce their rights as third-party beneficiaries before the EEA court of their habitual residence, or where appropriate, of the GDPR exporter's establishment. The data importer has to take additional binding and enforceable commitments (e.g. via contract between the GDPR exporter and the data importer) to give effect to these provisions.

While the GDPR Certification enables data subjects to file complaints against the data importer before DPAs and enforce their rights before courts, under the Global CBPR System, the availability of remedies is based on Members' domestic laws⁹. However, all certified organizations are required to establish procedures to receive and respond to individual complaints,¹⁰ and all Accountability Agents are required to provide dispute resolution for consumer complaints and to enforce certification requirements against certified organizations.¹¹ Accountability Agents also must commit to and in certain situations are required to cooperate with government authorities, notify enforcement authorities when there is a violation of domestic law that is not remedied, and provide information for individuals to contact their enforcement authority.¹² All participating jurisdictions must have a backstop enforcement authority for Global CBPR Program Requirements, and the enforcement authorities must join the Global CAPE, an arrangement among regulators to cooperate on enforcement matters. The Global CBPR Framework and the Global CBPR System therefore provide guidance and minimum requirements for Members to implement so as to provide appropriate remedies for such violations, the content of which depends on the particular Member's legal system.

Independent oversight

EU transfer tools require provisions that guarantee oversight by independent public authorities. GDPR Certification therefore explicitly requires the data

⁹ Global CBPR Framework pt. 50 a.

¹⁰ See Program Requirements 41 - 44, https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Program-Requirements_Final.pdf.

¹¹ See Accountability Agent Recognition Criteria: https://www.globalcbpr.org/wp-content/uploads/Accountability-Agent-Application_Final.pdf

¹² Ibid.

importer in the third country to cooperate with the competent EEA DPA, to accept to be audited and inspected, to take into account advice and to comply with the DPA's decisions. This requirement is separated from the oversight role of the accredited certification body or the DPA, which can withdraw or suspend certification in case the requirements are no longer met. In addition, a DPA can also take an enforcement action against the certified importer¹³ and a certification body¹⁴.

The Global CBPR System requires jurisdictions to demonstrate the existence of a PEA and how the PEA can enforce the Global CBPR Program Requirements against certified organizations and Accountability Agents for certification-related activities under domestic law. The role of the PEA is independent from an Accountability Agent's oversight and enforcement role over certified organizations. PEAs are defined as "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"¹⁵.

Government Access and Supplementary measures

The two systems also follow different approaches regarding government access to personal data held by certified, private organizations.

GDPR Certification imposes distinct obligations on the certified data importer in cases of requests for access by third country authorities: the data importer has to promptly inform the GDPR exporter, review the request and, when necessary, challenge its legality, and to minimise any information disclosed.¹⁶ GDPR Certification also requires that, where access requests by third country public authorities vis-à-vis the data importer are considered to be disproportionate, in particular where they require massive and indiscriminate transfers of personal data, they should not take place.¹⁷ In addition to this, GDPR Certification requires the data exporter to continuously (re-)assess whether the certification it relies on as a transfer tool is effective in light of the relevant laws and practices in the data importer's jurisdiction. If the assessment reveals that these laws and practices interfere with the effectiveness of the certification, the parties are required to adopt additional technical and organizational measures (i.e. supplementary measures) to ensure that the EEA data protection level is maintained or, where it is not possible, to stop the transfer.

The Global CBPR System requires that certified organizations have procedures for responding to judicial or other government subpoenas,

¹³ EDPB Guidelines 07/2022, pt. 45.

¹⁴ Art. 58(2)(h), and Art. 83(4)(a) and (b), (5) and (6) GDPR

¹⁵ <https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf>

¹⁶ EDPB Guidelines 07/2022, pt. 45.

¹⁷ Ibid.

warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject,¹⁸ but it does not prescribe how an organization should respond or that the data exporter should be informed.

Storage limitation

While under GDPR Certification, data importers should comply with the storage limitation principle and not store personal data longer than is necessary for the purposes of the transfer, the Global CBPR System does not prescribe when data must be disposed.

Data breach notifications

Under GDPR Certification, data importers acting as data controllers should be subject to a duty to notify personal data breach notifications to DPAs and individuals. The Global CBPR System does not require such notifications but encourages its Members to implement respective provisions into domestic laws.

Automated decisions (incl. Profiling)

While under the GDPR Certification, automated decision making should only take place under certain conditions and if specific safeguards, such as the right for individuals to obtain human intervention, are in place. Such a requirement does not exist under the Global CBPR System.

Notable Similarities:

Security of processing

Both the Global CBPR System as well as GDPR Certification adopt a risk-based approach regarding security of processing, meaning certified organizations would be required to implement technical and organisation measures to ensure a level of security appropriate to the risks processing posed for the individuals. Under GDPR Certification, these measures would also need to be supplemented depending on the results of a thorough assessment of the data importer's domestic jurisdiction.

¹⁸ See Program Requirement 45, https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Program-Requirements_Final.pdf.

Transparency and right to information

Both systems require certified organizations acting as controller to provide individuals with certain information relating to their processing activities before or at the time of data collection. This obligation may be subject to exemptions which differ under the two systems. Certified organizations are also required to provide information about the obtained certification.

Internal complaint handling procedures and Internal supervision

Under both systems, certified organizations are required to establish internal procedures to receive and respond to complaints of data subjects. Certified organizations should document compliance with their obligations and be prepared to demonstrate their compliance.

The following documents informed this comparative analysis:

GDPR Certification:

- Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR),
- Guidelines 01/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (EDPB Guidelines 01/2018) and Annexes,
- Guidelines 07/2022 on certification as a tool for transfers and Annex (EDPB Guidelines 07/2022).

Global CBPR:

- Global Cross-Border Privacy Rules (CBPR) Framework (Global CBPR Framework),
- Global Cross-Border Privacy Rules System Program Requirements Map, (Global CBPR Requirements),

- Global Cross-Border Privacy Rules System Intake Questionnaire (Global CBPR Intake Questionnaire),
- Global Cross-Border Privacy Rules and Global Privacy Recognition for Processors (PRP) Systems Policies, Rules and Guidelines (Global CBPR Policies, Rules and Guidelines),
- Global CBPR Forum Accountability Agent Recognition Application.

TABLE OF CONTENT

<u>1.</u>	<u>Structure of the mechanisms</u>	12
<u>1.1.</u>	<u>Purpose</u>	12
<u>1.2.</u>	<u>Scope</u>	13
<u>1.3.</u>	<u>Involved Actors</u>	14
<u>1.4.</u>	<u>Additional binding and enforceable commitments to be implemented for controllers and processors not subject to the GDPR</u>	15
<u>2.</u>	<u>Data Protection Principles and Safeguards</u>	17
<u>2.1.</u>	<u>Lawfulness</u>	17
<u>2.2.</u>	<u>Purpose limitation</u>	18
<u>2.3.</u>	<u>Storage limitation</u>	19
<u>2.4.</u>	<u>Security of processing</u>	19
<u>2.5.</u>	<u>Data breach notifications</u>	20
<u>2.6.</u>	<u>Special categories of data</u>	21
<u>2.7.</u>	<u>Onward transfer to Controllers and Processors</u>	22
<u>2.8.</u>	<u>Relationship with domestic laws</u>	24
<u>2.9.</u>	<u>Assessment of laws and practices in the third country</u>	25
<u>2.10.</u>	<u>Data access by third country authorities</u>	27
<u>3.</u>	<u>Data Subject Rights</u>	29
<u>3.1.</u>	<u>Transparency and right to information</u>	29
<u>3.2.</u>	<u>Automated Decisions (incl. Profiling)</u>	31
<u>3.3.</u>	<u>Access, Rectification, Objection, and Erasure of Personal Data, and restriction of processing</u>	32
<u>3.4.</u>	<u>Legal Remedies and Redress for data subjects and third-party beneficiary rights</u>	34
<u>4.</u>	<u>Accountability and Compliance</u>	37
<u>4.1.</u>	<u>Internal Supervision</u>	37
<u>4.2.</u>	<u>Supervision of compliance</u>	37
<u>4.3.</u>	<u>Consequences of Non-Compliance with the Certification</u>	38

<u>4.4.</u>	<u>Enforcement and Cooperation with Authorities.....</u>	39
<u>4.5.</u>	<u>Approval procedures</u>	40

1. Structure of the mechanisms

1.1. Purpose

GDPR Certification	Global CBPR
<p>Apart from being an accountability tool established for the purpose of demonstrating compliance with the GDPR of processing operations following within the scope of application of the GDPR ¹⁹, GDPR certifications could also be a voluntary tool aimed at ensuring appropriate safeguards for the transfer of personal data in accordance with Article 46 (2) (f) GDPR. The certification must include the existence of appropriate safeguards provided by controllers or processors outside the EEA not subject to the GDPR or constituting an international organization receiving data as importers from GDPR controllers (or processors) in line with the ones envisaged by the GDPR in the EEA. Their implementation and effectiveness should be ensured also taking into account any legislation in the third country which may impinge on the obligations the importer takes under the certification (and where its implementation could not be ensured, the certification cannot be used as a tool for transfers).</p>	<p>The Global CBPR System is a voluntary multilateral certification framework which establishes common enforceable data privacy and protection requirements for certified organizations across jurisdictions and provides a tool for organizations to demonstrate compliance with those requirements through a certification process verified by independent third-parties (Accountability Agents) appointed within their home jurisdictions.</p>

¹⁹ See Article 42 and seq. GDPR.

1.2. Scope

GDPR Certification	Global CBPR
<p>The requirements of the GDPR apply to personal data, i.e. any information relating to an identified or identifiable natural person (Art. 4 (1) GDPR) regardless of whether it is publicly available or whether it is collected from the individual or not. Such data may then fully fall in the scope of GDPR certification.</p> <p>The object of the certification should be the processing of the data received by or made available to the data importer in the third country and any operation under the control of the importer. Under Art. 4(2) of the GDPR, processing is defined as any operation or set of operations which is performed on personal data, whether or not by automated means. The transit of data may also be covered by the scope, if under the control of the importer. The object of certification can be a single processing operation or a set of operations.</p> <p>GDPR Certification can apply when the GDPR exporter and the data importers act as a controller or processor²⁰.</p>	<p>The Global CBPR System applies to personal information, i.e. any information about an identified or identifiable individual.²¹</p> <p>Global CBPR has limited application to publicly available information, e.g. as regards notice and choice requirements.²²</p> <p>The Global CBPR System applies only to organizations, not governments or individuals, and is not restricted to a processing operation but can apply organization-wide.</p> <p>The Global CBPR System is only applicable to personal information controllers; the Global CBPR Forum established a separate recognition system for personal information processors, the Global Privacy Recognition for Processors (PRP) System, which is not included in this assessment.</p>

²⁰ However, this document only analysis the requirements for transfers between controllers.

²¹ Global CBPR Framework, pt. 6.

²² Global CBPR Framework, pt. 8.

1.3. Involved Actors

GDPR Certification	Global CBPR
<p>EDPB: approves EEA-wide certification criteria (European Data Protection Seal) and accreditation requirements for certification bodies and provides opinions on DPAs’ draft decisions on certification criteria and accreditation requirements for certification bodies.</p> <p>Independent DPAs: approve the certification criteria of national certification mechanisms. Depending on the domestic system, DPAs may also accredit the certification body, design the certification criteria and issue certifications.</p> <p>National Accreditation Body: may accredit certification bodies by using ISO/IEC 17065 and the DPAs additional accreditation requirements.</p> <p>Scheme owner: organization which has set up certification criteria and the requirements against which conformity is to be assessed by the Certification body.</p>	<p>The Global Forum Assembly (GFA): is the policy-making body of the Forum which consists of all Members²⁴ (representatives from participating jurisdictions).</p> <p>Global CBPR Forum-approved Accountability Agent: an independent third-party certification body that certifies organizations to the Global CBPR System. Members of the Global CBPR Forum through consensus determine common criteria that must be met by all Accountability Agents, and Accountability Agents must be recognized by all Members and are subject to ongoing oversight by Members²⁵. To be approved as an Accountability Agent, an Applicant must submit necessary documents to the relevant government entities in any Member in which the Applicant Accountability Agent intends to operate. The government entities will review to ensure the necessary documentation have been included in the application and forward information to the Chair of the GFA and the Chair of the Accountability Agent Oversight and Engagement (AA) Committee. The AA Committee will review and make</p>

²⁴ Current Members are: Australia, Canada, Japan, Republic of Korea, Mexico, Philippines, Singapore, Chinese Taipei, the United States, and the United Kingdom is an Associate (non-voting).

²⁵ Accountability Agent Recognition Application

<p>Certification body: issues the certification²³. May design certification criteria and/or a detailed assessment methodology for the criteria.</p> <p>Data importer: certified entity who can act as data controller or processor.</p> <p>Data exporter: entity, acting as data controller or processor and relying on certification of the importer to ensure compliance of its transfers with the GDPR.</p>	<p>recommendations to the GFA on applications for recognition as an Accountability Agent, and Members must endorse an Accountability Agent by consensus.²⁶</p> <p>PEAs: 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.</p> <p>Personal information controller: a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information.</p>
---	---

1.4. Additional binding and enforceable commitments to be implemented for controllers and processors not subject to the GDPR

GDPR Certification	Global CBPR
<p>The GDPR requires in its Article 42 (2) that controllers and processors not subject to the GDPR adhering to a certification mechanism intended for transfers take, additionally, binding and enforceable commitments, via contractual or other legally binding instruments, to apply the appropriate safeguards provided by the certification</p>	<p>No equivalent.</p>

²³ As provided above, certification can be issued by certification bodies or by the competent data protection authority

²⁶ Accountability Agent APEC Recognition Application, p. 2.

mechanism including with regard to the rights of data subjects.

The commitments should be therefore enforceable by organization exporting the data but also by individuals having their personal data being processed, as third-party beneficiaries, against the importer and the exporter of data, including a right to bring claims, including for compensation, in front of EEA courts. The data importer has to accept the jurisdiction of EEA courts. The data importer and the GDPR exporter should also accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under Art. 80(1) GDPR.

As specified in the GDPR, such commitments may be taken by using a contract, which appears as the most straight forward solution. Other instruments could also be used, provided that the controller/processors adhering to the certification mechanism are able to demonstrate the binding and enforceable nature of such other means.

2. Data Protection Principles and Safeguards

Both Global CBPR and GDPR certification require the certified entity to ensure certain fundamental data protection principles and obligations are upheld when transferring data.

2.1. Lawfulness

GDPR Certification	Global CBPR
<p><i>Lawfulness of the processing is linked to the legal ground for transfers in place for the GDPR exporters and, when the data importer is a controller, the possible further processing activities.</i></p> <p>Where processing is based on consent, it should be unambiguous, specific, freely given and informed.²⁷</p> <p>Other than consent, legal grounds for processing are based, as applicable, on those laid down under the GDPR²⁸, i.e. where processing is</p> <ul style="list-style-type: none"> - necessary for 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, 	<p>The choice mechanism provided shall be clear, prominent, easily understandable, accessible and affordable.²⁹</p> <p>In certain situations, it may not be necessary or practicable to provide a mechanism to exercise choice, e.g. (inter alia) when consent of the individual is obviously implied, the information is publicly available or a choice mechanism would be technologically impractical at the time of collection.³⁰</p>
<ul style="list-style-type: none"> - necessary for 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, 	<p>Other than with consent, personal data may be processed</p> <ul style="list-style-type: none"> - for compatible or related purposes as identified in the certified organization's privacy statement and/or in the notice provided at the time of collection, - when compelled by applicable laws,

²⁷ Art. 4(11) GDPR

²⁸ EDPB Guidelines 01/2018, pt. 48, Annex 2, pt. 5, 6 (Art. 6 GDPR).

²⁹ Global CBPR Framework, pt. 23.

³⁰ Global CBPR Framework, pt. 23; Global CBPR Intake Questionnaire, pt. 20.

<ul style="list-style-type: none"> - necessary for compliance with a legal obligation to which the controller is subject, - necessary in order to protect the vital interests of the data subject or of another natural person, - necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, - necessary for the purposes of the legitimate interests pursued by the controller or a third party (when not overridden by the interests or fundamental rights of the data subject). 	<ul style="list-style-type: none"> - if necessary to provide a service or product requested by the individual.³¹
---	--

2.2. Purpose limitation

GDPR Certification	Global CBPR
<p>Under GDPR certification, the involved parties should adhere to the principle of purpose limitation³² and define the purpose of the transfer and processing operation(s) concretely.³³</p> <p>Personal data may only be processed for the purposes of the transfer and cannot be used in a way incompatible with these purposes.</p>	<p>Personal information should be used only to fulfil the purposes of its collection and other compatible or related purposes except:</p> <ul style="list-style-type: none"> - with the consent of the individual, - when necessary to provide a service or product requested by the individual or - by the authority of law and other legal instruments.³⁴

³¹ Global CBPR Requirements, pts. 9 – 13.

³² EDPB Guidelines 01/2018, pt. 48, Annex 2, pt. 6 (Art. 5 GDPR).

³³ EDPB Guidelines 07/2022, pt. 42.

³⁴ Global CBPR Framework, pt. 22.

2.3. Storage limitation

GDPR Certification	Global CBPR
The data importer should adhere to the principle of storage limitation, i.e. not store personal data for longer than is necessary for the purposes of the transfer. ³⁵	No equivalent.

2.4. Security of processing

GDPR Certification	Global CBPR
Certification criteria should require application of technical and organizational measures providing for confidentiality, integrity and availability of processing operations ³⁶ which take into account (inter alia) the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons. ³⁷	The certified organization must implement reasonable administrative, technical and physical safeguards, suitable to its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information. ³⁸

³⁵ EDPB Guidelines 01/2018, pt. 48, Annex 2, pt. 5, 6 (Art. 5 (1) e GDPR).

³⁶ EDPB Guidelines 01/2018, Annex 2 pt. 10.

³⁷ EDPB Guidelines 01/2018, pt. 48 (Art. 25, 32 GDPR).

³⁸ Global CBPR Requirements, p. 27.

<p>The implemented safeguards should take into account the state of the art³⁹ and require monitoring of evolving privacy and technology issues to update the scheme if needed.⁴⁰</p> <p>If the transit of data is included in the scope of the certification, the data importer is also required to implement appropriate safeguards to ensure the security of the personal data while transferred.⁴¹</p>	<p>The implemented safeguards should be subject to periodic review and reassessment and the certified organization shall adjust the security safeguards to reflect the results of such assessment.⁴²</p> <p>Certified organizations have to implement safeguards proportional to the probability and severity of the potential harm, the confidential nature or sensitivity of the information, and the context in which it is held. The certified organizations must employ suitable and reasonable means, such as encryption, to protect all personal information.</p>
--	---

2.5. Data breach notifications

GDPR Certification	Global CBPR
<p>Under GDPR certification, personal data breach notification duties should be carried out in due time and scope⁴³; i.e. the data importer should notify the GDPR exporter and, if acting as controller, notify the competent DPA (the authority in the EEA competent for the GDPR exporter⁴⁴) and communicate the breach to the data subjects where</p>	<p>The certified organization has to ensure that processors, agents, contractors, or other service providers to whom it transfers personal information notify the certified organization when they become aware of on occurrence of breach of the privacy or security of personal data of the certified organization’s customers.⁴⁶</p>

³⁹ Ibid.

⁴⁰ EDPB Guidelines 01/2018, Annex 2, pts. 7 d, 10 s.

⁴¹ EDPB Guidelines 07/2022, pt. 45.

⁴² Global CBPR Framework, pt. 25; Global CBPR Requirements, pt. 34.

⁴³ EDPB Guidelines 01/2018, Annex 2, pt. 10 q.

⁴⁴ EDPB Guidelines 07/2022, pt. 44.

⁴⁶ Global CBPR Requirements, pt. 35 b.

<p>it is likely to result in a high risk to their rights and freedoms.⁴⁵</p>	<p>There is no requirement to notify DPAs or individuals.</p> <p>However, within their domestic laws, Global CBPR Forum Members should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to PEAs and/or other authorities in the event of a significant security breach. 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 reasonable⁴⁷ as this may help to mitigate harmful consequences.⁴⁸ This would nevertheless not be part of the elements checked to deliver Global CBPR certification.</p>
---	---

2.6. Special categories of data

GDPR Certification	Global CBPR
<p>Processing of special categories of data (e.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, genetic or biometric data, data concerning health or concerning a person’s sex life or sexual</p>	<p>No equivalent.</p>

⁴⁵ In line with the requirements of Art. 34 GDPR.

⁴⁷ Global CBPR Framework, pt. 51.

⁴⁸ Global CBPR Framework, pt. 17.

<p>orientation) is prohibited if none of the exceptions in line with Art. 9 GDPR apply⁴⁹.</p>	
<p>Certification criteria must allow identifying special categories of data⁵⁰ and take into account the sensitivity of information and risk of processing when determining which technical and organizational measures (in particular to ensure appropriate security) to put in place.⁵¹</p>	<p>When assessing the permitted use of personal information and its specific purpose, the nature of the information has to be taken into account⁵², as some personal information (such as credit card numbers or bank account information) might be considered sensitive.⁵³</p> <p>The certified organization must implement reasonable safeguards that are suitable to the sensitivity of the personal information and proportional to the probability and severity of the harm threatened.⁵⁴</p>

2.7. Onward transfer to Controllers and Processors

GDPR Certification	Global CBPR
<p>Certification requires that the data importer uses an instrument for onward transfers that provides for specific safeguards in line with Chapter V GDPR to ensure that the level of protection guaranteed by the certification will not be undermined⁵⁵, i.e. onward transfers are subject to the same</p>	<p>Under the general accountability requirements, when transferring information, the certified organization should be accountable to ensure that the recipient will protect the information consistently with Global CBPR requirements when not obtaining consent and take</p>

⁴⁹ This considering that the GDPR does not directly apply to data importers.

⁵⁰ Ibid.

⁵¹ EDPB Guidelines 01/2018, Annex 2, pt. 14 b.

⁵² Global CBPR Requirements, p. 8, pt. 30.

⁵³ Global CBPR Framework, pt. 21.

⁵⁴ Global CBPR Requirements, pt. 27.

⁵⁵ EDPB Guidelines 07/2022, pt. 45 (3).

<p>level of requirements as the transfer between the initial GDPR exporter and data importer.</p> <p>This obligation applies to any onward transfer, i.e. to both controllers and processors in the country of the data importer or in other countries.</p> <p>Other than this, GDPR certification also allows for onward transfers in some limited exceptions, such as on the basis of the data's subject qualified consent or in case of important reasons of public interest.</p>	<p>reasonable steps to ensure the information is protected accordingly after it is transferred⁵⁶.</p> <p>The certified organization shall ensure that processors, agents, contractors or other service providers to whom it transfers personal information implement an information security program to protect against loss, unauthorized access, destruction, use, modification or disclosure or other misuses of the information.⁵⁷</p> <p>The certified organization has to implement mechanisms that require service providers to abide by Global CBPR-compliant or substantially similar privacy policies and practices and monitor compliance.⁵⁸ This includes the certified organization's obligations to the individual whose information it uses.⁵⁹</p> <p>In certain situations due diligence as described above may be impractical or impossible (e.g. when there is no on-going relationship between the certified organization and the third party to whom the information is disclosed).⁶⁰ In these circumstances, the certified organization must use other means to ensure that the</p>
--	---

⁵⁶ Global CBPR Requirements, p. 30.

⁵⁷ Global CBPR Requirements, pt. 35; Global CBPR Intake Questionnaire, pt. 35.

⁵⁸ Global CBPR Intake Questionnaire, pts. 46 – 49.

⁵⁹ Global CBPR Requirements, pt. 46.

⁶⁰ Global CBPR Framework, pt. 29.

	<p>information is protected consistent with Global CBPR requirements⁶¹ (e.g. obtain consent⁶²).</p> <p>In cases where disclosures are required by domestic law, the certified organization is relieved of any due diligence or consent obligations.⁶³</p>
<p>The data importer has to keep available the appropriate documentation to show that onward transfers adhere to above requirements on request of the certification body and the competent DPA.⁶⁴</p>	<p>No equivalent.</p> <p>In general, personal information controllers should be prepared to demonstrate their data protection and privacy management programmes at the request of a competent PEA 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 Framework⁶⁵.</p>

2.8. Relationship with domestic laws

GDPR Certification	Global CBPR
<p>The GDPR exporter must ensure that domestic laws and practices will not prevent the data importer from fulfilling its obligations under the certification (s. 2.9., 2.10).</p>	<p>No equivalent.</p>

⁶¹ Global CBPR Requirements, pt. 50.

⁶² Global CBPR Framework, pt. 29.

⁶³ Ibid.

⁶⁴ EDPB Guidelines 07/2022, pt. 45 (3).

⁶⁵ Global CBPR Framework, pt. 42

<p>The certification does not affect the data importer’s domestic legal obligations (subject to the requirements described under 2.9. - 2.10).</p>	<p>Participation in the Global CBPR System does not replace the certified organization’s domestic legal obligations. While the commitments carried out in order to participate in the Global CBPR System must be enforceable under a Member’s domestic law, additional domestic legal requirements may apply. Where these requirements exceed what is expected under the Global CBPR System, their full extent will continue to apply. Where the requirements of the Global CBPR System exceed domestic requirements, the certified organization will need to carry out such additional requirements in order to participate in the Global CBPR System.</p>
--	---

2.9. Assessment of laws and practices in the third country

GDPR Certification	Global CBPR
<p>The GDPR exporter has to assess whether the certification it intends to rely on as a transfer tool is effective in the light of the relevant laws and practices in force in the third country.⁶⁶ The assessment of the data importer’s processing should also include onward transfers and must ensure that the rules and practices of the third country (countries) will not prevent</p>	<p>No equivalent.</p>

⁶⁶ Ibid.

<p>the data importer from complying with its obligations and commitments under the certification.⁶⁷</p>	
<p>In practice, the data importer will assess the relevant rules and practices in the third country (countries) and document this assessment.⁶⁸ The competent certification body will then verify if the data importer has carried out the assessment duly and in a correct way and the data exporter can rely on it.⁶⁹</p>	<p>No equivalent.</p>
<p>The data importer has to warrant to the certification body and the data exporter that it has no reason to believe that the applicable legislation and practices (including requirements to disclose personal data or measures authorising access by public authorities)⁷⁰ may prevent it from fulfilling its obligations under the certification.⁷¹</p> <p>Where the data importer has reason to believe that changes in the relevant legislation and practices may prevent compliance with its obligations, it must promptly notify this to the certification body and to the data exporter, so that the latter can</p>	<p>No equivalent.</p>

⁶⁷ EDPB Guidelines 07/2022, pt. 25.

⁶⁸ EDPB Guidelines, pt. 45 (1).

⁶⁹ EDPB Guidelines, pts. 21, 34.

⁷⁰ EDPB Guidelines 07/2022, pt. 53.

⁷¹ EDPB Guidelines 07/2022, pt. 45 (1).

evaluate whether to immediately stop transfers. ⁷²	
---	--

2.10. Data access by third country authorities

GDPR Certification	Global CBPR
<p>In case of requests for access by third country authorities,⁷³ the data importer must promptly inform the GDPR exporter and take appropriate additional measures.⁷⁴</p> <p>These measures include the obligation to review and, when necessary, challenge the legality of the request⁷⁵ and to minimise any information disclosed.⁷⁶</p>	<p>No equivalent.</p> <p>The certified organization should have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information.⁷⁷</p>
<p>Certification criteria should require that transfers as a result of disproportionate access requests by third country authorities (in particular massive and indiscriminate transfers of personal data) should not take place⁷⁸, i.e. transfers to a public authority cannot go beyond what is necessary in a democratic society.</p>	<p>No equivalent.</p>

⁷² EDPB Guidelines 07/2022, pt. 45 (5); in this evaluation, the data exporter should identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. If it considers that no appropriate safeguards can be ensured, it shall suspend the transfer.

⁷³ Or if the data importer becomes aware of any direct access by public authorities.

⁷⁴ EDPB Guidelines 07/2022, pt. 45 (6).

⁷⁵ The data importer should review in particular if the request remains within the powers granted to the requesting authority.

⁷⁶ EDPB Guidelines 07/2022, pt. 45 (5).

⁷⁷ Global CBPR Requirements, pt. 45.

⁷⁸ EDPB Guidelines 07/2022, pt. 45 (6).

<p>Where needed after assessment of the rules and practices of the data importer’s domestic jurisdiction, the data importer is required to implement additional organizational and technological measures to provide the appropriate safeguards under Art. 46 GDPR⁷⁹ to ensure that the EEA level of protection of personal data would not be undermined in case of third country laws impinging on the commitments taken by the importer (supplementary measures).⁸⁰</p> <p>The data importer has to ensure that (where so envisaged) the supplementary measures it has identified are matched by corresponding supplementary measures on the GDPR exporter’s side.⁸¹</p>	<p>No equivalent</p>

⁷⁹ Taking into account the EDPB Recommendations 01/2020 on measures that supplement transfer tools.

⁸⁰ EDPB Guidelines 07/2022, pt. 45.

⁸¹ EDPB Guidelines 07/2022, pt. 46.

3. Data Subject Rights

Both Global CBPR and GDPR Certification grant certain rights to the individuals whose personal information is processed. While the GDPR Certification provides for judicial remedies and redress for individuals, under the Global CBPR System, the availability of legal remedies and redress for the individual largely depends on what is provided by domestic laws.

3.1. Transparency and right to information

GDPR Certification	Global CBPR
<p>Certification bodies should provide easily accessible, intelligible and meaningful information about the certified processing operation(s). This public information should include at least the</p> <ul style="list-style-type: none"> - description of the Target of Evaluation⁸² (ToE), - reference to the approved criteria applied to the specific ToE, - the methodology for the evaluation of the criteria, - the duration of the validity of the certificate.⁸³ 	<p>Transparency is a key element of the Global CBPR System and important information is made publicly available. For example, the Global CBPR Program Requirements that apply to all certified organizations, information on approved Accountability Agents including their completed Accountability Agent Recognition Applications, and a directory of participating companies are to be readily available online. Additionally, certified organizations are required to make information for how to submit complaints against them available to consumers along with other notice requirements. The directory is expected to list at a minimum:</p> <ul style="list-style-type: none"> - the name of the certified organization, - a website for the certified organization and a link to the organization’s privacy policy,

⁸² The object of the certification, EDPB Guidelines 01/2018, pt. 58; EDPB Guidelines 07/2022, pt. 16.

⁸³ EDPB Guidelines 01/2018, pt. 66.

	<ul style="list-style-type: none"> - contact information, - the Accountability Agent that certified the Participant, - the relevant PEA, - the scope of the certification, - the organization’s original certification date, - the date that the current certification expires.⁸⁴
<p>Certification criteria should require that certified bodies, when acting as data controller, must provide information on the processing activities to data subjects (essentially equivalent to the rights provided under Art. 12-14 GDPR⁸⁵) and require respective measures to be put in place.⁸⁶</p> <p>Information to be provided to the data subject may include (inter alia and as applicable)⁸⁷:</p> <ul style="list-style-type: none"> - identity and contact details of the controller, - purposes and legal basis for processing, - recipients of the personal data, - reference to the data subject’s rights, - if transfer to a third country is intended, reference to the respective adequacy decision or (where absent) the appropriate safeguards and a copy of them. 	<p>Certified organizations must ensure that individuals know their personal information is collected, to whom it may be transferred and for what purpose it may be used.⁸⁸</p> <p>Information to be provided to the individual includes (inter alia and as applicable)⁸⁹:</p> <ul style="list-style-type: none"> - purpose(s) for which the data is collected, - identity and contact details of the certified organization, - whether and how the individual can access and correct their personal information, - whether personal information is made available to third parties and for what purpose.

⁸⁴ APEC CBPR Compliance Directory

⁸⁵ EDPB Guidelines 01/2018, pt. 48; EDPB Guidelines 07/2022, pt. 43 b.

⁸⁶ EDPB Guidelines 01/2018, Annex 2, pt. 8.

⁸⁷ This information is provided on the basis of Art. 13, 14 GDPR; further information is required where necessary, having regard to the specific circumstances of data collection.

⁸⁸ Global CBPR Intake Questionnaire, p. 4.

⁸⁹ Global CBPR Requirements, pt. 1-4, Global CBPR Intake Questionnaire, pt. 1-4.

<p>The obligation to provide information does not apply where individuals already have the information, including when it has already been provided by the GDPR exporter or if provision proves impossible, or would involve a disproportionate effort.⁹⁰</p>	<p>In some circumstances, notice may not be necessary or practical:</p> <ul style="list-style-type: none"> - obviousness (of the individual’s consent), - collection of publicly available information, - technological impracticability, - lawful requests from government institutions, - disclosure to a third party pursuant to a lawful form of process, - when the controller receives personal information from a third party (third-party receipt), - legitimate investigation purposes, - emergencies.⁹¹
--	--

3.2. Automated Decisions (incl. Profiling)

GDPR Certification	Global CBPR
<p>The data importer, acting as data controller⁹² should not make a decision based solely on automated processing of the personal data (automated decision), including profiling which would produce legal effects concerning the data subject or significantly affects him/her, unless</p> <ul style="list-style-type: none"> - with explicit consent, 	<p>No equivalent.</p>

⁹⁰ In line with the requirements of Art. 13 (4), 14 (5) GDPR.

⁹¹ Global CBPR Intake Questionnaire, Qualifications to the Provision of Notice, p. 6.

⁹² When the data importer acts as processor, it can only process data in accordance with the instructions of the data exporter. Only the organization acting as controller can be in a situation to apply the exceptions to be able to carry out automated decisions.

<ul style="list-style-type: none"> - where it is necessary for entering into, or performance of, a contract with the data subject or - if authorised to do so under law (provided that the law lays down suitable measures to safeguard the data subject’s rights and interests, including the right to obtain human intervention, to express his or her point of view and to contest the decision)⁹³. <p>In any case, suitable safeguards for the data subject’s rights, freedoms and legitimate interests should be in place, i.e. at least the right to obtain human intervention, to express his or her point of view and to contest the decision.⁹⁴</p>	
--	--

3.3. Access, Rectification, Objection, and Erasure of Personal Data, and restriction of processing

GDPR Certification	Global CBPR
<p>Certification criteria should require that the data subjects are guaranteed their rights to access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction and objection to processing⁹⁵.</p>	<p>Upon request, the certified organization shall provide confirmation of whether or not it holds personal information about the requesting individual and provide access to the information. The certified organization shall also permit individuals to challenge the accuracy of their information, and</p>

⁹³ EDPB Guidelines 07/2022, pt. 43 b.

⁹⁴ Ibid.

⁹⁵ EDPB Guidelines 07/2022, pt. 41 b.

<p>The above rights should be “essentially equivalent” to those provided for by Art. 15 to 19 GDPR.⁹⁶</p>	<p>to have it rectified, completed, amended and/or deleted.⁹⁷</p> <p>The ability to access and correct personal information is generally regarded as a central aspect of privacy protection but is not an absolute right.⁹⁸</p>
<p>Those rights should be provided free of charge. Where a data subject’s requests are excessive (in particular because of their repetitive character) the data importer may either charge a reasonable fee taking into account the administrative cost or refuse to act on the request.⁹⁹</p> <p>The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed under Art. 23 GDPR.¹⁰⁰</p>	<p>A fee can be charged for providing access to information, providing it is not excessive¹⁰¹.</p> <p>In certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records and claims for access and correction shall therefore be denied.¹⁰²</p> <p>Denials are considered acceptable under following conditions¹⁰³:</p> <ul style="list-style-type: none"> - the burden or expense of providing access and correction would be unreasonable or disproportionate to the risks to the individual’s privacy (disproportionate burden), - to protect confidential information (due to legal or security reasons or to protect confidential commercial information),

⁹⁶ Ibid.

⁹⁷ Global CBPR Requirements, pts. 36-38; Global CBPR Intake Questionnaire, pts. 36-38.

⁹⁸ Global CBPR Framework pt. 26; Global CBPR Requirements, p. 21; Global CBPR Intake Questionnaire, p. 17.

⁹⁹ EDPB Guidelines 01/2018, pt. 48; EDPB Guidelines 07/2022, pt 43(a and b); (Art. 12(5) GDPR)

¹⁰⁰ EDPB Guidelines 01/2018, pt. 48; EDPB Guidelines 07/2022, pt 43(b); (Art. 23 GDPR).

¹⁰¹ Global CBPR Requirements, pt 37(e)

¹⁰² Global CBPR Requirements, p. 21.

¹⁰³ Global CBPR Intake Questionnaire, p. 19.

	<p>- when access or correction would violate the information privacy of person other than the individual (third party risk).</p> <p>Where confidential or third party's personal information can be severed from the information requested for access or correction, the controller must release the information after redaction.</p>
<p>If the data importer intends to refuse a data subject's request, it should inform the data subject of the reasons and the possibility of lodging a complaint with the competent DPA and seeking judicial redress (refer to 3.5).¹⁰⁴</p>	<p>If access or correction is refused, the certified organization shall provide the individual with an explanation and contact information for further inquiries.¹⁰⁵</p> <p>This includes information on how to request further inquiries about the denial (refer to 3.5).¹⁰⁶</p>

3.4. Legal Remedies and Redress for data subjects and third-party beneficiary rights

GDPR Certification	Global CBPR
<p>The data importer should establish an appropriate complaint handling procedure to ensure effective implementation of data subject rights.¹⁰⁷</p>	<p>The certified organization shall have procedures in place to receive, investigate and respond to privacy-related complaints. The response shall include an explanation of remedial action</p>

¹⁰⁴ EDPB Guidelines 01/2018, pt. 48 (Art. 12(4) GDPR).

¹⁰⁵ Global CBPR Requirements, pt. 38 e; Global CBPR Intake Questionnaire pt. 38 e.

¹⁰⁶ Global CBPR Framework, pt. 28; Global CBPR Requirements, p. 21.

¹⁰⁷ EDPB Guidelines 07/2022, pt. 43 c.

	<p>relating to the individual's complaint.¹⁰⁸</p> <p>An Accountability Agent must have a mechanism to receive and investigate complaints about certified organizations and to resolve disputes between complainants and certified organizations in relation to non-compliance with the Program Requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents when appropriate and where possible.¹⁰⁹</p>
<p>Data subjects should be able to lodge a complaint against the importer with a DPA in the EEA, in particular in the EEA State of their habitual residence, place of work or competent for the GDPR exporter(s).¹¹⁰</p> <p>The data importer should be required to cooperate with the EEA DPA competent for the GDPR exporter(s), accept to be audited and inspected, take into account its (their) advice and abide by its (their) decision.¹¹¹</p>	<p>The possibility to involve a PEA would be subject to domestic laws: Members of the Global CBPR Forum must have a PEA.¹¹² These should be able to review a Global CBPR related complaint/issue if the participating organization or the respective Accountability Agent cannot resolve it and when appropriate, investigate and take enforcement action.¹¹³</p>
<p>Data subjects should be able to enforce their rights as third-party beneficiaries against the data importer before the EEA court of</p>	<p>The possibility of redress is not mandatory and would be subject to domestic laws: Global CBPR Forum's Members' domestic laws</p>

¹⁰⁸ Global CBPR Requirements, pts. 41, 43.

¹⁰⁹ Accountability Agent Recognition Criterion 9.

¹¹⁰ EDPB Guidelines 07/2022, pt. 45.

¹¹¹ Ibid.

¹¹² Global CBPR Framework, pt. 38.

¹¹³ Global CBPR Policies, Rules and Guidelines, pt. 42.

<p>their habitual residence, or with an international organization, including for compensation for damage¹¹⁴ suffered in case of non-compliance with the certification scheme.¹¹⁵</p>	<p>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 (this may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems).¹¹⁶</p> <p>The range of remedies therefore depends on the particular Member’s domestic data protection and privacy system.</p>
<p>The data importer should take additional binding and enforceable commitments (via contractual or other legally binding instruments) to ensure that above rights and obligations are upheld (refer to 1.4).¹¹⁷</p>	<p>No equivalent.</p>

¹¹⁴ This includes material as well as non-material damages, Art. 82 GDPR.

¹¹⁵ EDPB Guidelines 07/2022, pt. 45.

¹¹⁶ Global CBPR Framework, pt. 50.

¹¹⁷ EDPB Guidelines 07/2022, pts. 47, 55.

4. Accountability and Compliance

4.1. Internal Supervision

GDPR Certification	Global CBPR
Where applicable, the data importer should appoint a Data Protection Officer (DPO) at the same conditions as the ones envisaged in Art. 37-39 GDPR ¹¹⁸ .	The organization shall appoint an individual(s) to be responsible for overall compliance with the Global CBPR Principles. ¹¹⁹
Organizations should document compliance with their obligations. ¹²⁰	A certified organization must be prepared to demonstrate the measures it takes to ensure compliance with the Global CBPR Privacy Principles at the request of a competent PEA or in response to a valid request by another appropriate entity (e.g. an Accountability Agent), which can be done through written policies, contracts or other ways. ¹²¹

4.2. Supervision of compliance

GDPR Certification	Global CBPR
Compliance is ensured by independent DPAs and the certification body (depending on national law). The certification body monitors adherence,	Accountability Agents recognized by the Global CBPR Forum Members monitor compliance of certified organizations, provide dispute resolution, annually re-

¹¹⁸ EDPB Guidelines 01/20108, Annex 2, pt. 7 to be tailored to transfer scenarios.

¹¹⁹ Global CBPR Requirements, pt. 40.

¹²⁰ EDPB Guidelines 01/2018, Annex 2, pt. 7; This relates for instance to document the assessment of the rules and practices of the third country where the data importer operates (EDPB Guidelines 07/2022, pt. 45.1.b.), document the organizational and supplementary measures implemented (EDPB Guidelines 07/2022, pt. 45.1.d), document existing onward transfers and rules relating to it (EDPB Guidelines 07/2022, pt. 20 and 45.3.a).

¹²¹ Global CBPR Program Requirement 39.

<p>reviews, handles complaints related to contractual issues with certified entities and withdraws certification.¹²²</p> <p>As explained in 3.4, DPAs can handle complaints from individuals¹²³ and their tasks and powers (including to impose corrective measures, such as fines) are not reduced due to the certification¹²⁴.</p> <p>The certification body is required to provide DPAs with information, especially on individual certifications, which is necessary to monitor the application of the certification mechanism.¹²⁵</p>	<p>certify organizations and submit information on certified organizations for the public compliance directory. Accountability Agents are required to submit applications for continued recognition after the first year and every two years thereafter, submit annual reports on complaints statistics, refer matters to an enforcement authority as appropriate, and respond to requests from Member authorities where possible.</p> <p>PEA(s) of Members 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 requirements¹²⁶.</p>
--	--

4.3. Consequences of Non-Compliance with the Certification

GDPR Certification	Global CBPR
<p>Withdrawal or suspension of certification by the certification body or by the DPA¹²⁷.</p> <p>Where the certification body is not a DPA, the DPA has the power and task to order the certification body</p>	<p>An Accountability Agent has a process in place for notifying certified organizations immediately of non-compliance with the Program Requirements and for requiring certified organizations to remedy the non-compliance within a specified time period.</p>

¹²² EDPB Guidelines 01/2018, pt. 27.

¹²³ EDPB Guidelines 07/2022, pt. 45.4.c.

¹²⁴ Article 42 (4) GDPR.

¹²⁵ Article 42 (7), 43 (5), 58 (2) h GDPR.

¹²⁶ Global CBPR Policies, Rules and Guidelines, pt. 44.

¹²⁷ Article 42(7) GDPR.

<p>not to issue or to withdraw the certification where the requirements are not or no longer met¹²⁸.</p> <p>In these cases, the GDPR exporter can no longer rely on the certification to lawfully transfer personal data to the data importer.</p> <p>The data importer should accept to cooperate and be subject to inspection and abide to decision with DPAs¹²⁹ (3.4) which can take enforcement actions against the data importer (4.2)¹³⁰.</p>	<p>An Accountability Agent has processes in place to impose penalties 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.</p>
--	---

4.4. Enforcement and Cooperation with Authorities

GDPR Certification	Global CBPR
<p>The data importer should be required to cooperate with the EEA DPA competent for the GDPR exporter(s), accept to be audited and inspected, take into account its (their) advice and abide by its (their) decision.¹³¹</p>	<p>No equivalent.</p>
<p>Where the certification body is not a DPA, the DPA has the power and task to order the certification body not to issue or to withdraw the certification where the</p>	<p>Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a</p>

¹²⁸ Article 58 (2) h GDPR

¹²⁹ EDPB Guidelines 07/2022, pt. 45.4.d.

¹³⁰ Article 42 (4) GDPR.

¹³¹ EDPB Guidelines 07/2022, pt. 45.

<p>requirements are not or no longer met¹³².</p> <p>A DPA can also take an enforcement action against the certified importer (4.3) and a certification body¹³³.</p>	<p>reasonable belief pursuant to its established review process that a Participant's failure to comply with the requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent so long as such failure to comply can be reasonably believed to be a violation of applicable law¹³⁴.</p> <p>PEAs must be able to enforce Global CBPR requirements against Accountability Agents for certification-related activities under domestic law.</p> <p>Where possible, Accountability Agent will respond to requests from enforcement entities of a Member that reasonably relate to that Member and to the Global CBPR-related activities of the Accountability Agent.¹³⁵</p>
<p>Under the GDPR, national DPA cooperate within the context of the EDPB which gathers all 27 authorities of the European Union as well as the European Data Protection Supervisors and the authorities from the EEA.</p>	<p>Members need to have at least one PEA participate in the Global CAPE, a practical multilateral mechanism creating a framework under which authorities may, on a voluntary basis, share information and request and render assistance in certain ways.</p>

4.5. Approval procedures

¹³² Article 58 (2) h GDPR.

¹³³ Article 83(4)(a) and (b) GDPR.

¹³⁴ Accountability Agent APEC Recognition Application, Annex A, pts. 14 – 15

¹³⁵ Ibid.

GDPR Certification	Global CBPR
<p>Certification procedure is voluntary. The certification is based on the evaluation of binding certification criteria according to a binding audit methodology. Those criteria will be approved by national DPAs after the EDPB issues an Opinion in accordance to the consistency mechanism, or by the EDPB in case of EEA-wide criteria. The Target of Evaluation should be checked under certification criteria by a certification body accredited by the national accreditation body or by the competent DPA, or both. According to Article 43 (1) GDPR, certification bodies which have an appropriate level of expertise in relation to data protection should, after informing the DPA in order to allow it to exercise its powers pursuant to point (h) of Article 58 (2) GDPR where necessary, issue and renew certification. According to Article 43 (5) GDPR, the certification bodies should provide the competent DPAs with the reasons for granting or withdrawing the requested certification. This does not mean that the certification body needs the authorisation of the DPA in order to issue certification. The certification body will be monitoring the compliance of its clients to the certification criteria.</p>	<p>Certification is voluntary, and all organizations seeking a certification must be certified according to requirements established by the Global CBPR Members and set forth in the Accountability Agent Application and the Global CBPR System Program Requirements Map. Certified organizations are subject to ongoing monitoring and compliance review and must undergo an annual re-certification process. All certified organizations are listed on a public directory maintained by the Global CBPR Forum.</p>

Depending on national laws, DPAs may also issue certification themselves. ¹³⁶	
--	--

¹³⁶ Article 42 (5) GDPR.