A New Era for Data Flows

ISRAEL AND THE GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FORUM

JUNE 2023

START-UP NATION
POLICY INSTITUTE

1 Introduction and objectives

Companies working in key sectors of the Israeli economy – hi-tech, bio-tech, finance and others – process personal data and thus are subject to local regulations on data protection. In case these companies export their products and services, or are involved in any form of cross-border data flows, they also need to comply and to be able to demonstrate compliance with data protection regulations of importing countries.

Transferring data across borders have become particularly challenging: privacy laws differ from country to country, including some countries with significant transfer restrictions on personal information collected for normal business purposes.[1] The need to address this challenge led to development of several international and regional arrangements in cross-border data flows and data protection.

On 21 April 2022, Canada, Japan, South Korea, the Philippines, Singapore, Chinese Taipei and the United States – 7 countries participating in the Asia-Pacific Economic Cooperation (APEC) – declared the establishment of the Global Cross-Border Privacy Rules (CBPR) Forum 'to promote interoperability and help bridge different regulatory approaches to data protection and security'.[2] The Global Forum operates two voluntary, accountability-based certification systems that allow organizations to demonstrate their compliance to internationally-recognized data protection and privacy standards: the CBPR System and Privacy Recognition for Processors (PRP) System.

The Global CBPR System, which is the main focus of this paper, was originally developed by APEC (and referred to as APEC CBPR) in 2011 to build consumer, business and regulator trust in cross border flows of personal information.[3] While APEC CBPR is a regional framework, the Global CBPR Forum intends to establish an international certification system (based on the

[1] CBPR website: http://cbprs.org/business/
[2] U.S. Department of Commerce. Global Cross-Border Privacy Rules Declaration. https://www.commerce.gov/global-cross-border-privacy-rules-declaration
[3] https://www.globalcbpr.org/about/

APEC CBPR and PRP Systems) and allow expansion of the membership beyond APEC to scale the collective benefits of the CBPR certification for companies, governments, and consumers. Importantly, the CBPR System does not substitute the APEC CBPR system, which continues to function as a regional framework.[4] As we show in the paper, APEC CBPR and Global CBPR systems have many common elements – e.g. share similar objectives and data protection principles - but have different organizational structures and operational procedures. Where possible, we compare the two systems to underline the differences between them; and, as Global CBPR is based on APEC CBPR, in cases only limited information is available on certain aspects of the Global CBPR (e.g., experience of business companies, application documents of the participating countries), we use the information on APEC CBPR to develop a broader picture on how the Global CBPR system should operate (even though it might not always be the case: the two systems are two separate entities).

The Global CBPR System is the only government backed voluntary international data privacy certification system that companies can participate in to demonstrate compliance with internationally recognized data privacy and facilitate cross-border data flows across multiple jurisdictions in the field of data protection and privacy. It is declared to be 'enforceable certification for companies to demonstrate compliance with internationally-recognized data privacy protections and facilitate cross-border data flows across multiple jurisdictions'.[5] Adobe, Apple, Mastercard, Cisco, HP, Electronic Arts are few examples of companies that are (APEC) CBPR certified.

[4] The first version of this paper was written about APEC CBPR, as limited information was available on the Global Forum.
[5] Aryeh Ness Presentation

This paper aims at providing responsible authorities with a basis for making a decision on whether Israel should join the Global CBPR Forum. To do so, we:

1. Describe Israel's profile in terms of data protection legislation and participation in international arrangements;
2. Identify the rationale for Israel to join the Global CBPR Forum;
3. Provide a detailed overview of the Global CBPR system (using APEC CBPR as example, where necessary), highlighting the differences with the GDPR approach, currently applied in Israel;
4. Analyze requirements for new countries and develop a draft implementation plan for Israel to join the Global CBPR system;
5. Provide examples of how APEC CBPR system was joined and is currently implemented by different countries (assuming that experience will be similar in case of Global CBPR system);
6. Analyzing commitments and potential consequences associated with joining the Global CBPR System.

2 Privacy and data protection legislation in Israel and international arrangements

Growing Internet connectivity and the digitization of the global economy, as well as increasing trade in data processing services and products, resulted in the rapid increase in the collection, use, and transfer of data across borders.[6] As the trend continues to accelerate, so grows the impact of data protection arrangements on international cooperation and trade.

Data protection is directly related to trade in goods and services in the digital economy, and data protection regulations should be proportionate to risks they set out to address. As it is the case in many other regulatory frameworks, the right balance between too stringent and insufficient regulation should be found, as:

- Too little protection can create negative market effects through affecting consumer confidence,
- Too much regulation can overly restrict business activities and trade.

Imbalanced data protection regulations can have serious consequences for either the protection of fundamental rights or for international trade. Ensuring that laws consider the global nature and scope of their application, and foster compatibility with other frameworks, is of importance for global trade.[7]

[6] U.S. Department of Commerce. Global Cross-Border Privacy Rules Declaration. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[7] Cecile Barayre, 2016. Data protection regulations and international data flows: implications for trade and development. https://www.wto.org/english/forums_e/business_e/3_4_cecile_ppt.pdf

2.1 Israel's privacy and data protection regulatory model

According to Digital Economy Report,[8] [9] Israel is one of 127 countries that have implemented data protection policies in national legislation (while 20 countries have only draft legislation and 48 reported to have no data protection legislation). Israeli local regulatory model, which is an adoption of the European regulation in the field of data protection (General Data Protection Regulation, implemented in 2018),[10] is characterized in the Report as "prescriptive" (as in case of other 22 countries,[11] including the European Union). Regulatory model of United States is characterized in the document as "light-touch", whereas that of China as "restrictive" (which makes the two countries the opposite ends of the "regulatory spectrum" with all other regulatory regimes falling somewhere in between).[12]

The regulatory model used in the European Union (GDPR) – which applies data protection and privacy requirements as direct law - has been adopted by many countries, including, as mentioned above, Israel. The reasons for the widespread adoption of the EU model are pragmatic:[13] The EU requires that countries wishing to do business in the EU have equivalent data protection requirements and basing local legislation on GDPR is a prerequisite for being recognized by the EU as "a country with an adequate level of data protection". Israel is one of several countries, for which EC adopted the "adequacy" decision. It means that "personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to [Israel] without any further safeguard being necessary. In others words, transfers to [Israel] will be assimilated to intra-EU transmissions of data".[14]

[8] UNCTAD, 2021. Digital Economy Report. https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf, as of 2021
[9] There are some inconsistencies in data of the report (e.g., UAE doesn't have local legislation according to one Annex, and has a prescriptive legislation according to another annex).
[10] GDPR EU Project. https://gdpr.eu/what-is-gdpr/
[11] The report evaluates regulatory model of only about 50 countries.
[12] Even though regulatory model of China is restrictive, the EU describes its regulatory model – see GDPR.EU project – as 'the toughest privacy and security law in the world'.
[13] Clare Sullivan, 2019. GDPR or APEC CBPR? https://www.sciencedirect.com/science/article/abs/pii/S026736491930038X

[14] European Commission, Adequacy Decisions. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

GDPR, according to the Digital Economy Report, is only one example of a ‘a regional trade-related’ arrangement on cross-border data flow, privacy and data protection, whereas the mechanism of “Adoption by EC of the "Adequacy" decision for a third country” is an example of an international arrangement in the field. By adopting the GDPR and getting an ‘adequacy’ decision, Israel participates in this arrangement and enjoys the benefits of free flow of data across borders.

2.2 Participation of Israel in international arrangements on data protection

At the same time, there are many other arrangements in this field. Digital Economy Report, apart from “trade related”, groups international arrangements on data protection as covering “economic domain” or being “beyond trade and economic domain”. Table 1 provides an overview of the existing arrangements on data protection, grouped by their type, and – for comparison purposes only – shows in which agreements participate Israel, EU (17 countries to which GDPR directly applies) and the US.

Table 1 Israel, EU and US in international and regional data protection arrangements

Arrangement	Israel	EU	US
International (trade related)			
World Trade Organization (WTO): Joint Statement Initiative (JSI) negotiations on e-commerce (2019)	Yes	Yes	Yes
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), signed in 2016 (initially TPP): Provisions for free data flows and ban on data localisation (exception clause for location of computing facilities)	No	No	No
Trade in Services Agreement (TiSA) (on hold), negotiations started in 2013: Commitment to free flow of data and a ban on data localisation	Yes	Yes	Yes
European Commission (EC): Adoption by EC of the "Adequacy" decision (Data protection) for a third country outside of the European Economic Area (Data Protection Directive, 95/46/EC, from 1995)	Yes	No (No need)	No
International (economic domain)			
G20: Osaka Track for the G20 initiative to implement "Data Free Flow with Trust" (signed in 2019)	No	No	Yes
Digital Economy Partnership Agreement (DEPA), signed in 2020: - Articles 4.3 and 4.4 respectively for free flows of cross-border data and ban on data localisation (with exception clauses for each)	No	No	No
Asia-Pacific Economic Cooperation (APEC): - Internet and Digital Economy Roadmap (IADER) (2017). - Cross-Border Privacy Rules (CBPR) System (2011) on voluntary basis	No	No	Yes
International (beyond trade and economic domain)			
Council of Europe (COE): - Convention 108+ (The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, convention 108 signed in 1981, amended in 2018 for 108+)	No	Yes	No
Organisation for Economic Co-operation and Development (OECD): - Guidelines on protection of privacy and transborder flows of personal data (2013) - “Principles for Internet Policy Making” (2014): support for free cross-border data flows	Yes	Yes	Yes
Red Iberoamericana de Datos Personales (RIDP), created in 2003: - Promotion of a regulatory framework for data protection (inspired by EU standards)	No	No	No
Economic Commission for Latin America and Caribbean (ECLAC): - Digital agenda "eLAC 2022", Goal 27: contains, among others, the mention of free flow of data with trust (2020)	No	No	Yes

Regional (trade related)			
European Union (EU) and European Economic Area (EEA): - General Data Protection Regulation (GDPR), implemented in 2018	No	Yes	No
United States Mexico Canada Agreement (USMCA), signed in 2019: - Binding commitment to free flow of data and a ban on data localisation	No	No	Yes
Dominican Republic-Central America Free Trade Agreement (CAFTA-DR): - Chapter 14 on e-commerce (2004)	No	No	Yes
Regional Comprehensive Economic Partnership (RCEP), signed in 2020: - Free flow of cross-border data and a ban on data localisation (with exception clauses for each)	No	No	No
Pacific Alliance (PA), founded 2011: - Cross-border data flows issues and ban on data computing localisation	No	No	No
MERCOSUR: - Digital Agenda Group (in Spanish GAD: Grupo Agenda Digital, created in 2017) with a proposal for an action plan on digital agenda	No	No	No
Regional (economic domain)			
Association of Southeast Asian Nations (ASEAN): - Agreement on E-Commerce (AE-Com) (2018): cross-border data flows facilitation and restriction on data localisation - Framework on Personal Data Protection (FPDP) (2016)	No	No	No
Regional (beyond trade and economic domain)			
African Union (AU): - Convention on Cyber Security and Personal Data (the Malabo Convention, 2014)	No	No	No
Organisation of American States (OAS): - “Updated Principles on Privacy and Protection of Personal Data” (2021) - "Legislative Guide on Privacy and Personal Data Protection in the Americas" (2015)	No	No	Yes

Israel has a unique profile in terms of its participation in international data protection arrangements. Along with the EU and US, Israel participates in the following international arrangements on data protection: WTO: JSI (2019), TiSA (on hold), OECD: Guidelines on protection of privacy and support for free CBDF.

As Israel is one of the countries for which EC adopted the "Adequacy" decision, in case Israel also participated in the “The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe”, then - from data protection regulation perspective - it would look just like any other EU country. Participation in the Convention, by the way, is the only difference between Israel and Switzerland.

United States, in contrast, participate in 9 multilateral arrangements, 3 of which are international in which neither Israel nor EU are present. The latter 3 arrangements, apart from CBPR, are Osaka Track and ELAC 2022. Together with the differences in regulatory model applied at the national level ("prescriptive" vs. "light-touch", according to the Report), participation in international agreements makes US regulatory framework different from that of EU and Israel.

At the same time, major differences between the Global CBPR System and GDPR (even though one is a voluntary multilateral regulatory arrangement and the second is a regulation) might not be in the essence of the applied data protection principles and regulatory requirements, but in the methods of assessing, ensuring and demonstrating compliance of business companies with these requirements.[15]

2.3 The main features of the Global CBPR System

Both APEC CBPR and the Global CBPR System are multilateral regulatory arrangements for data protection in which participation – on a governmental and business level – is voluntary. As it has been the case with APEC CBPR, the Global CBPR System "helps bridge different regulatory approaches by providing a single framework for the exchange of personal information among participating economies".[16] In contrast to General Data Protection Regulation (GDPR) – the CBPR System functions similarly to voluntary certification schemes (e.g., product certification, management system certification) and does not apply directly as law. As Israel is recognized by the EU as providing adequate protection, we won't describe all the available mechanisms for companies to prove compliance with GDPR, such as GDPR certification, and compare them with those of the Global CBPR System. A comprehensive analysis of the difference can be found in Sullivan, 2019.

[15] Detailed analysis of the requirements of the APEC Privacy Framework and GDPR can be found here: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_study_-_apec_cbpr_system_and_eu-us_privacy_shield_mapped_to_uk_gdpr.pdf

[16] In the original version it is "in the APEC region", but as Forum is open for participation, the objective spreads on all participating economies

The Global CBPR System can be described as:[17]

- **Voluntary**: The Global CBPR system is a voluntary set of operational program requirements based on the APEC Privacy Framework, that enables organizations and Businesses to show their compliance with international standards for privacy and data protection – and to improve their own data privacy programs.
- **Flexible**: The APEC Privacy Framework, on which both APEC and Global CBPR systems are based, explicitly calls for "flexibility in implementation" of its principles. The CBPR systems are designed to accommodate – rather than displace – the unique domestic privacy frameworks and legislative approaches of participating economies. Similarly, certified organizations are allowed flexibility to develop policies that meet their unique needs, so long as they demonstrate compliance with the CBPR program requirements.
- **Enforceable**: To participate in the Global CBPR system, each economy must designate a public authority that is "responsible for enforcing privacy law and that has the powers to conduct investigations or pursue enforcement proceedings." In case of APEC CBPR, each economy must join the APEC Cross-Border Privacy Enforcement Arrangement (CPEA), a collaborative, multilateral mechanism to promote cooperation and facilitate enforcement among their privacy enforcement authorities. Within the Global CBPR Forum, Private Enforcement Authorities of the economies participate in the Global Cooperation Arrangement for Privacy Enforcement (CAPE), which plays a role similar to that of CPEA.

[17] Based on the description of APEC CBPR in: CBPR, 2019. Benefits of CBPR System. http://cbprs.org/wp-content/uploads/2019/05/Benefits-of-CBPR-System-Guide_Jan-2019_FINAL.pdf

3 Rationale for Israel to join the Global CBPR Forum

Data protection arrangements play an increasingly important role in international trade, especially in trade in services, and most of the potential benefits associated with Israel's potential joining of the Global CBPR Forum are related to facilitation of international trade between Israel and other participating countries.

An Israeli company certified to the CBPR System will demonstrate its compliance with the data protection regulations of all jurisdictions that recognize CBPRs as a valid mechanism for data transfer, even if these regulations are different among the participating countries and between Israel and other countries (though both APEC and Global CBPR System are a voluntary certification scheme, they are recognized by governments).

Even if regulations in Israel are stricter than those of Global CBPR Forum participating countries, joining the Global CBPR System will lower compliance costs for Israeli companies as it is an efficient tool of demonstrating compliance with regulatory requirements of other countries.

The benefits of joining the Global CBPR System could be summarized as follows:[18]

1. **Membership in a club of countries with low acceptance costs**. Importantly, Israel can be one of the first countries outside the APEC region to join the club of countries, which, among other things, have a very different data protection/privacy profile (both in terms of national legislation and international arrangements – see Table 2 in Annex A.). The 'acceptance' costs will be low since the Global CBPR System itself is 'principles-based and flexible rather than prescriptive' and joining the System will not require any changes in legislation and will not create any contradiction with other international arrangements of Israel. As it is stated in the CBPR Policies, Rules and Guidelines (for the case of APEC CBPR),[19] and in the Global CBPR Framework (for the case of the Global CBPR System)[20]:

[18] CBPR, 2019. Benefits of CBPR System. http://cbprs.org/wp-content/uploads/2019/05/Benefits-of-CBPR-System-Guide_Jan-2019_FINAL.pdf
[19] CBPR, 2019. APEC CBPR. Policies. Rules and Guidelines. http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf
[20] https://www.globalcbpr.org/wp-content/uploads/Global-CBPR-Framework-2023.pdf

a. “The CBPR System does not displace or change an Economy’s domestic laws and regulations. Where there are no applicable domestic privacy protection requirements in an Economy, the CBPR System is intended to provide a minimum level of protection”.
b. “Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply. Where requirements of the CBPR System exceed the requirements of domestic law and regulation, an organization will need to voluntarily carry out such additional requirements in order to participate”.
c. The text of the APEC CBPR arrangement stresses that “nothing in this Cooperation Arrangement intends to create binding obligations, or affect existing obligations under international or domestic law, or create obligations under the laws of the Participants’ economies”.
d. One of the main requirements to join the framework for Israel will be to identify an appropriate regulatory authority as defined in the Global CBPR Framework to act as the Privacy Enforcement Authority (described further in the paper) in the Global CBPR System.
e. The 2023 Global CBPR Framework stresses the flexibility in implementing the CBPR Privacy Principles: “In view of the differences in social, cultural, economic and legal backgrounds of each Member, there should be flexibility in implementing the Global CBPR Privacy Principles”. It also states that “Members implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances”.

2. **Enhanced cooperation with regulatory authorities of the Global CBPR Forum countries**. Participation in the framework implies sharing of information, participation in investigations, etc. The system has an established mechanism to prioritize cases for

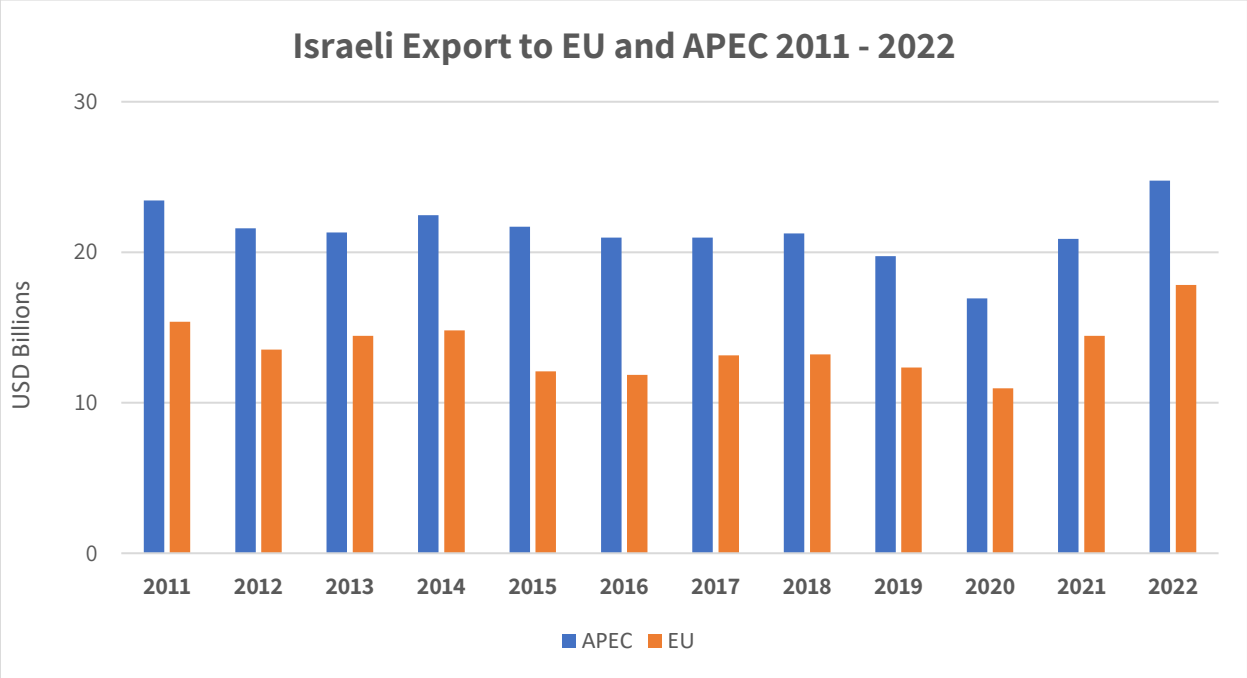
cooperation with public authorities in other economies based on the severity of the unlawful infringements of personal information privacy, the actual or potential harm involved, as well as other relevant considerations,[21] etc.

3. **Increasing the level of data protection and privacy enforcement in Israel, promoting compliance.** As the CBPR System is a voluntary framework, joining the Global CBPR Forum will result in creating a fully functional certification system in Israel. The CBPR System is very similar in some aspects (and even 'lighter') to voluntary management system certification: it relies on companies to set internal rules and procedures that meet high-standard principles of data protection, with external verification by third-party Accountability Agents and subject to enforcement by domestic privacy regulators. Delivering a ready-built, internationally-recognized framework will bolster privacy enforcement, facilitate compliance and increase investment attractiveness for Israeli companies;
4. **Using the Global CBPR System in the future Free Trade Agreements**. As of March 2023, Israel has Free Trade Agreements (in different development stages) with only 6 out of 21 APEC countries (Canada, US, Mexico, Korea, and Vietnam and China in late development phase), meaning 4 out of 7 countries that have joined the CBPR Forum. Participation in CBPR System is widely used in the existing Free Trade Agreements: for example, in the recent U.S.-Mexico-Canada Agreement (USMCA), the parties expressly recognized the CBPR system as "a valid mechanism to facilitate cross-border information transfers while protecting personal information", it is also the case with Australia-Singapore agreement). In case Israel joins the CBPR system, the framework can be referred to in future Free Trade Agreements between Israel and Global CBPR System countries.
5. **Efficient tool for demonstrating compliance**. Proving compliance to regulatory authorities of importing countries might be difficult even when a company is compliant

[21] Ibid.

with its regulations; CBPR system is an efficient tool for demonstrating compliance, including for the countries from the region importing to Israel. Singapore, for example, recognizes CBPR certifications under Personal Data Protection Regulations.

6. **Facilitating direct cooperation between Israeli and companies in the Global CBPR Forum Members**. CBPR certification will create a 'common language' and can be used as a reference in contracts; it will increase confidence and trust between trading partners. Not least important, it will increase consumer's trust in the region in Israeli companies, which is very significant in case of processing personal data. Since most of the Global CBPR Forum countries are from the APEC region, the graph below shows the importance of export to APEC region for Israel:



4 Overview of the CBPR Global Forum

4.1 Overview of the main documents establishing the Global CBPR System

The Global CBPR System is a government recognized data privacy certification that companies can join to demonstrate compliance with internationally-recognized data privacy protections. From the regulatory cooperation perspective, it is an example of a Multilateral Recognition Arrangement (such arrangements are quite common in the field of technical regulation).

The website of the Global Forum (https://www.globalcbpr.org/) contains a lot of useful information related to the functioning of the system, including the core documents that establish the international arrangement and the certification system. As the Global CBPR Forum establishes a certification system based on APEC CBPR and PRP Systems, description of the main documents establishing the APEC CBPR System might provide a broader perspective on the functioning of the new system and is presented in Box 1.

The main documents of the Global CBPR Forum include:

- The Global CBPR Declaration, which is a high-level document establishing the Global Forum. It was published on 21 April 2022, when Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America declared the establishment of a Global Forum to promote interoperability and help bridge different regulatory approaches to data protection and privacy. The document describes the rationale for the establishment of the Forum, defines its objectives and scope of activity, as well as its mode of operation, participation and organization of its work.
- Global CBPR Framework, another high-level but a more detailed (28 pages) document, describing:
    - The rationale for the establishment of the Forum and its main principles;
    - The scope of the Global CBPR Framework: definitions of the main terms, such “personal information”, “personal information controller”, ”publicly available

information" with commentaries, defining the scope of the system's application ("The Framework is intended to apply to information about natural living persons, not legal persons");
    - Global CBPR Privacy Principles (based on APEC Privacy Framework);
    - Guidance for domestic and international implementation.
- Global CBPR Forum Terms of Reference. The document supports the Declaration and the Framework (it refers to them as "setting forth the principles and objectives of the Forum) and provides information on:
    - The roles of Members and Associates of the Global CBPR system;
    - Organization structure of the Forum, its Global Forum Assembly, Committees (the Membership Committee, the Communications and Stakeholder Engagement, the Accountability Agent Oversight and Engagement) and their roles;
    - Selection, terms and functions of GFA Chair and Deputy Chair, Committee Chairs, as well as other details on organizational processes of the Forum.
    - Annex to the Terms of Reference describes a procedure for admission of Members and Associates to the Global CBPR Forum.
- Template of a Letter of Intent to Participate as Associate in the CBPR Forum, in which an applying economy, among other things, confirms that
    - it supports the principles and objectives of the Forum,
    - its legal system has the effect of protecting personal information
    - there is a public body responsible for the enforcement of the legal system, which has powers to conduct investigations or pursue enforcement proceedings.

Box 1. Overview of the main documents establishing the APEC CBPR System

The structure of the documents describing the APEC CBPR System is different from that of the Global CBPR Forum. The APEC CBPR documentation contains, inter alia, two sets of documents: one on the certification system applied to controllers (CBPR), and another on the certification scheme applied to processors (PRP).[22] So, the APEC CBPR documents can be divided into three groups:

- High-level documents, establishing the operation of the international arrangement and the principles of data protection. These documents are applicable to both CBPR and PRP and include:
    - APEC Privacy Framework,[23] the document containing, inter alia, the main principles of ensuring data protection to be applied within business companies
    - the Cross Border Privacy Enforcement Arrangement (CPEA),[24] establishing the system of governance of the framework and determining the roles and functions of the Joint Oversight Panel (JOP) and Electronic Commerce Steering Committee (ECSG)
    - JOP Charter for the CBPR and PRP Systems.[25]
- Documents, establishing the rules for CBPR system:
    - Policies, Rules and Guidelines.[26]
    - Program Requirements.[27]
    - Notice of Intent and Enforcement Map Template.[28]
    - Accountability Agent Application.[29]
    - Intake Questionnaire.[30]
- Documents, establishing the rules and procedures for PRP system. These documents are similar to those of CBPR, with the only difference that they also include "Purpose and Background Document".

CPEA is the abbreviation of the APEC Cross-border Privacy Enforcement Arrangement – it is the main 'operational' document of the APEC CBPR System. It describes CPEA as "a practical multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in cross-border privacy enforcement by creating a framework under which authorities may, on a voluntary basis, share information and request and render assistance in certain ways".

[22] As PRP functions similarly to CBPR, its detailed description is not within the scope of the paper.
[23] https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf
[24] http://cbprs.org/wp-content/uploads/2019/11/1.-Cross-Border-Privacy-Enforcement-Arrangement-updated-17-09-2019.pdf
[25] http://cbprs.org/documents/
[26] http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf
[27] http://cbprs.org/wp-content/uploads/2019/11/5.-Cross-Border-Privacy-Rules-Program-Requirements-updated-17-09-2019.pdf
[28] http://cbprs.org/wp-content/uploads/2019/11/6.-Template-Notice-of-Intent-to-Participate-in-the-CBPR-System-updated-17-09-2019.pdf
[29] http://cbprs.org/wp-content/uploads/2019/11/7.-Accountability-Agent-Application-for-CBPR-updated-2019.pdf
[30] http://cbprs.org/wp-content/uploads/2021/02/Cross-Border-Privacy-Rules-Intake-Questionnaire.pdf

The description of the Global CBPR Forum will cover:

- Objectives of the Forum;
- Main stakeholders of the Forum and their roles;
- Main principles, regulations and standard applied within the CBPR System;
- Certification scheme and the accreditation process;
- Enforcement and surveillance.

4.2 Objectives of the Global CBPR Forum

Objectives of the Global Forum, as they are described in the introduction to the Declaration on the establishment of the Forum, include 'ensuring trusted cross-border data flows' and balancing the advantages associated with cross-border data flows with the need of strong and effective data protection and privacy: it recognizes that "regulations can create barriers that will threaten to undermine opportunities created by the digital economy at a time when companies are relying increasingly on digital technologies and innovations". The APEC Privacy Framework, on which both APEC CBPR and Global CBPR Systems are based, contains a detailed description of the advantages associated with digital economy (see Foreword and Preamble) and defines the objectives of the (APEC CBPR) framework as "promoting electronic commerce throughout the Asia Pacific region". It is noted that the APEC Privacy Framework is based on the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines),[31] which we mentioned earlier and which are adopted by both US and EU, as well as Israel. The first version of the Guidelines was published in 1980 (and the previous version of the Framework (2005) was modelled upon this version. The current Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013) with due consideration for the different legal features and context of the APEC region.

The Global Forum declaration explicitly addresses 'companies across all sectors of the economy, including for micro, small and medium-sized businesses, workers, and consumers",

[31] OECD, 2018. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

highlighting that “trusted cross-border flows are indispensable not only for big, multinational technology companies”.

The Global CBPR Forum Framework adds that it specifically addresses the importance of protecting personal information and privacy while maintaining information flows. It states that the “practical and distinctive approach” of the Framework “is to focus attention on consistent rather than identical approaches to data protection and privacy”. The framework aims at finding the right balance between risk and regulation and “seeks to reconcile data protection and privacy with business and societal needs and commercial interests, and at the same time, accords due recognition to cultural and other diversities that exist within Members”.

To make the Global CBPR System operational both on international and business levels, the Global CBPR Framework calls its members to “refrain from restricting cross border flows of personal information between itself and another Member” if, inter alia, 1) “the other Member has in place legislative or regulatory instruments that give effect to the [Global CBRP] Framework” (international level) or the Global CBPR System is “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” (business level).

Any restrictions to cross-border flows of personal information should be proportionate 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.

Both APEC and Global CBPR Frameworks list the advantages of cross-border data flows that include greater international engagement, creating jobs, facilitating vital research and development in support of public health, fostering innovation and entrepreneurship, whereas the need for data protection is essential for strengthening consumer and business trust in digital transactions.

The APEC Privacy Framework was developed and updated in recognition of the importance of the following principles (which are applied, though through various mechanisms, within the Global CBPR System):

- Implementing appropriate privacy protections for personal information, particularly from the harmful consequences of intrusions and the misuse of personal information;
- The free flow of information to trade, and to economic and social growth in both developed and developing market economies;
- Enabling global companies that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- Empowering Privacy Enforcement Authorities to fulfill their mandate to protect individual privacy;
- Advancing international and regional mechanisms […] to promote and enforce privacy and to maintain the continuity of information flows among […] economies and with their trading partners;
- Encouraging organizations to be accountable for all personal information under their control; and
- Promoting interoperability between the Framework, and its implementing measures such as the CPEA (CAPE in case of the Global Forum) and CBPR system, and privacy arrangements in other regions.

4.3 The scope of the Global CBPR System

As in case of APEC CBPR, the Global CBPR Forum applies only to organizations (that is, businesses) and is not intended to deal with the personal information handling practices of governments or individuals.

The Global CBPR Framework contains two certification systems:

- Global CBPR system, applied to personal information controllers and
- Global PRP system, applied to processors.

In terms of data to be included into the scope, it is noted that information about "natural living persons, not legal persons" is included; it is explained that "the Framework applies to personal information, which is information that can be used to identify an individual" (or information that put together with other information would identify an individual).

According to the Global CBPR Framework, the CBPR System has four main components:

- Set criteria for bodies to become recognized as Global CBPR Forum Accountability Agents (bodies assessing compliance of business companies);
- a process for information controllers to be certified as Global CBPR system compliant by a recognized Accountability Agent;
- assessment criteria for use by recognized Accountability Agents when reviewing whether an information controller meets Global CBPR system requirements; and
- arrangements for enforcing Global CBPR system program through complaints processes provided by recognized Accountability Agents backed up by a Privacy Enforcement Authority (PEA) that is a participant in the Global Cooperation Arrangement for Privacy Enforcement.

The APEC CBPR and the Global CBPR systems have different organizational structures. The main stakeholders governing the APEC CBPR are Electronic Commerce Steering Group and Joint Oversight Panel, as well as controllers, Accountability Agents, CPEA, and Privacy Enforcement Authority. Within the Global CBPR Forum, the main stakeholders governing the

CBPR System are Global Forum Assembly and three Committees (Membership, Communications and Stakeholders Engagement, Accountability Agent Oversight and Engagement), as well as Global Cooperation Arrangement for Privacy Enforcement (instead of ECSG, JOP and CPEA in APEC CBPR). Their roles are described below.

4.4 Main players operating the international arrangement of the Global CBPR System

Within the Global Forum, the main players governing the work of the CBPR system are:

- Global Forum Assembly (GFA);
- Three Committees:
    - The Membership Committee;
    - The Communications and Stakeholders Engagement Committee;
    - The Accountability Agent Oversight and Engagement Committee.

GFA and Committees perform the roles similar to those of:

- Electronic Commerce Steering Group (ECSG) and
- Joint Oversight Panel

within the APEC CBPR system. Description of their functions is presented in Box 2.

Box 2. The ECSG and Joint Oversight Panel within APEC CBPR

Electronic Commerce Steering Group (APEC CBPR)

ECSG plays a key role in the governance of the framework – it designates the framework's administrator (it can be APEC Secretariat, or a Privacy Enforcement Authority of one of the participating countries). The roles of the administrator are described in APEC Cooperation Arrangement for CBPR,[32] and include, for example, receiving notices of intent to participate in the Cooperation, maintaining the list of current subscribers, etc.

It is the Chair of the Electronic Commerce Steering Group (ECSG Chair) who notifies the Economy that the necessary conditions have been met and it is considered a Participant in the Cross Border Privacy Rules (CBPR) System (CBPR Participant).[33] Another important function of ECSG is in establishing a Joint Oversight Panel, which plays a key "subject matter" role in the functioning of the system. Recommendations made by the Joint Oversight Panel take effect upon endorsement by the ECSG.

ECSG is the body that accumulates changes in national legislations: A CBPR and/or PRP Participant provide notice to the APEC ECSG Chair of 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 either system. The APEC ECSG Chair notifies APEC Economies of any notification received.

Joint Oversight Panel

The Joint Oversight Panel plays a key 'subject matter' role in governing the Framework:

1. It conducts consultations and evaluates countries willing to join the framework (submits to the Chair of the ECSG a report on the country willing to join the framework "as to how the conditions [required for] becoming a CBPR participant have been satisfied")
2. It performs activities similar to accreditation of Accountability Agents – recognizing Accountability Agents, ensuring continuous compliance with Accountability Agent Recognition Criteria, suspending the recognition; also, it advises to Accountability Agents whether or not to withdraw from particular engagements if a potential conflict is alleged.

JOP is established by ECSG and consists of representatives from three APEC Economies, for a two-year appointment; JOP Chairperson is elected for a two-year appointment from these three Economies. All recommendations of the Joint Oversight Panel will be made by simple majority.

[32] CPEA. http://cbprs.org/wp-content/uploads/2019/11/1.-Cross-Border-Privacy-Enforcement-Arrangement-updated-17-09-2019.pdf
[33] JOP Charter. http://cbprs.org/wp-content/uploads/2019/11/2.-JOP-Charter-updated-17-09-2019.pdf

4.4.1 Global Forum Assembly of the CBPR System

The Global Forum Assembly is a policy making body of the Forum. Its functions include:

- Setting the Forum's policy and strategy to advance the Forum's principles and objectives;
- Deliberating on, endorsing and implementing the GFA annual work program, documents, and other activities that contribute to the implementation of the Forum's principles and objectives;
- Establishing and dissolving Committees on an as-needed basis;
- Reviewing and endorsing recommendations made by its Committees;
- Appointing the GFA Chair and GFA Deputy Chair, as well as the Chairs and Members of its Committees.

The GFA consists of Members, Associates may participate in GFA meetings, unless the GFA Chair designates a meeting or part of a meeting as participation by Members only.

4.4.2 The Membership Committee

The Membership Committee of the Global CBPR Forum performs one of the roles of the Joint Oversight Panel of APEC CBPR. Specifically, the Committee:

1. Reviews and makes recommendations to the GFA on Membership and Associate applications;
2. Raises awareness of and promote participation in the Forum among jurisdictions;
3. Performs other tasks as assigned by the GFA Chair.

4.4.3 The Communications and Stakeholders Engagement Committee

The functions of the Communications and Stakeholders Engagement Committee are defined as follows:

1. Make recommendations to the GFA on developing and protecting the Forum brand;
2. Maintain the website, including the directory of Members and Associates, Global CBPR System - and Global PRP System - certified organizations, and AAs recognized by the Forum;
3. Manage the Forum documents and records database;
4. Raise awareness of and promote the Forum with stakeholders.

4.4.4 The Accountability Agent Oversight and Engagement Committee

Within the APEC CBPR System, it is the JOP that evaluates the applications for recognition of Accountability Agents. Within the Global CBPR System, this function is performed by the Accountability Agent Oversight and Engagement Committee. Its functions are defined as follows:

1. Review and make recommendations to the GFA on applications for recognition as an Accountability Agent **("AA")** [1];
2. Lead engagement with recognized AAs;
3. Provide oversight of and manage complaints against recognized AAs.

4.5 Main stakeholders of the Global CBPR certification system (on a country level)

4.5.1 Clients of the framework: controllers and processors

Personal information controllers are defined in the APEC Framework as "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". It is noted that the definition excludes:

- a person or organization who performs such functions as instructed by another person or organization.
- an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

The UK GDPR defines a controller as "the natural or legal person,[34] public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". It explains that "controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing". The following example is provided:

> A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information.
>
> The GP surgery will be the controller for the personal data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.

The Global CBPR Framework states that data protection and privacy management programs implemented by personal information controllers should:

a) be tailored to the structure and scale of the operations of the personal information controller, as well as the volume and sensitivity of the personal information under its control;

b) provide appropriate safeguards based upon risk assessment that take into account the potential harm to individuals;

c) establish mechanisms for internal oversight and response to inquiries and incidents;

d) be overseen by designated accountable and appropriately trained personnel; and

e) be monitored and be regularly updated.

[34] Information Commissioner's Office. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/

A list of controllers that are APEC CBPR certified is available at the CBPR website: http://cbprs.org/compliance-directory/cbpr-system/. The list includes Apple, Cisco, Electronic Arts, IBM, Mastercard, and many other companies.

The term **"Personal Information Processor"** is not defined in the APEC Framework. The UK GDPR defines a processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". It further explains that "processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own". Although a processor may make its own day-to-day operational decisions, it should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law. If a processor acts without the controller's instructions in such a way that it determines the purpose and means of processing, including to comply with a statutory obligation, it will be a controller in respect of that processing and will have the same liability as a controller. A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example a consultant.

The following example is given:

> A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations.
>
> The gym is the controller of the personal data processed in connection with the invitations. The gym determines the purposes for which the personal data is being processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the personal data using the data subjects' address details). The printing company is a processor processing the personal data only on the gym's instructions.

A list of processors that are APEC PRP certified is available at the PRP compliance directory at the APEC CBPR website: http://cbprs.org/compliance-directory/prp/. The list includes Adobe, Apple, HP, General Electric and many other companies.

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.

4.5.2 Accountability agents

Accountability agents play a role similar to that of certification bodies in product/management system certification. Accountability agent, by reviewing the questionnaires filled out by business companies, "determines whether an organization's privacy policies and practices are consistent with the program requirements of the CBPR System". The questionnaire only highlights the areas Accountability Agent is reviewing; internal review processes can differ from AA to AA.

APEC CBPR Policies, [35] Rules and Guidelines document lists requirements for Accountability agents (within APEC CBPR, to be approved by JOP, they need to provide evidence that these requirements are met; within the Global CBPR, they are approved by the Accountability Agents Oversight Committee). A country willing to participate in the Global CBPR System will nominate an Accountability Agent. Importantly, Accountability Agents can be nominated in any of the participating countries.

Within the APEC CBPR System, the Privacy Enforcement Authority (see below) of an Economy can assume the role of Accountability Agent. In this case, the nomination may be done by the Economy with a confirmation that the Privacy Enforcement Authority is a participant of the CPEA as well as a summary of how that privacy enforcement authority may enforce the program requirements of the CBPR system.

In the Global CBPR System, Accountability Agent needs to be independent of the Privacy Enforcement Authority. Within the APEC CBPR System, criteria for evaluating Accountability

[35] http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

Agents are formulated in Accountability Agent Recognition Application[36]. These criteria include requirements for:

- Avoiding conflicts of interest;
- Comprehensive review process;
- On-going monitoring and Compliance Review Process;
- Re-certification and annual attestation
- Dispute resolution;
- Mechanism for enforcing Program Requirements.

The document contains a self-assessment questionnaire to be filled by an applicant.

Nomination of accountability agents within the APEC CBPR system is organized as follows:

1. The participating country prepares an application, including:
    i. describing the relevant domestic laws and regulations which may apply to the activities of Accountability Agents
    ii. Accountability Agent Recognition Application;
    iii. A signed attestation by the Accountability Agent and all necessary supporting documentation as stipulated in the Accountability Agent recognition criteria.
2. Upon completion of the consultation process, the JOP in case of APEC will draft a report that recommends whether APEC member Economies should recognize that the applicant Accountability Agent has met the recognition criteria established in the *APEC Accountability Agent Recognition Application*;
3. Considering the request for recognition by the Economies, considering the recommendation of JOP;

[36] http://cbprs.org/wp-content/uploads/2019/11/7.-Accountability-Agent-Application-for-CBPR-updated-2019.pdf

4. If no objections are received from Economies within a set deadline, the request will be considered to be approved by the Global Forum Assembly. Once recognized, Accountability Agents must make their completed APEC Accountability Agent Recognition Application (excluding all business proprietary or confidential information) available on their website and easily accessible to consumers. The JOP will ensure that the Accountability Agent Recognition Application and associated findings report are circulated to all APEC member Economies by the APEC Secretariat and are posted on the CBPR website.
5. Re-evaluation (first time – after one year, then – biannually).

Within the Global CBPR system, the nomination of Accountability Agents is processed by the Accountability Agents Oversight and Engagement Committee.

Interestingly, Accountability Agents:

- Are required to release anonymized case notes and complaint statistics. Complaint handling is an important element of the CBPR System.
- Should consent to respond to requests from relevant government entities in any APEC Economy that reasonably relate both to that Economy and to the CBPR-related work of the Accountability Agent, where possible.
- Should endeavor to cooperate when appropriate and where possible in CBPR-related complaint handling matters with other recognized Accountability Agents.

4.5.3 Privacy Enforcement Authority and the Global CAPE

A Privacy Enforcement Authority is a public body that is responsible for enforcing Data Protection and Privacy Laws. It has powers to conduct investigations and/or pursue enforcement proceedings. A member may have more than one Privacy Enforcement Authority.[37]

The APEC CBPR Policy highlights the following roles of PEA:

- Review a CBPR complaint/issue if it cannot be resolved by the participating organization in the first instance or by the Accountability Agent and when appropriate, investigate and take enforcement action. The Privacy Enforcement Authority has the discretion to decide whether or not to deal with a Request for Assistance made by another Privacy Enforcement Authority.
- CPEA participation is the predicate step to any Economies' involvement in the CBPR System as the CPEA establishes that the Economy has a law in place "the enforcement of which, has the effect of implementing the APEC Privacy Framework."

Within the Global CBPR System, PEA participates in the Global CAPE: the Global Cooperation Arrangement for Privacy Enforcement. The Global CBPR Frameworks defines the Global CAPE as "a practical multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in cross-border 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". The roles of the Global CAPE within the Global CBPR System are similar to those of CPEA within the APEC CBPR System; the main difference is that in case a country becomes an Associate Member within the Global CBPR System (there is no such option in the APEC CBPR), its PEA does not need to join CAPE (the latter is required only in case of full membership).

[37] Global CBPR Framework.

4.6 Privacy and data protection principles and standards applied with the CBPR framework

APEC Framework is the main document on which the Global CBPR program requirements - criteria against which organizations are evaluated – are based.[38] Organizations that choose to participate in the CBPR System should implement privacy policies and practices consistently with these requirements.

The principles of the APEC Framework include:

1. Preventing harm
2. Notice
3. Collection Limitation
4. Uses of personal information
5. Choice
6. Integrity of personal information
7. Security Safeguards
8. Access and correction
9. Accountability

Principles are represented by a set of questions together with assessment criteria. Importantly, for the purposes of participation in the CBPR System, evaluation only applies to an organization's compliance with its CBPR commitments, not its compliance with applicable domestic legal requirements.

[38] http://cbprs.org/wp-content/uploads/2019/11/5.-Cross-Border-Privacy-Rules-Program-Requirements-updated-17-09-2019.pdf

4.7 Process for evaluating compliance

CBPR certification system contains the following main elements:

- Self-assessment
- Compliance review
- Recognition
- Enforcement

The process is organized as follows:

1. A business company willing to attain CBPR certification chooses an Accountability Agent (in case an Accountability Agent is from a different jurisdiction, JOP approval is necessary for APEC CBPR, and that of Accountability Agent Oversight Committee within the Global System), who provides a self-assessment questionnaire to the organization. The organization performs self-assessment against CBPR Program Requirements;
2. The company submits the questionnaire to the "appropriate CBPR-recognized Accountability Agent, in accordance with established selection requirements";
3. The Accountability Agent performs a confidential review against the baseline standards established in the CBPR program requirements, which might result in an iterative process. These program requirements are designed to provide the minimum standard that applicant organizations should meet in order to ensure that the assessment process is conducted in a consistent manner across participating Economies. An APEC-recognized Accountability Agent's assessment process may exceed this standard but may not fall below it. Accountability agent may request answers on additional questions, documentation or requests for clarification as part of the review process.
4. If the company is found to be compliant with the CBPR program requirements by an APEC-recognized Accountability Agent, it will be certified as CBPR compliant. Once an organization has been certified for participation in the CBPR System, these privacy policies and practices will become binding as to that participant and will be enforceable

by an appropriate authority, such as a regulator to ensure compliance with the CBPR program requirements.

5. Details on company's certification will be published on CBPR website in a publicly accessible directory of organizations that have been certified by Accountability Agents as compliant with the CBPR System. The information will include the the contact point information for the APEC- recognized Accountability Agent that certified the organization and the relevant Privacy Enforcement Authority. 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 Privacy Enforcement Authority.

4.8 Enforcement within the CBPR Framework

CBPR Policies, Rules and Guidelines determine both Accountability Agents and Privacy Enforcement Authorities as responsible for enforcement activities within the framework. It states that:

- Accountability Agents should be able to enforce the CBPR program requirements through law or contract; and
- The Privacy Enforcement Authorities 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 CBPR program requirements.

Enforcement activities are also supported within the framework on the international level (CPEA within the APEC CBPR System and the Global CAPE in the Global CBPR system); participation in the framework allows for joining information sharing among Privacy Enforcement Authorities of participating economies, provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions.

5 Joining the Global CBPR System: requirements, action plan and commitments

5.1 Associate and Member Status

Within the Global CBPR System, a country can be either an Associate or a Member.

To become a Full Member, a jurisdiction must be able to prove that it:

1. Concurs with the principles and objectives of the Global CBPR 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;
2. Has at least one Privacy Enforcement Authority as a participant in the Global Cooperation Arrangement for Privacy Enforcement ("Global CAPE"); and
3. Either:
    1. Intends to make use of at least one Forum-recognized Accountability Agent ("AA"), and submits an explanation of how the Global CBPR and/or Global PRP program requirements may be enforced in its jurisdiction; or
    2. 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.

Criteria for Associate Status are less stringent: apart from supporting the principles and objectives of the Forum, an applying country should demonstrate that it has laws/regulations the enforcement of which has the effect of protecting personal information and that it has at least one public body responsible for enforcing these regulations (and which has powers to conduct investigations or pursue enforcement proceeding).

It is noted in the document, that the Associate status is granted initially for a period for two years, during which an Associate is expected to initiate an application for Membership. A year into the start of its Associate status, an Associate should provide updates on its plans for the initiation of Membership application to the Chair of the Membership Committee, including a description of work done to date.

5.2 Application process

The process of joining the Global CBPR Forum is described in Annex A of the Global CBPR Forum Terms of Reference "Admission of Members and Associates to the Global CBPR Forum" and contains the following steps:

- Submission of Application. The application for Membership or Associate status should be submitted, with the letter of intent signed by an appropriate governmental representative of the Applicant, to the GFA Chair, with copy to the Chair of the Membership Committee.
- Review of Application. Upon receipt of the application, the Membership Committee reviews the application as to whether the conditions for Membership applications or for Associate status applications, whichever is applicable, have been satisfied.
- Consultations. As part of the review, the Membership Committee may undertake consultations with the Applicant to clarify elements of the application or ask for additional information or clarification from the Applicant.
- Once the Membership Committee has completed its review, it transmits a recommendation to the GFA for consensus decision.
- Notification. The GFA Chair communicates the outcome of the application in writing to Applicants.

5.3 Requirements for a country to join the Global CBPR as a Member

To join the Global CBPR Forum as Member, the following the following actions are required:

1. Israel must maintain a Privacy Enforcement Authority, which "should be provided with governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions in an objective, impartial and consistent basis". It is noted that PEA "mmay 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".

2. Privacy Enforcement Authority of Israel must participate in the Global CAPE.
3. Israel must express its intention to participate in the Global CBPR system by submitting a letter of intent (its template is available on the website) addressed to the Chair of the Global Forum Assembly with a copy to the Chair of the Membership Committee containing:
    1. A confirmation that Israel supports the principles and objectives of the Forum set forth in the 2022 Global CBPR Declaration and the Global CBPR Framework;
    2. A confirmation that Israel intends to make use of at least one Forum-recognized Accountability Agent ("AA"), and submits an explanation of how the Global CBPR program requirements may be enforced in its jurisdiction. In case Israel does not intend to make use of a Forum-recognized Accountability Agents, the application should demonstrate that Israel's domestic system recognizes the Global CBPR System and/or Global PRP System as a valid data transfer mechanism.
    3. Narrative description of relevant domestic laws, regulations and administrative measures (overview of the domestic legal system) and the relevant authority or authorities responsible for enforcement of those laws, regulations and administrative measures and how those domestic laws, regulations and administrative measures could be enforced**.**

       Letter can be submitted by appropriate government representative.

(In case of the APEC CBPR, an applicant economy must also complete the APEC Cross Border Privacy Rules System Program Requirements Enforcement Map with details of relevant domestic laws, regulations and administrative measures that would have the effect of protecting personal information consistent with the APEC CBPR system

requirements and how they would be enforced with respect to organisations operating from or within the country's jurisdiction. Template notice of intent and enforcement map).

4. Once the above information is received, the Membership Committee will initiate a review of the application (as to whether the Membership conditions are satisfied) and, if needed, a consultation process with the Applicant.
5. At the end of the consultation process, the Membership Committee will transmit a recommendation to the GFA for a consensus decision.

5.4 Action plan for Israel to join the CBPR Framework

1. Identifying a Privacy Enforcement Authority;
2. Initiating participation of the Israeli PEA in the Global CAPE;
3. Making a decision on whether to use a Forum-recognized Accountability Agent or to recognize the Global CBPR System and/or Global PRP System as a valid data transfer mechanism;
4. Preparing the letter of intent and description of the domestic legal system.

Templates and the documents to be submitted by participating countries can be found at the Global CBPR website; for information, examples of documents submitted by countries participating in the APEC CBPR system (descriptions of legal systems, regulations, etc.) can be found at http://cbprs.org/documents/.

5.5 After joining CBPR: commitments and potential consequences

Joining the framework will require – on a government level:

- Ensuring the functioning of the enforcement body (PEA);
- Engaging in active cooperation within relevant non-governmental stakeholders (citizens, consumers, industry and technical and academic communities) to ensure the achievement of Framework's objectives;

- Publicizing how Data Protection and Privacy Laws and other arrangements provide protections to individuals, engaging in awareness raising activities and capacity building efforts across the public and private sectors;
- Participating in the functioning of the arrangement: participation in the work of the Global Forum Assembly, sharing information surveys and research in respect of matters that have a significant impact on data protection and privacy, sharing techniques in investigating violations, etc.
- Cooperating with other participating countries in the enforcement of data protection and privacy laws.
- Providing assistance to other PEAs within the framework.

Potential implications to be addressed:

- Regulatory framework in Israel is tougher than the one described in the APEC Framework. Creating additional certification system for companies that work in a more stringent regulatory environment which is not based on third party certification process, might create 'dual responsibility' situation. Measures should be taken to ensure that participation in the Global CBPR system does not compromise existing regulatory requirements.
- Participation in the Global CBPR System should not have any negative impact on Israel's participation in other international arrangements.

6 Experience of APEC CBPR participating countries

This section provides an overview of countries experience in participating in the APEC CBPR System. Though it is an entity separate from the Global CBPR System, documents submitted by CBPR participants to JOP to be accepted to the framework provide a lot of useful information on regulatory frameworks of the countries and can be used as templates when preparing Israel's letter of intent and enforcement map. Time difference between the date of submission of a letter of intent and publication of JOP finding's report can be used to evaluate the duration of the acceptance process.

6.1 United States

United States sent the letter of intent to join the Framework on 22 May 2012. The letter of intent and the supporting attachments were submitted as one document which can be found here: http://cbprs.org/wp-content/uploads/2021/02/13_ecsg_dps1_011_US-notice-of-intent_LIMITED_25-COPIES-ONLY.pdf

The JOP findings report was published on 25 July 2012 and can be found here: http://cbprs.org/wp-content/uploads/2021/02/13_ecsg_dps1_012_US-findings-report.pdf

Accountability Agents in the US include: [39]

- TRUSTe
- BBB National Programs
- NCC Group Security Services, Inc
- Schellman & Company, LLC

[39] Present in the compliance directory, only CBPR scheme.

6.2 Mexico

Mexico sent the letter of intent and the enforcement map as two separate documents on 24 September 2012: http://cbprs.org/wp-content/uploads/2021/02/13_ecsg_dps1_009_mexico-notice-of-intent.pdf and https://cbprs.blob.core.windows.net/files/Mexico%20Enforcement%20Map%20and%20Annex%20A.pdf

The JOP findings report was published on 16 January 2013.

No information on Accountability Agents in Mexico is available.

6.3 Japan

Japan submitted the letter of intent and a completed Enforcement map on 7 June 2013.

Confirmation of CPEA participations of Japan was submitted on 5 February 2014.

JOP findings report was published on 25 April 2015.

Accountability agents in Japan:

- JIPDEC

6.4 Canada

Canada submitted the documents for participating in the framework on 7 August 2014. JOP findings report was published on 1 April 2015.

No information on Accountability Agents in Canada is available.

6.5 Korea

Korea submitted the letter of intent and an Enforcement Map on 28 September 2016. JOP findings report was published on 1 June 2017.

Accountability agents in Korea:

- Korea Internet & Security Agency (KISA)

6.6 Singapore

Singapore submitted the letter of intent on 23 June 2017, together with two separate documents: “Domestic Laws Regulations Applicable to Accountability Agents” and “Singapore CBPR Enforcement map”. JOP findings report was published on 15 December 2017.

Accountability agents in Singapore:

- Infocomm Media Development Authority

6.7 Australia

Australia sent the letter of intent and a completed enforcement map on 1 August 2018. JOP findings report was published on 02 November 2018.

No information on Accountability Agents in Australia.

6.8 Philippines

The Philippines letter of intent and enforcement map was sent to JOP on 19 August 2019. JOP findings report was published on 9 March 2020.

No information on Accountability Agents in the Philippines is available.

6.9 Chinese Taipei

Chinese Taipei letter of intent is and completed enforcement map was submitted on 6 June 2018, JOP findings report was published on 21 November 2018.

No information on Accountability Agents in Chinese Taipei is available.

7 Joining the CBPR Framework: business perspective

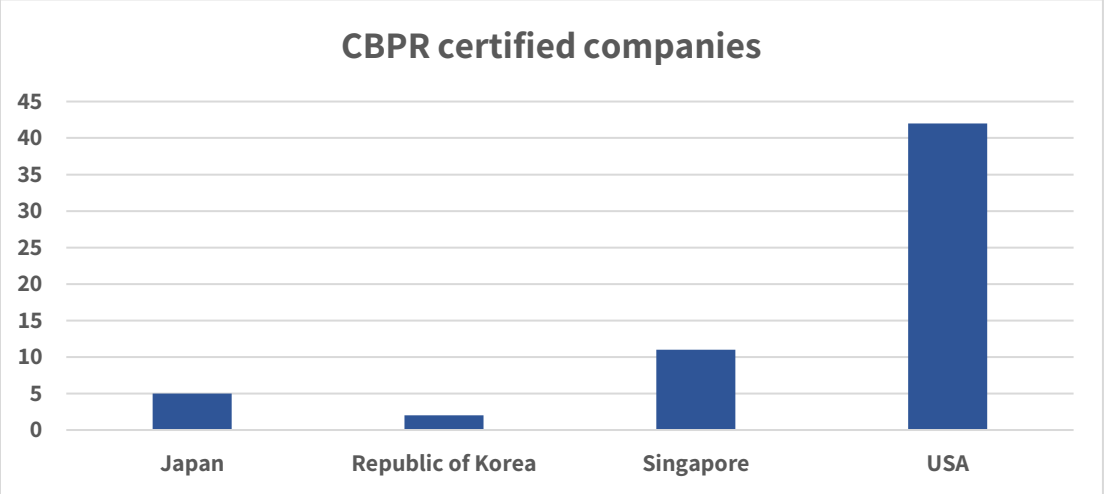
This section describes the business perspective of joining the CBPR framework and focuses on the main reasons why the framework should be suitable for the Israeli companies, in particular start-ups. We analyze:

- The sectoral profile of APEC CBPR certified companies - to show that it reflects the main activity sectors of Israeli start-ups;
- Dynamics of the APEC CBPR system - to highlight that the system is still relatively young and growing;
- Information available in the APEC CBPR compliance directory - to evaluate the reputational benefits of APEC CBRP certification;
- Certification process – to conclude that it should be at least less stringent than alternative data protection certifications;
- Costs associated with APEC CBPR certification and with maintenance of the system - to show that certification should not be associated with substantial costs and is suitable for small start-ups (though most of the CBPR certified businesses are big companies).

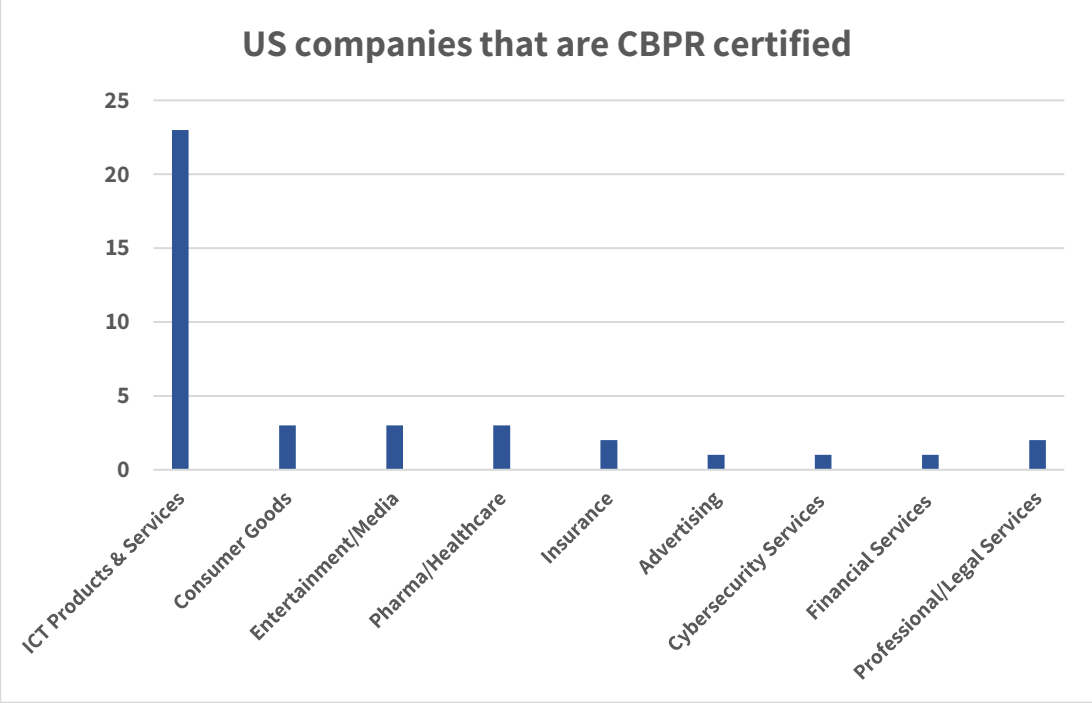
7.1 Business profile of certified companies reflects the key areas of Israeli start-ups

The CPBR website contains a "compliance directory",[40] in which all certified companies are listed.

As of April 2023, 60 companies are CBPR certified; 70% of these companies are from the US:



Distribution of these companies across sectors is the following:



[40] http://cbprs.org/compliance-directory/cbpr-system/

Most of the certified companies in the US (as mentioned above - 70% of total amount of certified companies in the world) belong to, not surprisingly, the "ICT Products&Services", [41] whereas other sectors, represented by less than 3 companies each, include:[42]

- Consumer goods,
- Entertainment/media,
- Pharma/Healthcare,
- Insurance,
- Advertising
- Cybersecurity
- Financial Services
- Professional/Legal Services.

The distribution of certified companies across sectors closely represents the structure of investments in private high-tech companies by area of activity (as of 2021 and shown here),[43] so profile of CBPR certified companies fits the Israeli start-up industry.

7.2 A new but growing network of certified companies

CBPR is still a relatively new certification system which obviously hasn't yet reached its full potential – as shown in the graph below, it has been slowly growing since 2015:

[41] TRUSTe is the most popular Accountability Agent, as 33 were certified by TRUSTe (4 by NCC, and 3 by BBB).
[42] Aryeh Ness presentation; it also states that there are more than 1800 entities certified.
[43] https://innovationisrael.org.il/en/reportchapter/part-israeli-high-tech-2022-situation-report

Joining the framework at the beginning of its development can give Israeli start-ups a competitive advantage in terms of global reputation, as well as in positioning on the US and other participating jurisdiction's market.

7.3 A "user-friendly" certification process

In case a company has developed and implemented privacy policies necessary to comply with the CBPR framework (discussed later in this section), the certification process includes the following steps (accountability agents might have slightly different processes, so below is a compilation of various descriptions):

- Selection of an Accountability Agent (US is the only country which has several Accountability Agents);
- Submitting an application to the Accountability Agent;
- Performing a self-assessment - filling out an Intake Questionnaire (50 questions);
- Due diligence of company's policies and practices by the Accountability Agent;
- Processing the Accountability Agent's feedback and, if necessary, modifying company's policies to meet CBPR requirements;
- Providing a proof of certification by Accountability Agent.

As in most third-party certification frameworks, getting a certification signifies only the beginning of cooperation between a company and an accountability agent, as:

- Certified companies are subject to ongoing monitoring and guidance by Accountability Agents;
- Accountability agents participate in dispute resolution and enforcement, if needed.
- Re-certification (certification renewal) is conducted on the annual basis.

The most resource consuming activity in the process is self-assessment, which requires providing information on 50 questions. The questionnaire is available online and reflects the main principles of the APEC framework;[44] the certification process does not require an on-site audit, which is the main source of costs for businesses participating in other certification systems.

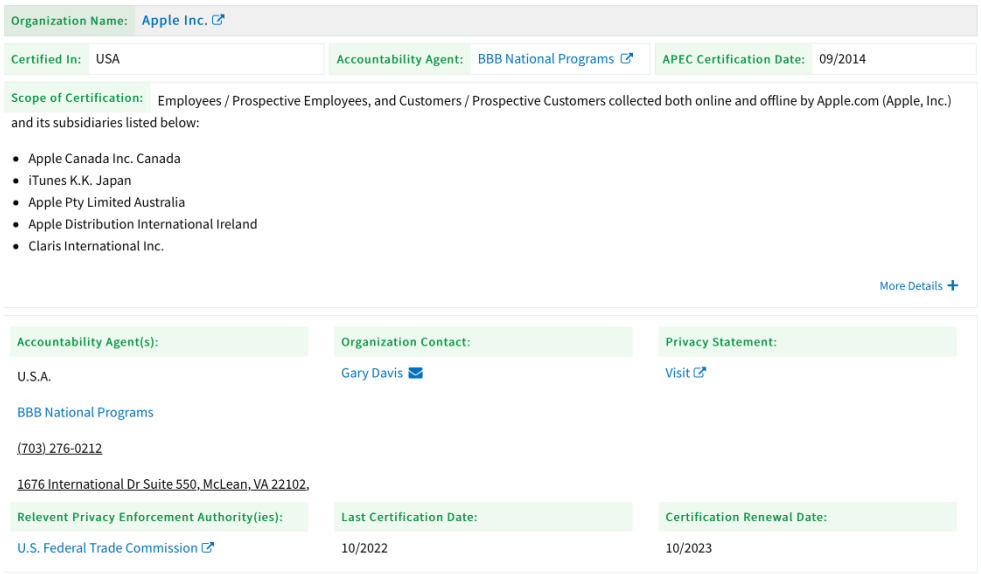
[44] http://cbprs.org/wp-content/uploads/2021/02/Cross-Border-Privacy-Rules-Intake-Questionnaire.pdf

7.4 Getting into the CBPR online inventory

As stated above, organizations that are certified are listed on the CBPR website. The following information is available about each company:

- Organization name;
- Country in which the company is certified;
- Accountability agent;
- Certification date;
- Scope of certification;
- Organization contact;
- A link to company's privacy statement;
- Relevant Privacy Enforcement Authority;
- Last certification date;
- Certification renewal date.

An example of company's profile is below:



Companies currently listed in the APEC CBPR compliance directory include:

Company name	Country	Certification year
1. [24]7.ai, Inc.	USA	2018
2. Alibaba Cloud (Singapore) Private Limited	Singapore	2021
3. Apple Inc.	USA	2014
4. Assurant, Inc.	USA	2020
5. Asurion, LLC.	USA	2017
6. BitSight Technologies, Inc.	USA	2021
7. Box, Inc.	USA	2014
8. Cisco Systems, Inc.	USA	2016
9. Computer Expert Group LLC	USA	2022
10. Credly, Inc.	USA	2020
11. CrimsonLogic Pte Ltd	Singapore	2020
12. Crowley Webb & Associates, Inc.	USA	2018
13. Cvent, Inc.	USA	2021
14. DoubleVerify Inc.	USA	2021
15. Electronic Arts	USA	2017
16. Expedia, Inc.	USA	2021
17. Foris Asia Pte. Ltd.	Singapore	2022
18. Foris DAX Asia Pte. Ltd.	Singapore	2022
19. General Electric Company	USA	2018
20. GoTo Group, Inc.	USA	2020
21. Herbalife Nutrition	USA	2021
22. Hewlett Packard Enterprise Company	USA	2015
23. HP Inc.	USA	2014
24. Hyland Software, Inc.	USA	2022
25. Infor (US), LLC	USA	2019
26. Intasect Communications, Inc.	Japan	2016
27. International Business Machines Corporation (IBM)	USA	2013
28. Internet Initiative Japan Inc.	Japan	2022
29. Johnson Controls, Inc.	USA	2020
30. Kobre & Kim LLP	USA	2017
31. Kyndryl, Inc.	USA	2021
32. Lark Technologies Pte. Ltd.	Singapore	2022
33. Mastercard International, Inc.	USA	2019
34. Medallia, Inc.	USA	2021

35. Midea Electric Trading (Singapore) Co. Pte. Ltd.	Singapore	2021
36. NAVER Cloud Corporation	Republic of Korea	2023
37. NAVER Corporation	Republic of Korea	2022
38. Organon & Co.	USA	2021
39. Paidy inc.	Japan	2018
40. PayPay Corporation	Japan	2022
41. PGA Tour	USA	2018
42. Rackspace Technology Global, Inc.	USA	2017
43. Reltio Inc.	USA	2019
44. Rimini Street, Inc.	USA	2014
45. Rubrik	USA	2023
46. Salesforce.com Inc.	USA	2022
47. Sapience Consulting Pte Ltd	Singapore	2023
48. Singapore Life Ltd	Singapore	2022
49. Talkdesk, Inc.	USA	2021
50. The Great Eastern Life Assurance Company Limited	Singapore	2020
51. TRS Forensics Pte Ltd	Singapore	2021
52. Twilio, Inc.	USA	2022
53. UKG	USA	2016
54. United Overseas Bank Limited	Singapore	2022
55. Workday, Inc.	USA	2014
56. World Wrestling Entertainment, Inc.	USA	2017
57. Yahoo Japan Corporation	Japan	2022
58. Yardi Systems, Inc.	USA	2021
59. Yodlee, Inc.	USA	2013
60. Ziff Davis, LLC	USA	2014

Getting into the CBPR compliance directory can give Israeli companies a competitive advantage in terms of international reputation.

7.5 Business costs of CBPR compliance

As in any certification framework, costs of compliance include:

- Costs for building a data protection management system within a business company (in case of Global CBPR System, based on the APEC Privacy Framework and CBPR program requirements), such as those associated with design and implementation of controls to prevent harms resulting from the wrongful collection and misuse of personal information, etc.;
- Certification costs;
- Costs for maintaining the system, such as those associated with reviewing and updating of data protection controls and internal procedures;
- Re-certification costs.

According to the Global Framework, the personal information controllers shall develop and implement data protection and privacy management programs for all personal information under their control. Data protection and privacy management programs should:

a) be tailored to the structure and scale of the operations of the personal information controller, as well as the volume and sensitivity of the personal information under its control;

b) provide appropriate safeguards based upon risk assessment that take into account the potential harm to individuals;

c) establish mechanisms for internal oversight and response to inquiries and incidents;

d) be overseen by designated accountable and appropriately trained personnel; and

e) be monitored and be regularly updated.

Costs for building/maintaining a privacy/data protection system according to the CBPR systems are hard to evaluate as they might differ from company to company. It is important to note, though, that "concerns raised by US multinationals about compliance costs [associated with GDPR]"[45] were one of the rationales for building the CBPR framework. Sullivan (2019) also

[45] Clare Sullivan, 2019. GDPR or APEC CBPR?

states that “in the US, the APEC approach using its CBPR scheme is widely considered to be the better model for cross border data transfer, primarily because it is regarded as less prescriptive and restrictive than the GDPR and therefore more conducive to facilitating international data flows”. One of the reasons why CBPR is less prescriptive is that the Framework is based on risks to the data and not “framed in terms of risk to data subjects and their rights”, as it is the case with GDPR. Since Israeli companies comply with GDPR regulations and there is a 61% overlap between the GDPR and CBPR requirements,[46] the costs for adapting the data protection system to conform with the requirements of the framework should not be substantial.

The only information on certification/re-certification costs available at the time of the writing was found at the website of the Singapore Accountability Agent (IMDA), which states that “Application fee of S$535 (inclusive of GST) is payable to IMDA. Assessment fee, payable to the Assessment Body, ranges and depends on the size of the organization (e.g., annual sales turnover, no. of sites, etc.) and the Assessment Body you engaged”.[47] In any case, certification costs should not be very different from other certification frameworks, as, in any case, certification does not include an onsite audit.

An overview of the business perspective of joining the CBPR frameworks shows that:

- A distribution of companies that are already CBPR certified across sectors is very similar to those of the Israeli start-ups.
- CBPR is a growing system and Israeli companies could enjoy the benefits of joining the framework when it is still relatively young;
- CBPR compliance costs should not be substantial as the framework was developed in response to concerns raised by US multinationals regarding the costs associated with compliance to regulations that are similar to those currently applied in Israel.

[46] Centre for Information Policy Leadership. APEC Cross-Border Privacy Rules Requirements and EU-U.S. Privacy Shield Requirements Mapped to the Provisions of the UK General Data Protection Regulation,

[47] https://www.imda.gov.sg/how-we-can-help/cross-border-privacy-rules-certification

8 Conclusion

Digital Economy Report stresses that "the state of the international debate on how to regulate cross-border data flows is at an impasse,[48] and positions tend to be polarized as current regulatory landscape is patchy, reflecting starkly different approaches adopted by different countries, with strong influences from the major economic powers"; it calls for "for moving away from the silo approach towards a more holistic, coordinated global approach".

Local privacy/data protection legislation of Israel is based on EU GDPR, which is more stringent than the model of the Global CBPR Forum. As GDPR compliant companies should be compliant with CBPR Program Requirements, and while global approach to data protection is still under development, joining the Forum will provide an effective method for demonstrating compliance of Israeli companies with regulations of participating countries of the Forum.

Joining the Global CBPR Forum has relatively low costs: it will not require any changes in legislation. The existing Privacy Enforcement Authority could represent Israel at the Forum; the only substantial change that will need to be made is the appointment of an Accountability Agent.

Obtaining and maintaining CBPR certification is not expected to be associated with substantial costs for Israeli companies, as the framework was developed in response to concerns raised by US multinationals regarding the costs associated with compliance to regulations that are similar to those currently applied in Israel. The framework, hence, should be suitable to start-ups as well as to big companies. When certified, Israeli companies will be listed in the CBPR compliance directory, along with Apple, HP, Mastercard and many other well-known companies.

[48] https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf

One of the concerns associated with joining the forum discussed in the paper is that introducing a less stringent voluntary model might have undesirable effects on the compliance with a more stringent obligatory model. These issues, however, can be addressed by ensuring awareness of CBPR participants on the differences between obligatory and voluntary frameworks.

Participation in the Global Forum can bring a lot of advantages in terms of cooperation with the region: both in terms of direct cooperation among trading partners and in future (and existing) Free Trade Agreements and in enhancing data protection in Israel.

Israel can become one of the first countries out of the APEC region to join CBPR, which can provide it with advantage within the Forum. In general, diversifying international arrangements on data protection can be of strategic importance in the changing world of global data protection regulations.

9 Annex A. Comparing the regulatory profiles of Israel and other Global CBPR Forum countries (local data protection legislation and participation in international arrangements)

The table below summarizes "regulatory profiles" of Israel and countries participating in the Global CBPR Forum.

Table 2. Israel has a very different profile than CBPR countries

	Israel	Philippines	US	Republic of Korea	Australia	Mexico	Japan	Canada	Singapore
Local legislation	Prescriptive, GDPR based	Light-touch	Light-touch	Prescriptive (but not too much)	Light-touch over-all	Light-touch	Favoring a light-touch	Light-touch (some exceptions)	Light-touch
WTO: JSI (2019)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CPTPP	No	No	No	No	Yes	Yes	Yes	Yes	Yes
TiSA (on hold)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
EC adopted the "Adequacy" decision	Yes	No	No	Yes	No	No	Yes	Yes	No
USMCA	No	No	Yes	No	No	Yes	No	Yes	No
CAFTA-DR	No	No	Yes	No	No	No	No	No	No
RCEP	No	Yes	No	Yes	Yes	No	Yes	No	Yes
Pacific Alliance	No	No	No	No	No	Yes	No	No	No
Osaka Track	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Depa	No	No	No	No	No	No	No	No	Yes
ASEAN: AE-Com and FPDP	No	Yes	No	No	No	No	No	No	Yes
COE: Convention 108+	No	No	No	No	No	Yes	No	No	No
OECD: Guidelines	**Yes**	No	Yes	Yes	Yes	Yes	Yes	Yes	No
RIDP	**No**	No	No	No	No	Yes	No	No	No
ELAC 2022, Goal 27.	**No**	No	Yes	Yes	No	Yes	Yes	Yes	No
OAS: privacy and data protection	**No**	No	Yes	No	No	Yes	No	Yes	No