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

CONTENTS

GLOBAL CROSS-BORDER PRIVACY RULES (CBPR) FRAMEWORK

Part I. Preamble

Recognising that growing Internet connectivity and the digitisation of the global economy have resulted in the rapid increase in the collection, use, and transfer of data across borders, a trend that continues to accelerate;

Conscious that trusted cross-border data flows are indispensable – not just for big, multinational technology companies, but for companies across all sectors of the economy, and for micro, small- and medium-sized businesses, workers, and consumers as well;

Believing that cross-border data flows increase living standards, create jobs, connect people in meaningful ways, facilitate vital research and development in support of public health, foster innovation and entrepreneurship, and allow for greater international engagement;

Acknowledging that regulatory barriers threaten to undermine opportunities created by the digital economy at a time when companies are relying increasingly on digital technologies and innovations to continue business operations and recover economically;

Recognising the importance of strong and effective data protection and privacy in strengthening consumer and business trust in digital transactions;

Acknowledging the important contribution made by the Asia-Pacific Economic Cooperation (APEC) in developing the APEC CBPR System to foster cross-border data flows and interoperability;

1. This Framework is based on the APEC Privacy Framework and is consistent with the core principles of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines).

2. The Framework specifically addresses the importance of protecting personal information and privacy while maintaining information flows. Its practical and distinctive approach is to focus attention on consistent rather than identical approaches to data protection and privacy. In so doing, it 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.

3. The Framework is intended to inform the interpretation of the Global Cross-Border Privacy Rules (CBPR) and Global Privacy Recognition for Processors (PRP) Systems program requirements that were developed based on the nine Global CBPR Privacy Principles.

4. Global CBPR Forum Members, acknowledging the Framework as an important tool in encouraging the development of appropriate data protection and privacy approaches and enabling trust in cross-border flows of personal data, should review

the Global CBPR and Global PRP Systems program requirements periodically so that the Global CBPR Forum can continue to effectively promote data protection practices which facilitate cross-border data flows globally.

Part II. Scope

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

CORE DEFINITIONS	COMMENTARY
6. **Personal information** means any information about an identified or identifiable individual.	6. The Framework is intended to apply to information about natural living persons, not legal persons. The Framework applies to personal information, which is information that can be used to identify an individual. It also includes information that would not meet this criterion alone, but when put together with other information would identify an individual. For example, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behavior, social relationships, private preferences and identity.
7. **Personal information controller** means a person or organization who controls the collection, holding, processing, use, disclosure or transfer of personal information. It includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization. It also excludes an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.	7. The Framework applies to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information. For the purposes of the Framework, where a person or organization instructs another person or organization to collect, hold, use, process, transfer or disclose personal information on its behalf, the instructing person or organization is the personal information controller and is responsible for ensuring compliance with the Global CBPR Privacy Principles. Individuals will often collect, hold and use personal information for personal, family or household purposes. For example, they often keep address books and phone lists or prepare family newsletters. The Framework is not intended to apply to such personal, family or household activities.

8. **Publicly available information** means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or that is legally obtained and accessed from:

   a) government records that are available to the public;

   b) journalistic reports; or

   c) information required by law to be made available to the public.

8. The Framework has limited application to publicly available information. Notice and choice requirements, in particular, often are superfluous where the information is already publicly available, and the personal information controller does not collect the information directly from the individual concerned. Publicly available information may be contained in government records that are available to the public, such as registers of people who are entitled to vote, or in news items broadcast or published by the news media.

ADDITIONAL DEFINITIONS

9. **Data Protection and Privacy Laws** means laws and regulations of a Member, the enforcement of which have the effect of protecting personal information consistent with the Global CBPR Framework.

9. Data Protection and Privacy Laws come in a variety of forms. Some are general privacy or data protection statutes while others take a sectoral approach covering particular areas such as credit reporting or health information. In some cases, the relevant legal provisions are contained within broader laws dealing with such issues as telecommunications or consumer protection. It is not important for the purposes of the definition what the laws are called: it is the effect of the laws that matters.

10. **Global CBPR System** is the abbreviation of the **Global** Cross-Border Privacy Rules System.

10. The Global CBPR System is a voluntary accountability-based scheme to facilitate data protection- and privacy-respecting personal information flows across jurisdictions. It has four main components:

- set criteria for bodies to become recognised as Global CBPR Forum Accountability Agents;

- a process for personal information controllers to be certified as Global

CBPR System-compliant by a recognized Accountability Agent;

- assessment criteria for use by recognised Accountability Agents when reviewing whether a controller meets Global CBPR System program requirements; and

- arrangements for enforcing Global CBPR System program requirements through complaints processes provided by recognised Accountability Agents backed up by a Privacy Enforcement Authority that is a participant in the Global Cooperation Arrangement for Privacy Enforcement ("Global CAPE").

11. **Global PRP System** is the abbreviation of the Global Privacy Recognition for Processors System.

11. The Global PRP System represents the baseline requirements a personal information processor must meet in order to be recognized by an approved Accountability Agent and provide assurances with respect to the processor's data protection and privacy policies and practices. The Global PRP System helps processors to demonstrate their ability to provide effective implementation of a personal information controller’s data protection and privacy obligations related to the processing of personal information.

12. **Privacy Enforcement Authority** means any public body that is responsible for enforcing Data Protection and Privacy Laws, and that has powers to conduct investigations and/or pursue enforcement proceedings.

12. 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.

13. Global CAPE is the abbreviation of the Global Cooperation Arrangement for Privacy Enforcement which is a practical multilateral mechanism which

13. The Global CAPE is a multilateral mechanism which enables Privacy Enforcement Authorities to cooperate in cross-border enforcement of Data Protection and Privacy Laws. Any Privacy

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.	Enforcement Authority may participate. The Global CAPE aims to: a) facilitate information sharing among participating Privacy Enforcement Authorities; b) provide mechanisms to promote effective cross-border cooperation between Privacy Enforcement Authorities in the enforcement of Data Protection and Privacy Laws; and c) encourage information sharing and cooperation on data protection and privacy investigation and enforcement with privacy enforcement authorities not participating in the Global CAPE.

APPLICATION

14. 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.	14. Although it is not essential for electronic commerce that all laws and practices be identical, compatible approaches to data protection and privacy among Members will greatly facilitate international commerce and privacy enforcement cooperation. Nonetheless, the Framework recognizes the need also to take into account social, cultural and other differences among Members.
15. Exceptions to the Global CBPR Privacy Principles, including those relating to national sovereignty, national security, public safety and public policy, should be: a) limited and proportional to meeting the objectives to which the exceptions relate; and b) (i) made known to the public; or	15. Members implementing the Framework at a domestic level may adopt suitable exceptions that suit their particular domestic circumstances. While recognizing the importance of governmental respect for data protection and privacy, the Framework is not intended to impede governmental actions authorized by law when taken to protect national security, public safety, national sovereignty or achieve other important public policy objectives. Nonetheless, Members should endeavor to ensure that

(ii) in accordance with law.	the impact of these activities upon the rights, responsibilities and legitimate interests of individuals and organizations is as limited as possible.

Part III. Global CBPR Privacy Principles

16. The Global CBPR Privacy Principles should be read as a whole rather than as individual principles as they are inter-related.[1]

PRINCIPLES	COMMENTARY
I. Preventing Harm	
17. Recognizing the interests of the individual to legitimate expectations of data protection and privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.	17. This Principle recognizes that one of the primary objectives of the Framework is to prevent misuse of personal information and consequent harm to individuals. Therefore, data protection and privacy approaches, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, organizational controls should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection, use or transfer of personal information. Where there has been a significant security breach affecting personal information, it may help to reduce the risk of harmful consequences to the individuals concerned to give notice to Privacy Enforcement Authorities and/or the individuals concerned.

[1] There may be some minor inconsistency in language usage between principles (e.g. in relation to how the principles describe the use of personal information). Unless, the context suggests otherwise, 'use' of personal information should be considered to include collection, holding, processing, use, disclosure or transfer of personal information.

II. Notice

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

    a) the fact that personal information is being collected;

    b) the purposes for which personal information is collected;

    c) the types of persons or organizations to whom personal information might be disclosed;

    d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information;

    e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

19. All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.

20. It may not be appropriate for personal information controllers to

18-20. This Principle is directed towards ensuring that individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organization.

Depending on the context in which the personal information is collected, notice may be provided using various methods. For example, one common method of compliance with this Principle is for personal information controllers to post notices on their websites. Where organizations engage individuals in offline settings, such as in person or via the telephone, posted or written notices or telephone scripts may be used. In other situations, placement of notices on intranet sites or in employee handbooks, for example, may be appropriate. There are practical challenges to giving notice in the mobile context. To provide notice on small screens, personal information controllers may want to consider the value of standard notices, icons, or other measures.

Organizations should inform relevant individuals at the time of, or before, information is collected about them. At the same time, the Principle also recognizes that there are circumstances in which it would not be practicable to give notice at or before the time of collection, such as in some cases where digital technology automatically collects information when a prospective customer initiates contact, as is often the case with the

provide notice regarding the collection and use of publicly available information.

use of cookies.

Moreover, where personal information is not obtained directly from the individual, but from a third party, it may not be practicable to give notice at or before the time of collection of the information. For example, when an insurance company collects employees' information from an employer in order to provide medical insurance services, it may not be practicable for the insurance company to give notice at or before the time of collection of the employees' personal information.

Additionally, there are situations in which it would not be necessary to provide notice, such as in the collection and use of publicly available information, or of business contact information and other professional information that identifies an individual in his or her professional capacity in a business context. For example, if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect to be given notice regarding the collection and normal use of that information for expected business purposes.

Further, if colleagues who work for the same company as an individual were to provide the individual's business contact information to potential customers of that company, the individual would not have an expectation that notice would be provided regarding the transfer or the expected use of that information.

III. Collection Limitation

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

21. This Principle limits collection of personal information by reference to the purposes for which it is collected. The collection of the personal information should be relevant to such purposes, and necessity and proportionality to the fulfillment of such purposes may be factors in determining what is relevant.

This Principle also provides that collection methods must be lawful and fair. For example, obtaining personal information under false pretenses (e.g., where an organization uses phishing, telemarketing calls, or pretexting emails to fraudulently misrepresent itself as another company in order to deceive consumers and induce them to disclose their credit card numbers, bank account information or other sensitive personal information) may in many Members be considered unlawful. Therefore, even in those Members where there is no explicit law against these specific methods of collection, they may be considered to be unfair means of collection.

The Principle also recognizes that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate. For example, in a situation where there is an outbreak of food poisoning, it would be appropriate for the relevant health authorities to collect the personal information of patrons from restaurants without providing notice to or obtaining the consent of individuals in order to inform them of the potential health risk.

IV. Uses of Personal Information

22. Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:

    a) with the consent of the individual whose personal information is collected;

    b) when necessary to provide a service or product requested by the individual; or,

    c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.

22. This Principle limits the use of personal information to fulfilling the purposes of collection and other compatible or related purposes. For the purposes of this Principle, "uses of personal information" includes the transfer or disclosure of personal information.

    Application of this Principle requires consideration of the nature of the personal information, the context of collection, the individual's expectations and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" would extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization.

V. Choice

23. Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be

23. The general purpose of the Choice Principle is to ensure that individuals are provided with choice in relation to collection, use transfer and disclosure of their personal information. Whether the choice is conveyed electronically, in writing or by other means, notice of such choice should be clearly worded

appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

and displayed clearly and conspicuously. The mechanisms for exercising choice should be accessible and affordable to individuals. Ease of access and convenience are factors that should be taken into account.

Where an organization provides information on available mechanisms for exercising choice, consideration should be given to tailoring the information and the way it is conveyed to make it more "easily understandable" to particular groups of individuals (e.g., by providing explanations in relevant languages, if the information is aimed at children, in ways that are age- appropriate).

This Principle also recognizes, through the introductory words "where appropriate", that there are certain situations where it would not be necessary to provide a mechanism to exercise choice.

In many situations it would not be necessary or practicable to provide a mechanism to exercise choice when collecting publicly available information. For example, it would not be necessary to provide a mechanism to exercise choice to individuals when collecting their name and address from a public record or a newspaper.

In specific and limited circumstances, it would not be necessary or practicable to provide a mechanism to exercise choice when collecting, using, transferring or disclosing other types of information. For example, when business contact information or other professional information that identifies an individual in his or her professional capacity is being exchanged in a

business context, it is generally impractical or unnecessary to provide a mechanism to exercise choice, as individuals in these circumstances would expect that their information be used in this way.

Further, in certain situations, it would not be practicable for employers to provide a mechanism to exercise choice related to the use of the personal information of their employees when using such information for employment purposes. For example, if an organization has decided to centralize human resources information, that organization should not be required to provide a mechanism to exercise choice to its employees before engaging in such an activity.

VI. Integrity of Personal Information

24. Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

24. This Principle recognizes that a personal information controller is obliged to maintain the accuracy and completeness of records and keep them up to date as necessary to fulfill the purposes of use. Making decisions about individuals based on inaccurate, incomplete or outdated information may not be in the interests of individuals or organizations.

VII. Security Safeguards

25. Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of

25. This Principle recognizes that individuals whose personal information is entrusted to others are entitled to expect that their information be protected with reasonable security safeguards.

information, or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

VIII. Access and Correction

26. Individuals should be able to:

    a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

    b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;

        (i) within a reasonable time;
        (ii) at a charge, if any, that is not excessive;
        (iii) in a reasonable manner;
        (iv) in a form that is generally understandable; and,

    c) challenge the accuracy of personal information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

27. Such access and opportunity for correction should be provided except where:

26-28. The ability to access and correct personal information, while generally regarded as a central aspect of data protection and privacy, is not an absolute right. This Principle includes specific conditions for what would be considered reasonable in the provision of access, including conditions related to timing, fees, and the manner and form in which access would be provided. What is to be considered reasonable in each of these areas will vary from one situation to another depending on circumstances, such as the nature of the information processing activity. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access.

Access must be provided in a reasonable manner and form. A reasonable manner should include the normal methods of interaction between organizations and individuals. For example, if a computer was involved in the transaction or request, and the individual's email address is available, email would be considered "a reasonable manner" to provide information. Organizations that have

a) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's personal information and privacy in the case in question;

b) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or

c) the personal information and privacy of persons other than the individual would be violated.

28. If a request under 25(a) or 25(b) or a challenge under 25(c) is denied, the individual should be provided with reasons why and be able to challenge such denial.

transacted with an individual may reasonably be expected to answer requests in a form that is similar to what has been used in prior exchanges with said individual or in the form that is used and available within the organization, but should not be understood to require separate language translation or conversion of code into text.

Both the copy of personal information supplied by an organization in response to an access request and any explanation of codes used by the organization should be readily comprehensible. This obligation does not extend to the conversion of computer language (e.g., machine-readable instructions, source codes or object codes) into text. However, where a code represents a particular meaning, the personal information controller must explain the meaning of that code to the individual. For example, if the personal information held by the organization includes the age range of the individual, and that is represented by a particular code (e.g., "1" means 18-25 years old, "2" means "26-35 years old, etc.), then when providing the individual with such a code, the organization shall explain to the individual what age range that code represents.

Where an individual requests access to his or her information, that information should be provided in the language in which it is currently held. Where information is held in a language different from the language of original collection, and if the individual requests the information be provided in that original language, an organization should supply the

information in the original language if the individual pays the cost of translation.

The details of the procedures by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.

Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other information subject to an access request, the organization should redact the protected information and make available the other information. However, in some situations, it may be necessary for organizations to deny claims for access and correction, and this Principle sets out the conditions that must be met in order for such denials to be considered acceptable, which include: situations where claims would constitute an unreasonable expense or burden on the personal information controller, such as when claims for access are repetitious or vexatious by nature; cases where providing the information would constitute a violation of laws or would compromise security; or, incidences where it would be necessary in order to protect commercial confidential information that an organization has taken steps to protect from disclosure, where disclosure would benefit a competitor in the marketplace, such as a particular computer or modeling

program.

"Confidential commercial information" is information that an organization has taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against the business interest of the organization causing significant financial loss. The particular computer program or business process an organization uses, such as a modeling program, or the details of that program or business process may be confidential commercial information. Where confidential commercial information can be readily separated from other information subject to an access request, the organization should redact the confidential commercial information and make available the non-confidential information, to the extent that such information constitutes personal information of the individual concerned. Organizations may deny or limit access to the extent that it is not practicable to separate the personal information from the confidential commercial information and where granting access would reveal the organization's own confidential commercial information as defined above, or where it would reveal the confidential commercial information of another organization that is subject to an obligation of confidentiality.

When an organization denies a request for access, for the reasons specified above, such an organization should provide the individual with an explanation as to why it has made that determination and information on how to challenge that denial. An

organization would not be expected to provide an explanation in cases where such explanation would violate a law or judicial order.

IX. Accountability

29. A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

29. Efficient and cost-effective business models often require information transfers between different types of organizations in different locations with varying relationships. When transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, personal information controllers should take reasonable steps to ensure the information is protected in accordance with these Principles, after it is transferred.

There are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed. In these types of circumstances, personal information controllers may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations.

A useful means for a personal information controller to help ensure accountability for the personal

information it holds is to have in place a data protection and privacy management programme.[2]

Part. IV. Implementation

30. Part IV provides guidance to Members on implementing the Global CBPR Framework. Section A focuses on measures that Members should consider in implementing the Framework domestically, while Section B sets out Forum-wide arrangements for the implementation of the Framework's cross-border elements.

A. GUIDANCE FOR DOMESTIC IMPLEMENTATION

31. Members should have regard to the following basic concept in considering the adoption of measures designed for domestic implementation of the Global CBPR Framework:

I. Maximizing Benefits of Data Protection and Privacy and Information Flows

32. Personal information should be collected, held, processed, used, transferred, and disclosed in a manner that (a) protects individuals' data and privacy, and (b) allows individuals and Members to maximize the benefits of data flows within and across borders.

33. Consequently, as part of establishing or reviewing their data protection and privacy approaches to give effect to the Global CBPR Framework, Members should take all reasonable and appropriate steps to identify and remove unnecessary barriers to information flows and avoid the creation of any such barriers.

II. Giving Effect to the Global CBPR Framework

34. There are several options for giving effect to the Framework and securing data protection and privacy for individuals, including legislative, administrative, industry self-regulatory or a combination of these policy instruments. In practice, the Framework is meant to be implemented in a flexible manner that can accommodate various models of enforcement, including through Privacy Enforcement Authorities, multi-agency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as Members deem appropriate.

35. The means of giving effect to the Framework will often differ between Members. A Member may determine that different Global CBPR Privacy Principles call for different means of domestic implementation. Whatever approach is adopted in a particular circumstance, the overall goal should be to develop compatible data protection and

[2] See paras 40-42 below.

privacy approaches among Members that are respectful of individual Members' requirements.

36. Members should adopt non-discriminatory practices in giving effect to the Framework's principles and in protecting individuals from data protection and privacy violations occurring in that Member's jurisdiction. For example, Members should ensure that laws or other approaches that give effect to the protections in the Framework do not impede individuals living in other jurisdictions from benefitting from those protections.

37. Coordination across government agencies and other stakeholders is important to identify ways to strengthen data protection and privacy without creating obstacles to national security, public safety, and other public policy objectives.

38. Members should maintain Privacy Enforcement Authorities. These Privacy Enforcement Authorities should be provided with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions in an objective, impartial and consistent basis.

39. Privacy Enforcement Authorities may find it useful to apply a risk-based approach to selected oversight efforts and, where permitted, to prioritize their enforcement efforts according to the likelihood and severity of harm that might result from data protection and privacy violations or from an action taken or proposed.[3]

III. Data Protection and Privacy Management Programmes

40. An operative data protection and privacy management programme will provide a sound basis for a personal information controller to demonstrate that it is complying with measures that give effect to the Global CBPR Privacy Principles.

41. Accordingly, Members should consider encouraging personal information controllers to develop and implement data protection and privacy management programmes for all personal information under their control. Data protection and privacy management programmes 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;

[3] See the Preventing Harm Principle.

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

e) be monitored and be regularly updated.

42. Personal information controllers should be prepared to demonstrate their data protection and privacy management programmes at the request of a competent Privacy Enforcement Authority of that Member or in response to a valid request by another appropriate entity, such as an Accountability Agent designated under the Global CBPR Forum or under an industry code of conduct giving effect to the Framework.

IV. Promotion of technical measures to protect personal information and privacy

43. Technical measures can make a significant contribution to the overall effectiveness and impact of domestic data protection and privacy regimes, by supplementing and complementing legal protections of personal information and privacy. Therefore, when considering approaches to give effect to the Framework, Members should promote technical measures which help to protect personal information and privacy.

44. Members may, for example, encourage personal information controllers to make full use of readily available technical safeguards and measures. In addition, they may promote research and development, encourage further data protection and privacy innovation and support the development of technical standards that embed best data protection and privacy practice into systems engineering.

V. Public education and communication

45. For the Framework to be of practical effect, it should be known and accessible. Accordingly, Members should:

a) Publicize how their Data Protection and Privacy Laws and other domestic arrangements provide protections to individuals;

b) engage in activities that raise awareness amongst:

i. personal information controllers about the Member's Data Protection and Privacy Laws and the controllers' responsibilities;

ii. Personal information processors about practices that help provide effective implementation of a personal information controller's data protection and privacy obligations related to the processing of personal information; and

iii. individuals about how they can report violations and how remedies can be pursued; and

c) Encourage or require Privacy Enforcement Authorities and other bodies having responsibilities to administer Data Protection and Privacy Laws established at the domestic level (for example, Global CBPR Forum-recognized Accountability Agents or bodies established to give effect to self-regulatory schemes) to report publicly on their activities where appropriate.

VI. Cooperation within and between the Public and Private Sectors

46. Active participation of non-governmental entities will help ensure that the full benefits of the Framework can be realized. Accordingly, Members should engage in a dialogue with relevant non-government stakeholders, including those representing citizens, consumers and industry and technical and academic communities, to obtain input on data protection and privacy and information flow issues and to seek cooperation in furthering the Framework's objectives.

47. Members should seek the cooperation of non-governmental entities such as those representing citizens and consumers in raising public awareness about data protection and privacy issues. As well, Members should encourage these entities to actively engage in promoting and supporting the personal information and privacy interests of individuals, for example by referring complaints to Privacy Enforcement Authorities and publicizing the outcomes of those complaints.

48. Members should consider developing strategies that reflect a coordinated approach to data protection and privacy across governmental bodies.

49. Members should also consider undertaking consultation and capacity building efforts across the public and private sectors, and with non-government stakeholders, including, for example, by:

    a) developing or supporting networks of individuals responsible for data protection and privacy compliance within organizations; and

    b) producing informational materials and arranging experience sharing events.

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

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

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

pursue legal action, industry self-regulation, or a combination of systems); and

b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.

51. A Member should consider encouraging or requiring personal information controllers to provide notice, as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach affecting personal information under its control. Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable.

VIII. Reporting Domestic Implementation of the Global CBPR Framework

52. Members should provide timely notice to the Global Forum Assembly on their domestic implementation of the Framework, including any new laws or regulations and any amendments to existing laws or regulations, as well as all other developments that may affect the operation and enforcement of the Global CBPR System and/or Global PRP System.

B. GUIDANCE FOR INTERNATIONAL IMPLEMENTATION

53. In addressing the international implementation of the Global CBPR Framework, and consistent with the provisions of Part A, Members should consider the following points relating to the protection of the privacy of personal information:

I. Information sharing among Members

54. Members are encouraged to share and exchange information, surveys and research in respect of matters that have a significant impact on data protection and privacy.

55. Members are encouraged to educate one another in issues related to data protection and privacy and to share and exchange information on promotional, educational and training programs for the purpose of raising public awareness and enhancing understanding of the importance of data protection and privacy and compliance with relevant laws and regulations.

56. Members are encouraged to share experiences on various techniques in investigating violations of data protection and privacy and regulatory strategies in resolving disputes involving such violations including, for instance, complaints handling and alternative dispute resolution mechanisms.

57. Members should designate and make known to the other members the public authorities within their own jurisdictions that will be responsible for facilitating cross-border cooperation and information sharing between members in connection with data protection and privacy.

58. Members should encourage the development of internationally comparable metrics to inform the policy making process relating to data protection and privacy and personal information flows.

II. Cross-border cooperation in investigation and enforcement

59. Taking into consideration existing international arrangements (including the Global CAPE) and existing or developing self-regulatory or co-regulatory approaches, and to the extent permitted by domestic law and policy, members should expand their use of existing cooperative arrangements and consider developing additional cooperative arrangements or procedures, as necessary, to facilitate cross-border cooperation in the enforcement of Data Protection and Privacy Laws. Such cooperative arrangements may take the form of bilateral or multilateral arrangements.

60. The preceding paragraph is to be construed with regard to the right of Members to decline or limit cooperation on particular investigations or matters on the ground that compliance with a request for cooperation would be inconsistent with domestic laws, policies or priorities, or on the ground of resource constraints, or based on the absence of a mutual interest in the investigations in question.

61. In civil enforcement of Data Protection and Privacy Laws, cooperative cross-border arrangements may include the following aspects:

    a) mechanisms for promptly, systematically and efficiently notifying designated public authorities in other Members of investigations or data protection and privacy enforcement matters that target conduct that is (i) inconsistent with the protections set forth in the Framework and (ii) may affect individuals or personal information controllers in those other Members;

    b) mechanisms for effectively sharing information necessary for successful cooperation in cross-border data protection and privacy investigation and enforcement cases;

    c) mechanisms for investigative assistance in data protection and privacy enforcement cases;

    d) mechanisms to prioritize cases for cooperation with public authorities in other Members based on the severity of the unlawful infringements of personal information and privacy, the actual or potential harm involved, as well as other relevant considerations; and

    e) steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.

III. Cross-border data protection and privacy mechanisms

62. Members recognize the importance of protecting personal information and privacy while maintaining the free flow of personal information across borders and encourage the implementation the Framework to provide conditions in which information can flow safely and accountably, for instance through the use of the Global CBPR and PRP Systems.

63. Members should endeavor to support the development and recognition or acceptance of cross-border data transfer and privacy mechanisms for use by organizations to transfer personal information globally, recognizing that organizations would still be responsible for complying with the local data protection and privacy requirements, as well as with all applicable laws. Such mechanisms should be consistent with the Global CBPR Privacy Principles.

64. To give effect to paragraph 62, Members participate in the Global CBPR System, which provides a practical mechanism to implement the Global CBPR Framework in an international, cross-border context, and to provide a means for organizations to transfer personal information across borders in a manner in which individuals may trust that the privacy of their personal information is protected.

65. The Global PRP System complements the Global CBPR System to help personal information processors demonstrate their ability to provide effective implementation of a personal information controller's obligations related to the processing of personal information.

IV. Cross-border transfers

66. A Member should refrain[4] from restricting cross border flows of personal information between itself and another Member where (a) the other Member has in place legislative or regulatory instruments that give effect to the Framework or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the Global CBPR System) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it.

67. 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.

V. Interoperability with data protection and privacy frameworks

68. Members should promote interoperability of the Global CBPR System and PRP System with other data protection and privacy frameworks that give practical effect to this

[4] Cross border data flows remain subject to members' applicable domestic laws, regulations, and international agreements and commitments.

Framework.

69. Improving the global interoperability of data protection and privacy frameworks can bring benefits in improved personal information flows, help ensure that data protection and privacy requirements are maintained when personal information flows beyond Members and can simplify compliance for personal information controllers and processors. Global interoperability can also assist individuals to assert their personal information and privacy rights in a global environment and help authorities to improve cross-border privacy enforcement.