Bermuda Report on Information Accountability: Prepared by the Information Accountability Foundation for the Office of the Privacy Commissioner for Bermuda

Lynn Goldstein, principal author

28 March 2020

Introduction

Personal data must be used in liberal democracies such as Bermuda to fuel all facets of human life but must be used in a manner that is respectful of all three vital interests related to data protection. Those three interests are: (1) individual autonomy so individuals may frame their identities and how they are framed by their data tracks; (2) seclusion from public view where appropriate; and (3) fair processing of data so it is used in a manner that creates value for individuals, groups of individuals, society and private interests and so harms to individuals are avoided to the extent possible and/or practical. The Bermuda Parliament had these rights and interests in mind when it adopted the Personal Information Protection Act 2016 (PIPA) and recognized that PIPA was critical for Bermuda's advancement and recognition as a democratic and just society and for the protection of Bermuda's economic interests, especially in the digital age.[1]

PIPA applies to every organisation that uses personal information in Bermuda where that personal information is used for basic uses (e.g. fulfilling a purchase using a credit card) and also for more advanced data processing (e.g. using artificial intelligence, facial recognition technology and/or automated decisions that could impact an individual).

Although PIPA does not have an express accountability principle, it does, in Section 5, Responsibility and Compliance,[2] set forth some of the elements of the accountability principle found in the Canadian privacy Law, Personal Information Protection and Electronic Documents Act (PIPEDA)[3] and of a privacy management programme which has been set forth in guidance by regulators in Canada and followed by regulators in Hong Kong, Colombia and Australia. This guidance was issued by these regulators so they could advise organisations on what it means to be an accountable organization. So, by setting forth in Section 5 some elements of the accountability principle and of a privacy management programme and by requiring organisations to act in a reasonable manner in meeting these requirements, PIPA does, in essence, have an accountability requirement and does require every organization that uses personal information for basic and advanced data processing to be an accountable organization.

[1] Ministerial Statement by the Minister of Economic Development, 1 July 2016, https://www.gov.bm/articles/personal-information-protection-bill-2016

[2] PIPA § 5

[3] S.C. 2000, c. 5

This Report reviews the privacy frameworks and laws and regulations that contain an accountability principle and the guidance from privacy regulators on what it means to be an accountable organization. The Report then discusses how the elements of accountability should be enhanced to accommodate the changes brought about by advanced data processing which often is conducted without some of the human accountability expected by the guidance issued by the privacy regulators and expected by PIPA. Finally, the Report provides direction on what the Office of the Privacy Commissioner for Bermuda could cover in guidance regarding a privacy management programme that includes advanced data processing.

Accountability as a Privacy and Data Protection Principle

Frameworks

The roots of the accountability principle can be found in one of the oldest international frameworks for data protection, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980.[4] According to the OECD accountability principle, the party who decides about the contents and use of personal data, the data controller, should be accountable for complying with measures which give effect to the other privacy principles in the OECD Guidelines: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, and individual participation.[5] The Explanatory Memorandum to the OECD Guidelines, whose purpose was to explain and elaborate on the OECD Guidelines, expanded upon the accountability principle as follows:

> The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevent service bureaux personnel, "dependent users," . . . and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information . . . . Accountability . . . refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.[6]

---

[4] Organisation for Economic Co-operation and Development, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [hereinafter OECD Guidelines]; C. Raab, The Meaning of 'Accountability' in the Information Privacy Context, at 2, https://fpf.org/wp-content/uploads/The-Meaning-of-'Accountability'-in-the-Information-Privacy-Context-Charles-Raab.pdf [hereinafter Raab]

[5] OECD Guidelines ¶ 14. The OECD Guidelines were revised in 2013, but the text of the accountability principle remained unchanged. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[6] OECD Guidelines ¶ 62

Thus, the term "accountable" is used to mean both responsibility and liability, and it is likely that it is this meaning that policymakers and regulators have in mind when they use the term "accountability."[7]

The concept of accountability next was addressed in 2005 in the APEC Privacy Framework. Principle IX of the APEC Privacy Framework provides that a "personal information controller should be accountable for complying with measures that give effect to" the other APEC privacy principles: preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, and access and correction.[8]

The OECD Privacy Framework was updated in 2013. In that Framework, the accountability principle remained the same, but a section on implementing accountability was added. That section provides that a data controller should have in place a privacy management programme that gives effect to the Guidelines for all personal data under its control; is tailored to the structure, scale, volume and sensitivity of its operations; provides for appropriate safeguards based on privacy risk assessment; is integrated into its governance structure and establishes internal oversight mechanisms; includes plans for responding to inquiries and incidents; and is updated in light of ongoing monitoring and periodic assessment. It also requires a data controller to be prepared to demonstrate its privacy management programme as appropriate to privacy enforcement authorities or entities responsible for promoting adherence to a code of conduct and to provide notice, as appropriate, to privacy enforcement or other relevant authorities when there has been a significant security breach affecting personal data and, where the breach is likely to adversely affect individuals, to affected individuals.[9]

Neither the OECD Guidelines nor the APEC Privacy Framework are binding on organisations. However, they do influence the development of global privacy laws and guidance from regulators.

Laws and Regulations

In 2000 Canada adopted PIPEDA. Schedule 1 of PIPEDA contains the accountability principle which provides that the "organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with" the following principles: identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance. The clauses to PIPEDA's accountability principle begin to define what it means for an organization to be accountable and how to be an accountable organization. The

[7] Raab at 2-3

[8] http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf The remainder of Principle IX and all of the commentary to Principle IX concern accountability when personal information is transferred both domestically and internationally. The APEC Privacy Framework was revised in 2015, but the text of, and the commentary to, the accountability principle remained unchanged. https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[9] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

first and second clauses provide that responsibility for accountability rests with designated individual(s) within the organization, but other individuals within the organization may be responsible for day-to-day processing of personal information or may be delegated to act on behalf of the designated individual(s) and that the identity of the designated individual(s) must be made known upon request. The third clause provides that the organization is responsible for personal information in its possession or custody, including information transferred to it for processing, and that contractual or other means must be used to provide a comparable level of protection for information being processed by a third party. The establishment and implementation of policies and practices is required by the fourth clause, including procedures to protect personal information and to receive and respond to complaints and inquiries, training of staff on the policies and practices, and developing of information to explain policies and procedures.[10]

In 2010 Mexico enacted the Federal Law on Protection of Personal Data Held by Private Parties (FDPL). The FDPL provides that data controllers must adhere to principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the law.[11]

In 2016 the EU adopted the General Data Protection Regulation (GDPR). The 2010 European Union Article 29 Data Protection Working Party Opinion on the principle of accountability (Accountability Opinion) advised the European Commission on how to amend the EU Data Protection Directive to add an accountability principle. The Accountability Opinion recommends a statutory requirement binding upon all data controllers consisting of two main elements: (1) appropriate and effective measures to implement data protection principles, and (2) demonstration upon request that appropriate and effective measures have been taken.[12] That is exactly how accountability was drafted into the GDPR. Article 5(2) of the GDPR provides that the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to the processing of personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality. Articles 24 and 25 of the GDPR require controllers to: (1) implement appropriate technical and organisational measures which are designed to implement the data protection principles and to integrate necessary safeguards into the processing, and (2) demonstrate that implementation through implementation of appropriate data protection policies and adherence to approved codes of conduct or approved certification mechanisms.[13]

[10] PIPEDA Schedule 1, 4.1.1 – 4.1.4

[11] https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf

[12] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

[13] The Accountability Opinion also gave examples of accountability mechanisms, and those accountability mechanisms were enacted into the GDPR:

Accountability Opinion	GDPR
Implementation of privacy impact assessments for higher risk processing operations	Articles 35 and 36
Appointment of data protection officer	Articles 37, 38 and 39
Advancement of adequate safeguards for the transfer of personal data such as Binding Corporate Rules	Article 47
Implementation of security policy	Article 32

In 2018 Brazil approved the General Data Protection Law (LGPD). Some provisions already have been amended, including the postponement of its enforceability to August 2020. The LGPD contains ten principles that should be taken into account in the processing of personal data: purpose limitation, suitability, necessity, free access, quality of the data, transparency, security, prevention, nondiscrimination, and a new principle of accountability. Under the LGPD, accountability makes it mandatory for the data controller and data processor to fully and transparently demonstrate the adoption of effective measures capable of proving compliance with the rules for data protection. These measures include data protection assessments and methodologies provided for by law.[14]

Regulatory Guidance

In 2012 the Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia worked together to develop Getting Accountability Right with a Privacy Management Program (Canadian Privacy Management Program).[15] In 2014 the Office of the Privacy Commissioner of Personal Data, Hong Kong, issued Getting Accountability Right with a Privacy Management Programme, A Best Practice Guide,[16] and in 2015 the Colombian Superintendence of industry and Commerce issued the Guide for the Implementation of the Principle of Demonstrated Responsibility (Accountability)[17] and the Office of the Australian Information Commissioner issued the Privacy Management Framework: enabling compliance and encouraging good practice.[18]

All of these four documents are very similar. According to the Canadian Privacy Management Program, an accountable organization must have in place appropriate policies and procedures that promote good practices, and these policies and procedures, taken as a whole, constitute a privacy management program. The four documents provide guidance on what it means to be an accountable organization and on what each of these regulators expect to see in a privacy management program. These documents describe the fundamentals of a comprehensive privacy management program (organizational commitment which includes the appointment of a Privacy Officer and the establishment of a Privacy Office and program controls which include internal policies, risk assessment tools and service provider management) and how to maintain

Implementation of procedures to prevent and detect breaches and response plan	Articles 33 and 34
Adoption of codes of practice	Articles 40 and 41
Development of certification programs or seals	Articles 42 and 43

[14] Renato Leite Monteiro, The New Brazilian General Data Protection Law, https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/; DLA Piper Data Protection Laws of the World, https://www.dlapiperdataprotection.com/?t=law&c=BR

[15] https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf

[16] https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf. The Best Practice Guide was reissued in 2018. https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf

[17] https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

[18] https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/

and improve a privacy management program on an ongoing basis (development of an oversight and review plan and assessment and revision of program controls). The result should be employees, customers, partners, and service providers who are aware of and understand the privacy management program, and organizations who are able to demonstrate to Privacy Commissioners that they have an effective privacy management program in place.

Revision of the Accountability Principle for Advanced Data Processing

In 2009 the Global Accountability Dialogue first met in Dublin to explore how the accountability principle might be used to create confidence in data transfers from one country to another. The group, comprised of diverse stakeholders, reached a consensus on the essential elements to guide organization accountability (Essential Elements of Accountability):

1. Organisational commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies into effect, including tools, training and education.
3. Systems for internal ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanisms for individual participation.
5. Means for remediation and external enforcement.[19]

During the Global Accountability Dialogue's second year, as discussed above, the Accountability Opinion took the accountability concept beyond data transfers to an overarching governance structure for implementing data protection within an organization. In the years that followed, 2012-2015, as discussed above, regulators in Canada, Hong Kong, Colombia and Australia adopted accountability guidance based upon the Essential Elements of Accountability, and in 2016, as discussed above, accountability is the foundation of the GDPR. The guidance and the adoption of the GDPR elevated accountability from check-box compliance to a risk-based approach but did not keep up with advanced data processing, such as artificial intelligence (AI) and machine learning (ML), that may impact individuals in a significant manner. So, in 2019, the Information Accountability Foundation released enhanced data stewardship accountability elements.[20]

In order to be able to transform data into information and information into knowledge and insight and knowledge into competitive advantage, and in order for individuals to be able to trust advanced data processing that might not be within their expectations, the Essential Elements of Accountability were revised to update the concept of data stewardship. The Galway Paper that described the 2009 Essential Elements of Accountability described stewardship in the following manner:

---

[19] https://informationaccountability.org; Data Protection Accountability: The Essential Elements [hereinafter The Galway Paper], https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf

[20] https://b8e.99c.myftpupload.com/wp-content/uploads/Data-Stewardship-Elements-002.pdf

> Accountability is the obligation to act as a responsible steward of the personal information of others, to take responsibility for the protection and appropriate use of that information beyond mere legal requirements, and to be accountable for any misuse of that information.

This 2009 description of a data steward was a clear statement that data users must take responsibility for the information they use. It was data use focused and gave a sense of governance in a period where advance data processing was beginning to disrupt consent and the actual application of data to problem solving. However, the focus was still on personal information. Data stewards were still custodians for that data to make sure the obligations associated with it were recognized as new insights were created.

Advanced data processing requires data stewardship be taken to a new level. The systems themselves, based on human set objectives, make decisions that impact individuals. While humans set the objectives, the direct human accountability for the decisions made has been lost. To regain that accountability, it is necessary that people be depended on to build accountability into the objectives for the systems through accountable governance. Therefore, it is necessary that stewards make decisions that consider the interests of external stakeholders, the parties impacted by the processing. As the role of the data steward has changed, the data steward has moved beyond being a mere custodian of the data and of the obligations that come with the data to being a data steward that makes sure that outcomes are legal, fair and just to the various stakeholders. Future data stewards must be stakeholder interests focused. As organisations move up the technology curve, and by extension use more data that can impact individuals, they must move up the responsibility curve as well. That increased responsibility resulted in the Enhanced Data Stewardship Accountability Elements which are the Essential Elements of Accountability updated to take into account the concept of enhanced data stewardship.[21]

[21] Artificial Intelligence, Ethics and Enhanced Data Stewardship, September 20, 2017, at 6-7, https://b8e.99c.myftpupload.com/wp-content/uploads/Artificial-Intelligence-Ethics-and-Enhanced-Data-Stewardship.pdf

The table below compares the 2009 Essential Elements and the 2019 Enhanced Data Stewardship Accountability Elements

Essential Elements of Accountability	**Enhanced Data Stewardship Accountability Elements**
Essential Element #1 Organisation commitment to accountability and adoption of internal policies consistent with external criteria. An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices. An organisation must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies, and monitor those mechanisms. Those policies and the plans to put them into effect must be approved at the highest level of the organisation, and performance against those plans at all levels of the organisation must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organisation priorities. An organisational structure must demonstrate this commitment by tasking appropriate staff with implementing the policies and overseeing those activities. Many global organisations have established policies in accordance with accepted external criteria such as the EU Directive, OECD Guidelines or APEC Principles. These companies demonstrate high-level commitment to those policies and the internal practices that implement them by requiring their review and endorsement by members of the organisation's executive committee or board of directors.	Enhanced Element #1 As a matter of organizational commitment, organizations should define data-stewardship values that are condensed to guiding principles and then are translated into organizational policies and processes for ethical data processing. a) These values and principles should be organizationally derived and should not be restatements of law or regulation. They may go beyond what the law requires, but at a minimum, they should be aligned, and not be inconsistent, with existing laws, regulations, or formal codes of conduct.[22] Organizations should be open about their values and principles. b) Organizational policies and processes derived from these values should be anchored to clearly defined, accountable individuals within the organization and should be overseen by designated senior executives. c) The organization's data stewardship guiding[23] principles should be easily understood by all staff, and in particular by technical staff, and should be capable of being programmed into activity objectives.

[22] Examples of existing professional or industry codes of conduct are those that relate to AI or ML. These Elements should work with those codes and not replace them.

[23] See IAF Blog: The Need for an Ethical Framework, https://informationaccountability.org/the-need-for-an-ethical-framework/ .

Essential Element #2	Enhanced Element #2
Mechanisms to put privacy policies into effect, including tools, training and education. The organisation must establish performance mechanisms to implement the stated privacy policies. The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information. The tools and training must be mandatory for those key individuals involved in the collection and deployment of personal information. Accountable organisations must build privacy into all business processes that collect, use or manage personal information. Organisations in Europe, North America and Asia-Pacific have implemented comprehensive privacy programmes that incorporate personnel training, privacy impact assessments and oversight. In some cases, organisations have automated processes and integrated responsibility for programme obligations into all levels and across all aspects of the enterprise, while responsibility for compliance, policy development and oversight remain in the privacy office.	Organizations should use an "ethics by design" process to translate their data-stewardship values into their data-analytics and data-use system design processes so that society, groups of individuals, or individuals themselves, and not just the organizations, gain value from the data processing activities, such as AI or ML. a) Advanced data-processing activities, such as AI and ML, that affect individuals should have beneficial impacts accruing to individuals and communities of individuals, particularly those to whom the underlying data pertains. b) Where an analytical data driven use has potential impact at the individual level, or at a higher level, such as groups of individuals and society, the risks and benefits should be explicitly defined. The risks should be necessary and proportional to the benefits and should be mitigated to the extent possible. c) The systems, and the data that feeds those systems, should be assessed for appropriateness based on the decision the data is being used for and should be protected proportional to the risks. d) Where appropriate, organizations should follow codes of conduct that standardize processes to industry norms. e) Ethical Data Impact Assessments (EDIAs)[24] should be required when advanced-data analytics may impact people in a significant manner and/or when data- enabled decisions are being made without the intervention of people. (1) An EDIA is a process that looks at the full range of benefits, risks, rights, obligations, and interests of all individuals, groups of individuals, society and other data stakeholders, such as regulators. (2) An EDIA is a means of determining whether an instance of processing is in accordance with the data stewardship values and guiding principles established by the

[24] See here for A Model EDIA

	organization. Processing includes all steps necessary to achieve an outcome, from the collection of data through the implementation of data-driven outcomes. (3) Organizations should have EDIAs that achieve an "ethics by design" process that is integrated into systems development. All staff involved in data impacting processing should receive training so that they may competently participate in an "ethics by design" process.
<u>Essential Element #3</u> Systems for internal ongoing oversight and assurance reviews and external verification. Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its transmission across borders, to its destruction when it is no longer useful – and must be subject to some form of monitoring. The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to the outside vendors and independent third parties. The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its	<u>Enhanced Element #3</u> There should be an internal review process that assesses whether EDIAs have been conducted with integrity and competency, if the issues raised as part of the EDIA have been resolved, and if the advanced data processing activities are conducted as planned. [25] a) Where data processes begin with analytic insights, those insights should be tested for accuracy, predictability, and consistency with organizational values. b) Intensive data impacting systems should be reviewed so that outcomes are as intended with the objectives of the activity, risks are mitigated as planned, harms are reduced, and unintended consequences are understood. c) Where internal reviewers need external expertise, that expertise should be sought. d) The review of the EDIA process is separate and independent from the EDIA process.

[25] See here for A Model Oversight Assessment

internal audit department to perform this function so long as the auditor's report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution. External verification must be both trustworthy and affordable. Privacy officers may work with their audit departments to ensure that internal audits are among the tools available to oversee the organisation's data management. Organisations may also engage firms to conduct formal external audits. Seal programmes in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.	
<u>Essential Element #4</u> Transparency and mechanisms for individual participation. To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms. When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also provides for those instances when it is feasible. In such cases it should be made available to the	<u>Enhanced Element #4</u> Processes should be transparent and, when possible, should enhance societal, groups of individual or individual interests. The data-stewardship values that govern the advanced data-processing activities, such as AI or ML systems developed, and that underpin decisions, should be communicated widely. Furthermore, all societal and individual concerns should be addressed and documented as part of the EDIA process. a) Organizations should be able to explain how data is used, how the use may benefit and potentially pose risks to society, groups of individuals, or individuals themselves are associated with the processing, and how society, groups of individuals and individuals themselves may participate and object. b) Individual accountability systems that provide appropriate opportunities for feedback, relevant explanations, and appeal options for impacted individuals should be designed and be effective, and effectiveness should be tested.

consumer and should form the basis for the organisation's decisions about data use. Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.	c) Organizations should be open about how analytical data use and advanced data processing activities, such as AI or ML systems, have been developed. Individual and societal concerns should be part of the data system evaluation lifecycle.
<u>Essential Element #5</u> Means for remediation and external enforcement. The organisation should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of resolution and establish a process by which those complaints are reviewed and addressed. The accountable organization may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organization and enhance its reputation for complying with its policies and meeting its obligations to individuals. Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organization should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organization recognize and respond to the legal authority exercising proper jurisdiction.	<u>Enhanced Element #5</u> Organizations should stand ready to demonstrate the soundness of internal processes to the regulatory agencies that have authority over advanced data-processing activities, such as AI or ML processes, as well as certifying bodies to which they are subject, when data processing is or may impact people in a significant manner. a) Organizations should be open about core values in regulator-facing disclosures. b) Organizations should stand ready to demonstrate the soundness of the policies and processes they use and how data and data-use systems are consistent with their data stewardship values and guiding principles. Depending on how data is used and what type of data is used, soundness of internal processes may be demonstrated by privacy impact assessments (PIAs), data protection impact assessments (DPIAs) or EDIAs.

Privacy Management Program for Advanced Data Processing

As discussed above, the 2009 Essential Elements of Accountability were the basis for the regulatory guidance issued between 2012 and 2015 on how to be an accountable organization. However, with the growth of advanced data processing, the Essential Elements of Accountability were updated in 2019 as the Enhanced Data Stewardship Accountability Elements. The below outline shows how the Canadian Privacy Management Program, upon which the Hong Kong, Colombian and Australian guidance is based, could be updated to reflect the Enhanced Data Stewardship Accountability Elements (updates are in red). This updated outline shows how the Office of the Privacy Commissioner for Bermuda could issue privacy management programme guidance for the advanced data processing covered by PIPA.

Canadian Privacy Management Program Updated for Advanced Data Processing

I. Part A: "Building blocks" or baseline fundamentals that every organization needs to have to develop a comprehensive privacy management program
    A. Organizational commitment which includes:
        1. Buy-in from the top – Senior management should:
            a. Define data-stewardship values if the organisation engages in advanced data processing
            b. If the organisation engages in advanced data processing, designate senior/executive employees who are responsible for advanced data processing
            c. Appoint the privacy point person(s) (Privacy Officer)
            d. Endorse the program controls
            e. Monitor and report to the Board, as appropriate, on the program
        2. The Privacy Officer should:
            a. Establish and implement program controls
            b. Coordinate with other appropriate persons responsible for related disciplines and functions within the organization
            c. Be responsible for the ongoing assessment and revision of program controls
            d. If the organisation engages in advanced data processing, be responsible for the ongoing assessment of advanced data processing
            e. Represent the organization in the event of a complaint investigation by a privacy commissioner's office
            f. Advocate privacy within the organization
        3. The Staff of the Privacy Office should:
            a. Have delegated responsibilities to monitor compliance and foster a culture of compliance within the organization
            b. Work to ensure that privacy protection is built into every major function involving the use of personal information, including product development, customer services, ~~or~~ marketing initiatives

or if the organisation engages in advanced data processing, advanced data processing activities

4. Reporting – An effective reporting program:
    a. Clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach
    b. Tests and reports on the results of its internal reporting structures
    c. Documents all of its reporting structures
    d. Documents how all accountability requirements have been met

B. Program controls help ensure that what is mandated in the governance structure is implemented in a privacy management program
    1. Personal Information Inventory – Every organization needs to determine:
        a. What personal information it holds and where it is held (within the organization or by third parties, for example) and document this assessment
        b. Why it is collecting, using or disclosing personal information and document these reasons
        c. The sensitivity of the personal information it holds
    2. Develop and document internal policies – Key policies organization must have in place are:
        a. Collection, use and disclosure of personal information, including requirements for consent and notification
        b. Access to and correction of personal information
        c. Retention and disposal of personal information
        d. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls
        e. Challenge organization's compliance
        f. If organisation engages in advanced data processing, a policy on advanced data processing
    3. Risk assessment tools
        a. Conduct risk assessment on, at least, an annual basis
        b. Conduct risk assessments for all new project involving personal information and on any new collection, use or disclosure of personal information
        c. Develop procedures for conducting risk assessments and develop a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs
        d. If organisation engages in advanced data processing, conduct advanced data processing assessment that:
            i. Establishes objectives and context of data driven activity
            ii. Determines all stakeholders and acceptable level of risk in light of expected benefits for all stakeholders

iii. Assesses risk by identifying risk factors and evaluates likelihood and severity of risk occurrence
iv. Treats and reduces risk to acceptable level through appropriate measures
v. Conducts advanced data processing assessments continually and repeatedly
vi. Monitors on an ongoing basis content of advanced data processing assessment and keeps it current

4. Training and education requirements
    a. Employees need to be educated in privacy protection generally
    b. Those employees who handle personal information directly need additional training specifically tailored to their roles
    c. If organization engages, in advanced data processing, all staff involved in advanced data processing should receive training
    d. For privacy training and education to be effective, it must:
        i. Be mandatory for all new employees before they access personal information and periodically thereafter
        ii. Cover the policies and procedures established by the organization
        iii. Be delivered in the most appropriate and effective manner, based on organizational needs
        iv. Circulate essential information to relevant employees as soon as practical if an urgent need arises
5. Breach and incident management response protocols – Organizations should:
    a. Have procedure in place and a person responsible for managing a personal information breach
    b. Report to privacy commissioners and notify affected individuals
6. Service provider management – Requirements should include:
    a. Privacy provisions in contracts setting out requirements for compliance including binding the service provider to the policies and protocols of the organization and requiring the organization in the event of a breach
    b. Training and education for all service provider employees with access to personal information
    c. Sub-contracting
    d. Audits and agreements with service provider employees stating they will comply with the organization's privacy policies and protocols
7. External communication should:
    a. Provide enough information so that the public knows the purpose of the collection, use and disclosure of personal information as well as how it is safeguarded and how long it is retained

b. If organisation engages in advanced data processing, make advanced data processing transparent and communicate widely data stewardship values that govern advanced data processing
c. Notify individuals if their personal information is being transferred outside of Canada
d. Include information on who to contact with questions or concerns
e. Be made easily available to individuals

8. If organization engages in advanced data processing, Individual Rights – Organization should:
    a. Be able to explain how advanced data processing may benefit and potentially pose risks to society, groups of individuals and individuals themselves
    b. Provide appropriate opportunities for feedback, relevant explanations and appeal options for impacted individuals
    c. Be open about how advanced data processing systems have been developed

II. Part B: How to maintain and improve a privacy management program on an ongoing basis, i.e. the building blocks must be monitored and assessed on a regular basis and be updated accordingly:
    A. Develop an oversight and review plan that at least on an annual basis:
        1. Sets out how and when the Privacy Officer will monitor and assess the organization's privacy management program's effectiveness
        2. Establishes performance measures and includes a schedule of when all policies and other program controls will be reviewed
        3. If organisation engages in advanced data processing, assesses whether advanced data processing assessments have been conducted with integrity and competency, whether issues raised as part of the assessment have been resolved, and whether the advanced data processing has been conducted as planned (internal oversight)
        4. If organisation engages in advanced data processing, enables the organisation to stand ready to demonstrate soundness of internal processes to regulatory agencies and certifying bodies
    B. Assess and revise program controls – The following actions need to be taken by the Privacy Officer:
        1. Monitor and update personal information inventory
        2. Review and revise policies
        3. Treat privacy impact assessments, ~~and~~ security threat and risk assessments, and if organisation engages in advanced data processing, advanced data processing assessments as evergreen documents
        4. Review and modify training and education
        5. Review and adapt breach and incident management response protocols
        6. Review, and where necessary fine tune, requirements in contracts with service providers
        7. Update and clarify external communications

Conclusion

Section 5 of PIPA has some of the elements of the accountability principle and of a privacy management program. The outline of the Canadian Privacy Management Program sets forth the basic elements of a privacy management programme found in the guidance issued by the privacy regulators in Canada, Hong Kong, Colombia and Australia and would be an excellent place for a regulator that has a new privacy law and has not issued guidance before to start. However, PIPA goes further as does the GDPR and covers advanced data processing, and many businesses in Bermuda may be engaged in advanced data processing. Therefore, the Office of the Privacy Commissioner for Bermuda, if it chooses to do so, has the opportunity to advance the guidance on accountability by issuing guidance regarding a privacy management programme that includes advanced data processing.