January 2019

The Essential Elements of Accountability were developed by a multi-stakeholder group that met in Dublin Ireland as the Global Accountability Dialogue. The Essential Elements provided granularity for the OECD Accountability Principle. It is the basis for the privacy accountability movement that led to new regulatory guidance and new approaches to law. For example, in 2010, the EU Article 29 Data Protection Working Party issued opinion 3/2010 on the principle of accountability.[1] The Office of the Privacy Commissioner of Canada and provincial commissioners in Alberta and British Colombia adopted accountability guidance in 2012.[2] Hong Kong issued accountability guidance in 2014 and updated it in 2018,[3] and Colombia issued accountability guidance in 2015.4 Now, accountability is the foundation of the General Data Protection Regulation (GDPR).[5]

The guidance and the adoption of the GDPR has elevated accountability from check-box compliance to a risk-based approach but has not kept up with the advanced data-processing activities, such as AI and ML, that may impact people in a significant manner. 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 data processing activities that might not be within their expectations, enhanced data stewardship accountability elements are needed.[6]

---

[1]. Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010.

[2]. The Office of the Privacy Commissioner of Canada (OPC) and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, "Getting Accountability Right with a Privacy Management Program," April 17, 2012. https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf .

[3]. Hong Kong Privacy Management Programme guidance was issued in 2014 and reissued in 2018. https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf .

[4]. Columbia Superintendence of Industry and Commerce, "Guidelines for the Implementation of the Accountability Principle," May 2015. https://iapp.org/media/pdf/resource_center/Colombian_Accountability_Guidelines.pdf .

[5]. General Data Protection Regulation 2016/679. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN .

GDPR Article 5(2).

[6]. Stephen Wong, "Protecting Consumers & Competition – International Emerging Technologies," 66th ABA Section of Antitrust Law Spring Meeting, April 11, 2018, 20 ("[A]ccountability represents a perfect balance between seemingly irreconcilable interests of personal data protection and innovative use of data in data-driven economies.

The Essential Elements are still key for building an accountability-based data protection or privacy program. When organisations mature beyond core processing activities to uses beyond common understanding such as advanced analytics, the Internet of Things, artificial intelligence and advanced analytics, governance needs to move from being a data custodian to a data steward. To facilitate that change the IAF developed "Enhanced Data Stewardship Accountability Elements."

These were first developed as part of the IAF's work on Artificial Intelligence, Ethics and Enhanced Data Stewardship. They were revised as part of work commissioned by the Privacy Commissioner for Personal Data, Hong Kong to explore a project to enable Legitimacy of Data Processing through an Ethical Accountability Framework.

To be able to transform data into information and information into knowledge and insight and knowledge into competitive advantage, for individuals to be able to trust data processing activities that might not be within their expectations, enhanced Data Stewardship Accountability (Enhanced Accountability) is needed.

The table below compares to the 2009 Essential Elements and the 2019 Enhanced Data Stewardship 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	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.7 Organizations should be open about their values and principles. b) Organizational policies and processes derived from these values should be anchored to clearly defined,

It helps data protection regulators realise abstract privacy principles and allows businesses to make innovative uses of data so long as they use data responsibly, minimize risks and prevent harms to data subjects.")

[7]. 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.

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.	accountable individuals within the organization and should be overseen by designated senior executives. c) The organization's data stewardship guiding8 principles should be easily understood by all staff, and in particular by technical staff, and should be capable of being programmed into activity objectives.
<u>Essential Element #2</u> 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.	<u>Enhanced Element #2</u> 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.

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

	e) Ethical Data Impact Assessments (EDIAs)9 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 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	<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.10 a) Where data processes begin with analytic insights, those insights should be tested for accuracy, predictability, and consistency with organizational values.

[9]. See here for A Model EDIA.
[10]. See here for A Model Oversight Assessment.

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 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 programmes13 in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.	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.
<u>Essential Element #4</u> Transparency and mechanisms for individual participation. To facilitate individual participation, the organisation's	<u>Enhanced Element #4</u> Processes should be transparent and, when possible, should enhance societal, groups of individual or individual interests. The data-

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 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.	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. 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 harm14 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	<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

serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed. The accountable organisation 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 organisation 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 organisation should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organisation recognise and respond to the legal authority exercising proper jurisdiction.	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.