IAF
Information Accountability Foundation

December 2020

The Essential Elements of Accountability were developed by a multi-stakeholder group as part of the Global Accountability Dialogue. The Essential Elements provided granularity for the OECD Accountability Principle. It was 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] *Colombia issued accountability guidance in 2015.*[4] *, And lastly, the Singapore Personal Data Protection Commission's "Guide to Developing a Data Protection Management Programme" was released in November 2017.* [5] *Now, accountability is the foundation of the General Data Protection Regulation (GDPR).*[6]

The guidance associated with the adoption of the GDPR has elevated accountability to specific requirements and to a risk-based approach but has challenges in terms of innovative data uses and 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

[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] Guide-to-Developing-a-Data-Protection-Management-Programme-(18-Nov-2020).pdf (pdpc.gov.sg)

[6] . 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).

insight and knowledge into competitive trusted advantage, and for individuals to trust data processing activities that might not be within their expectations, fair processing demonstrable accountability elements are needed.[7]

The Essential Elements are still key for building an accountability-based data protection or privacy program and for meeting legal compliance obligations. When organisations evolve beyond core processing activities to uses that are more complex and which increasingly involve the Internet of Things, artificial intelligence and other advanced analytics technologies, governance needs to move from being a data custodian to a fair processing data steward.

*As part of this evolvement, the IAF first developed "Enhanced Data Stewardship Accountability Elements." As calls for more fair processing and/or ethics based data processing, more demonstrable accountability has grown and the growth of artificial intelligence and its data impact reinforce the need for trusted technology, not just trusted data, these elements have evolved to encompass "**Fair Processing Demonstrable Accountability.**"*

This evolvement was first developed as part of the IAF's work on Artificial Intelligence, Ethics and Enhanced Data Stewardship. The elements 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. These elements evolved based on work done in Canada seeking to find solutions to accountable People Beneficial Data Processing. These elements are also reflected in the Fair and Open Use Act, a broader form of privacy legislation that shows how an advanced form of accountability can support effective privacy legislation in an era of advanced data processing. More recently the IAF's work studying The Movement Towards Demonstrable Accountability – Why It Matters, highlights a next stage in the evolvement of fair processing accountability.

Fair Processing Demonstrable Accountability Elements
Organisational commitment to fair processing demonstrable accountability and the adoption of internal policies consistent with external criteria and established fair processing principles.

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

As a matter of commitment, organisations should define fair processing values and/or principles which then are translated into organisational policies and processes for fair data processing.

a. These principles should be organisationally derived and should be in addition to laws or regulations. They may go beyond what the law requires but should be aligned, and not be inconsistent, with existing laws, regulations, or formal codes of conduct.[8]
b. Organisational policies and processes derived from these principles should be anchored to clearly defined, accountable individuals within the organisation and should be overseen by designated senior executives.
c. The organisation's fair processing guiding[9] principles should be easily understood by all staff, and in particular by technical staff, and should be capable of being programmed into activity objectives.

Mechanisms to put fair processing policies into effect, including risk based adverse impact assessments, tools, training and education.

Organisations should use a risk based "fair processing by design" process to translate their fair processing principles and other policy requirements into their data-analytics and data-use system design[10] processes so that society, groups of individuals, or individuals themselves, and not just the organisations, gain value from the data processing activities, such as AI or ML.

a. Organisations should establish a programmatic risk management approach to identify, assess, mitigate and monitor processing benefits and detriments on an ongoing basis.
b. At a minimum, "processing risk" should assess the level of "adverse processing impact" potentially created by processing that includes the likelihood that adverse processing impact will occur as a result of processing and the degree, magnitude, or potential severity of the adverse processing impact should it occur.
c. Processing risk should assess the benefits and/or missed outcomes that may or may not occur.[11]
d. All staff involved in data impacting processing should receive training so that they may competently participate in a "fair processing by design" process.
e. Where appropriate, organisations should follow codes of conduct that standardize processes to industry norms.
f. Fair Processing Impact Assessments (FPIAs)[12] 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. FPIAs should include a risk-based approach to assess the likelihood and significance of benefits and adverse impacts.

[8] 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.

[9] See IAF Blog: The Need for an Ethical Framework, https://informationaccountability.org/2017/01/iag-blog-ethical-principles-and-framework/

[10] Big data analytics, advanced analytics, ML and AI all refer to analytic operations that take advantage of the massive data sets and processing capabilities that have become available in the past decade or so and that use them to find correlations and make and use predictions

[11] The IAF believes that a risk assessment should include both benefits and adverse impacts.

[12] See here for A Model EDIA (FPIA). This assessment can be added to or incorporated into an organisation's existing assessment process.

1. 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 benefits and adverse impacts should be explicitly defined and balanced. The adverse impacts should be necessary and proportional to the benefits and should be mitigated to the extent possible.
2. Adverse impacts and benefits should be assessed using the established programmatic risk management approach.
3. Where data processes begin with analytic insights, those insights (and the underlying data) should be tested for accuracy, predictability, bias and fairness and consistency with organisational values.
4. The systems, technology and the data that feed those systems should be assessed for appropriateness based on the decision the data are being used for and should be protected proportional to the risks. This assessment should be ongoing.
5. Instrumentation and/or tooling should be developed and implemented to help enable the outcomes of a FPIA and to support the development of products and services that meet the organisation's fair processing principles and other policy requirements.

Internal review processes that assess higher risk FPIAs[13] and the overall fair processing program.

a. Higher risk or higher impacting data initiatives, or where the adverse impacts have not been sufficiently addressed, should be referred to more senior organisational decision-making group(s) for their review and approval.

b. The escalation process should be based on and be part of the programmatic risk management approach and should address that issues raised as part of the FPIA have been resolved and that the advanced data processing activities have been conducted as planned.

c. Where internal reviewers need external expertise, that expertise should be sought.

d. The full organisational fair processing system should be assessed for its effectiveness and whether the controls are effectively established and are meeting the organisation's risk objectives.

e. The review of the fair processing process should be separate and independent from the parts of the organisation implementing and governing the fair processing process.

Individual and organisational demonstrability and mechanisms for individual participation.

The fair processing principles that govern the advanced data-processing activities and that underpin decisions should be communicated widely; processes should be proactively transparent and explainable wherever possible. Furthermore, societal and individual concerns should be addressed and documented as part of the FPIA process, and accountability feedback mechanisms should be established.

a. Organisations should be open about their fair processing principles, making them publicly accessible.

b. Organisations should be able to explain how data are used, how the use may benefit and potentially pose detrimental impact to society, groups of individuals, or individuals themselves whose data are associated with the processing, and how society, groups of

[13] What is "higher risk" is scenario and impact driven. See Assessment Choice for Ethical Data Stewardship as one example of determining risk levels

individuals and individuals themselves may participate and object. This explanation should allow individuals to understand the nature and elements of the decision to which they are being subject or the rules that define the processing and the decision's principal characteristics.

c. Some form of meaningful explanation always should be possible without compromising intellectual property.
d. Organisations should make public on at least an annual basis the types of advanced analytics activities the organisation engages in, how data are used to achieve each beneficial purpose and a summary of the decision process relative to these data activities**.** This disclosure should include the types of third parties to which personal data may be transferred as part of these data activities.
e. Organisations should document and disclose descriptions of the fair processing governance processes they employ (e.g., policies and procedures) and make public program elements.
f. Organisations should be open and provide a clear explanation 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.
g. 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.
h. Specific mechanisms should provide individuals with the ability to challenge the outcome of automated processing.

Means for remediation and external enforcement.

Organisations should stand ready to demonstrate the soundness of internal processes to the regulatory agencies that have authority over them, including certifying bodies to which they are subject, advanced data-processing activities, such as AI or ML processes, as well as when data processing does or may impact people in a significant manner.

a. Organisations 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 fair processing principles. Organisations must maintain and document an accountable processing management program, taking into account the entity's size and complexity, activities, and legal requirements. The program should be designed to:
    1. Achieve compliance with the applicable legal or regulatory requirements, industry best practices, and organisational policies;
    2. Promote effective management and oversight of processing;
    3. Manage risk, including processing risk, on an ongoing basis;
    4. Evaluate both adverse and beneficial impacts of processing; and
    5. Demonstrate the entity's ongoing commitment to fair processing.