The Essential Elements of Accountability

The global accountability project began in 2009 as a dialogue co-facilitated by the Office of the Privacy Commissioner of Ireland and the Centre for Information Policy Leadership at Hunton & Williams LLP. Privacy enforcement agencies, governments, civil society and business met twice in Dublin, Ireland. The project published "Data Protection Accountability: The Essential elements" in October, 2009. The five Essential Elements below are the structural building block for accountability-based privacy governance.

An accountable organization demonstrates commitment to accountability, implements data privacy policies linked to recognized outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organization policies. The essential elements articulate the conditions that must exist in order that an organization establish, demonstrate and test its accountability. It is against these elements that an organization's accountability is measured.

The essential elements are:

1. **Organization commitment to accountability and adoption of internal policies consistent with external criteria.**

   An organization must demonstrate its willingness and capacity to be both responsible and answerable for its data practices. An organization 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 organization, and performance against those plans at all levels of the organization must be visible to senior management. Commitment ensures that implementation of policies will not be subordinated to other organization priorities. An organizational structure must demonstrate this commitment by tasking appropriate staff with implementing the policies and overseeing those activities.

2. **Mechanisms to put privacy policies into effect, including tools, training and education.**

   The organization 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 organizations must build privacy into all business processes that collect, use or manage personal information.

3. **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 organizations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organization'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 organization should establish programs 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 organization and to outside vendors and independent third parties. The organization 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 organization can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organization 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 organization that would take responsibility for their resolution.

4. **Transparency and mechanisms for individual participation.**

   To facilitate individual participation, the organization's procedures must be transparent. Articulation of the organization's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organization develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organization's data practices as he or she requires. The accountable organization 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 organization's decisions about data use. Individuals should have the ability to see the data or types of data that the organization 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.

5. **Means for remediation and external enforcement.**

   The organization 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 organization'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 organization should identify an individual to 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 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 programs and dispute resolution.