Self-Assessment of a Comprehensive Privacy Programme: A Tool for Practitioners

The Accountability Project ("the Project") is pleased to release "Self-Assessment of a Comprehensive Privacy Programme: A Tool for Practitioners." This tool is the product of the Project's fourth year and responds to the need for a practical means to help organisations implement and evaluate the programmes and practices necessary to establish accountability for responsible data protection.

Background

In its first year, the Accountability Project articulated the essential elements that an organisation must adopt to be accountable. It stated that an organisation demonstrates commitment to accountability, implements data privacy policies linked to recognized external criteria and implements mechanisms to promote responsible decisions about the management and protection of data. Such external criteria include applicable law and regulation, and recognized external guidelines. The Project's first year established that to be accountable, an organisation should design and implement comprehensive data and privacy protection programmes based on analysis of the risks data use raises for individuals and on responsible decisions about how those risks can be appropriately mitigated.

In its second year, the Project proposed the fundamental conditions that an organisation should put in place and be able to demonstrate to regulators. It further considered how, and under what circumstances, regulators, data protection authorities and their designated agents would measure accountability. The Project anticipated that organisations and regulators must be able to implement and measure the fundamentals in a manner suitable for the organisation, its business model and the way it collects, uses and stores data.

In year three, the Project considered accountability as an approach to privacy and data protection required and implemented across the marketplace, and articulated the benefits that would accrue to individuals, the market and organisations as a result. While in such a model all organisation would adopt accountability, the Project identified instances in which an organisation might seek recognition of its accountability. It also described under what circumstances organisations would be required to demonstrate their accountability, and what that demonstration would entail.

When the Project continued into its fourth year in 2012, accountability had emerged as a recognized approach to privacy and data protection. The European Commission had proposed a data protection regulation that would apply across European Union member countries and in which accountability played a critical role. The Privacy Commissioners of Alberta and British Columbia in Canada had released a document articulating what data protection authorities would expect of organisations under an

accountability approach. The Organisation for Economic Cooperation and Development is considering possible revisions to the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, among them a more fully developed description of the principle of accountability. The Asia-Pacific Economic Cooperation forum (APEC) finalized its Cross-Border Privacy Rules system, an accountability-based code of conduct for businesses in the APEC region.

In light of the evolution of accountability into an accepted, practical approach to privacy and data protection, the Accountability Project set as a goal development of a tool that would assist organisations in evaluating the steps they have taken internally to establish the conditions for accountability and in demonstrating them to data protection authorities or their recognized third-party agents.

The Self-Assessment Tool

The attached self-assessment tool is designed to facilitate the internal review of an organisation's privacy and data protection programmes and practices. It is also intended to help the organisation evaluate and make responsible decisions about what measures are working and what are not, determine whether or not their programmes foster responsible decisions about data protection and data use, and determine when changes or enhancements may be necessary and what those may be. It is not expected to take the place of a comprehensive review or audit. While it is anticipated to serve primarily as an instrument for use within organisations, it also may be useful as they demonstrate their accountability to data protection authorities.

In considering this tool, it is important to emphasize that accountability does not take the place of compliance with applicable law or regulation. Rather, it serves as a way for organisations to ensure that their internal policies correspond to criteria in law and legislation (and, where appropriate, recognized external guidance) and that their internal practices foster their effective implementation.

Users of this document should also bear in mind that accountability is not a "one-size-fits-all" approach. Organisations will establish the essential elements of accountability by creating conditions that meet requirements but also correspond to their size and complexity, and to the extent and sensitivity of their data holdings and processing. The response of small and medium-size enterprises to the elements listed in this tool may differ markedly from those of large organisations, but still be entirely appropriate and legitimate if they serve the intended goal of accountability.

Finally, while this instrument can serve all data holders, its primary focus is data controllers. While both controllers and processers may wish to establish the conditions for accountability, different requirements may apply, as controllers and processors may be accountable for implementing different measures.

As in the past, the work of this phase of the Accountability Project was undertaken by international experts from government, regulatory agencies, industry, academia and civil society who oversaw the drafting of this document by the Centre as it carried out the work as secretariat. The tool was circulated among all participants for their comments and revisions and reflects the result of that process. This collaboration was critical to the success of the work, but the Centre alone is responsible for any errors.

Self-Assessment of a Comprehensive Privacy Programme: A Tool for Practitioners[1]

This survey is intended for use by organisations conducting a self-assessment of their privacy programmes. The results of this review would help organisations determine which programme areas would require a more in-depth review or enhancements. While not designed to support a comprehensive review, the results of this survey may also be useful in demonstrating to regulators and other interested constituencies the design of an organisation's privacy programme. This survey is the work of the Accountability Project - an international, multi-stakeholder initiative begun in 2009 that seeks an innovative approach to privacy and data protection based on an organisation's comprehensive programme to implement data protection policies linked to applicable law, regulation and recognized guidance, and assessment and mitigation of risks to individuals raised by the collection and use of data.[2]

Elements of a Comprehensive Privacy Programme

Element	Description
I. Organisational Commitment	
A. Commitment by senior decision-makers	The organisation's senior decision-makers commit to an internal data privacy policy linked to external criteria in law, regulation and recognized guidance as appropriate; a programme that implements the policy; and an organisational culture that respects privacy. 1. Mechanism exists to assure senior decision-makers have endorsed the organisation's privacy programme. 2. Programme resources are proportional to the

[1] This self-assessment tool was prepared by the Centre for Information Policy Leadership as secreteriat to the Accountability Project, and has not been endorsed by any regulatory agencies or official bodies. It is adapted from "Getting Accountability Right with a Privacy Management Program," a document developed by the Office of the Federal Privacy Commissioner of Canada and the Information Commissioners of Alberta and British Columbia.

[2] For a comprehensive discussion of accountability, see "Data Protection Accountability: The Essential Elements," "Demonstrating and Measuring Accountability," and "Accountability: Data Governance for the Evolving Digital Marketplace," and related materials athttp://www.informationpolicycentre.com/resources/#accountability.

Element	Description
	volume and sensitivity of the data holdings and processing, and the risks to individuals they may raise. 3. Senior decision-makers communicate their endorsement to employees.
EXPLAIN:	
B. Responsible privacy personnel	• Organisation establishes an internal role responsible for: 1. Developing and implementing the privacy programme; 2. Reviewing and revising the privacy programme; 3. Ensuring that privacy protections are built into all major organisation functions involving personal information; and 4. Monitoring compliance for the privacy programme. • Where applicable, the privacy role meets the requirements of law and regulation. • Responsibilities of the privacy role are clearly defined and are communicated throughout the organisation. • Organisation decision-makers and organisational structure supports monitoring and compliance functions of the privacy role. • Budget and personnel resources appropriate to the size and complexity of the organisation, and the volume and sensitivity of its data and data processing functions are identified and allocated to support the privacy role.
EXPLAIN:	
C. Reporting	• Reporting mechanisms are clearly defined and documented, and reflect the organisation's programme controls. • Processes are in place to escalate issues to

Element	Description
	appropriate senior levels.
EXPLAIN:	
II. Implementation Controls and Procedures	
A. Personal information inventory	The organisation or the business units that make up the organisation conduct periodic inventory of its data holdings. The organisation is able to identify and document: 1. The personal information in its custody or control; 2. Its authority, according to law or regulation where applicable, for the collection, use and disclosure of the personal information; and 3. The sensitivity of the personal information.
EXPLAIN:	
B. Policies	The organisation has implemented and documented policies that link to external criteria in applicable law, regulation and accepted guidance.
EXPLAIN:	
C. Risk assessment and mitigation	The organisation conducts and documents regular assessments of the risks to individuals caused by the loss, compromise or misuse of data and takes steps to mitigate the risks identified. The risk assessment is proportional to the volume and sensitivity of the data holdings and processing and the risks to individuals they may raise.
EXPLAIN:	
D. Training and education requirements	Documented programmes exist to train employees to understand the organisation's policies and procedures. Training is differentiated based on employee roles.
EXPLAIN:	
E. Breach and incident management response protocols	Processes and responsibilities for dealing with breaches and similar incidents are documented and clear.

Element	Description
EXPLAIN:	
F. Service provider management	• Risks to individuals related to use of third party processors have been assessed • Contracts contain provisions that: 1. Bind the services provider to the privacy policies and protocols of the organisation that are relevant to the data they have contracted to process; 2. Require that the organisation be notified if there is a breach at the service provider that compromises the organisation's data.
EXPLAIN:	
G. External communication	Individuals are made aware of: 1. The organisation's commitments with respect to data pertaining to the individual; 2. The organisation's data policies and procedures; 3. How to contact organisation
EXPLAIN:	
H. Oversight and review plan	The organisation develops and documents an oversight and review plan.
EXPLAIN:	
I. Assess and revise programme controls as necessary	The organisation: 1. Updates personal information inventory; 2. Revises policies; 3. Revisits risk assessment tools to assure they are effective to deal with emerging applications of data; 4. Modifies training and education; 5. Adapts breach and incident response protocols;

Element	Description
	6. Fine-tunes service provider management; and 7. Improves external communication.
EXPLAIN:	