Effective Data Protection Governance
An Approach to Information Governance in an Information Age

OECD Expert Consultation
Boston October 2016
Today’s Objectives Are the Same, But the Challenges Are Different

• Data protection and privacy law have always had the dual objectives of facilitating the free flow of information, while protecting individuals’ interests in privacy and preventing inappropriate uses.
• Today, data protection is being thought about as ensuring a full range of individual interests has been considered while enabling knowledge growth through data.
• The acceleration of data generated from analytics, the increasing velocity of data flows, and the vastly expanding potential uses of data, even by entities that have no direct relationship with the individual, require a fresh new, dynamic and ethical approach to best accomplish these dual objectives.
• The Effective Data Protection Governance Project
  – Born from a recognized need by business sponsors that a new model was required
  – Rapidly developing and iterating a framework that is actually applied, not just theoretical
  – Builds on work done by the IAF (specifically Big Data Ethics) – and work underway (Legitimate Interest Balancing)
  – Short and Long-term utility - helpful as today’s policy models develop and are implemented
  – Time to test in a specific test case – an IoT scenario
  – Time to more broadly engage with stakeholders
Key Questions for an Effective Data Protection Governance System

1. What broader responsibilities are required for data stewards?
2. How would a Comprehensive Data Impact Assessment work and how would it scale (up and down a data intensity scale)?
3. What level of participation is meaningful and practical for an individual to have; meaningful yet puts/keeps the individual in the center?
   - When should individual participation occur?
   - How does the individual exercise his/her control?
4. What types of oversight are needed?
   - How would enforcement work?
5. How does an evolved governance system benefit regulators, individuals (consumers) and business?
Why is Today More Complicated?

A Two Dimensional Problem - Information flows and uses are beyond the ability and expectations for individuals to manage and for regulators to easily enforce. **Breadth & Depth**
Future Framework for Ethical Data Governance

(A Data and Data Use Based Approach)

- **Data** (Collected, Observed, Created)
- **Known & Unknown Use(s)**
- **Upstream Obligations**
- **Legitimate Data**
- **Data Provenance**

Comprehensive Data Impact Assessment

Acceptable Application of Data

Downstream Obligations

Obligations

**Transparency**
- Comprehensive Notice
  - Optional
- Privacy policy

**User Engagement**
- Opt-Out (Implied Consent)
- Opt-In (Affirmative)
- Access/Correction/Deletion
- Compliant Handling /Redress

**Standard**
- Accountability Program
- Independent Oversight
- Reasonable Security
- Data Integrity
- Cross-Border Obligations
- Other Legal Obligations
- Self-Regulation
- Data Retention
- Data Provenance
- Legitimate Sources
- Upstream Obligations
- Legitimate Recipient
- Downstream Obligations

**Downstream Obligations**
Framework for Ethical Data Governance
Comprehensive Data Impact Assessment

- Upstream Obligations
- Legitimate Data Source
- Data Provenance

Data (Collected, Observed, Created)

- Identifiability
- Sensitivity of Data and/or Use
- Cross-Border Obligations
- Self-Regulatory Obligations
- Other Legal Obligations

- Known & Unknown Use(s)
- Fair/Ethical Use
- Data/Use Benefit(s)
- Legitimate Interest

- Reasonable Security
- Data Retention
- Data Integrity

- Acceptable Data Recipient
- Downstream Obligations
- Notice for Regulators

- Meaningful User Engagement(s)
- Access, Correction & Deletion
- Complaint Handling

- Independent Oversight
- Accountability Program

- Sensitivity of Data and/or Use
- Legitimate Data Source
- Data Provenance

- Framework for Ethical Data Governance
- Comprehensive Data Impact Assessment
Benefits?

• **Regulators**
  – More thorough application of privacy principles by businesses that include what is currently non-PII data and is not covered by most data protection laws.
  – More effective information governance covering a broader range of interests, including more meaningful and innovative ways in which individuals are engaged relative to collection and use of information about them.
  – A process to establish an organization’s use of legitimate interest and increased and greater use of assessments.
  – More accountability/enforceability over responsible business use of information about individuals including areas that may not be subject to direct regulation, and/or where a direct consumer relationship may not exist.
  – Define domains where codes of conduct would enhance protection when data is used beyond the understanding and expectations of individuals

• **Individuals**
  – More relevant ways for individuals to engage with information about them and more contextual ways to participate in meaningful control over that data.
  – With more accountability for businesses to use information about individuals responsibility, there is less risk to the individual, resulting in higher confidence that business are focused on a broader set of the individuals risks around the use of information about them.

• **Business**
  – Greater confidence in their information governance system because it manages a broader set of interests and risks allowing businesses to aggressively leverage information to create value.
  – Clarity around regulator expectations for an accountable process to establish objective based obligations.
  – Freedom to innovate through data “discovery” (learning).
  – Flexibility to innovate around consumer centric engagement.
Next Steps

• Engage individuals/small groups for interactive/collaborative feedback
  – Test, explore, develop the framework with wearable (IoT) scenario through a multi-stakeholder approach

• Further refine and test the framework applicability to other information intensive scenarios

• Design/Test an assessment approach/tool

• **Areas still to develop** – Role and function of the Regulator, Oversight, How is Risk to be determined, What demonstration of Accountability is needed. Define the parameters that establish processing for a research (learning) purpose **Impact vs Engagement; when to engage with an individual.**

• **Key Questions:**
  – Trust?