Data Stewardship Accountability, Data Impact Assessments and Oversight Models

Detailed Support for an Ethical Accountability Framework

I. Enhanced Data Stewardship

The proliferation of information and communication technologies (ICT), like the Internet of Things, big data analytics, and artificial intelligence (AI), in recent years has brought significant changes to the scale and way personal data is collected, processed and used. ICT is bound to drive economic growth in the data economy of the 21st century and to bring tremendous benefits to both organizations and society by improving, for example, communications, resource allocation, productivity, and customer/client satisfaction. Data, in particular personal data, is the key element that fuels this growth engine. In addition, data-intensive activities that can involve advanced technologies are increasingly accessing and using nonpersonal data and yet can still have an impact on individuals. This use of ICT poses challenges to privacy-protection laws that rely heavily on the notions of "collection, transparency, notice and consent" and that focus just on personal data to protect the individual's right to personal data privacy.

Against this backdrop, the question arises: What would an accountable, trustworthy data-processing model look like in which data - intensive activities and technologies that may have an impact on individuals are conducted in a fair and ethical manner? For example, uses of data by an organization where the use does not easily enable meaningful consent, uses that may not be within the individual's expectation, uses that cannot be explained effectively through transparency alone can raise issues about trustworthiness of advanced data-processing activities. How does the individual trust that the organization is not using the data in a way that adversely impacts his or her rights or interests yet may also provide substantial benefits?

In order to encourage innovation in various global regions, digital information strategies are being adopted that recognize that the Internet and digital technologies are transforming the world, that the needs of business, government, and the general public impact the competitiveness of their country's economy, and that the protection of personal data and fair data processing are needed for the development of Internet-based economies.[1] If individuals do not trust how organizations are using their data, and how organizations are transforming data into information and information into knowledge, and the law is not keeping up with the technology, organizations need guidance on how to act ethically and apply equitable principles particularly in advanced data-processing activities, such as AI and machine learning (ML), and the application of knowledge to enable data-driven innovation to reach its full potential.[2]

---

[1]. E.g. Hong Kong Government's ICT Strategy & Initiatives, Hong Kong Digital 21 Strategy, March 2018. https://www.gov.hk/en/residents/communication/government/governmentpolicy.htm , and EU Digital Single Market Strategy, https://ec.europa.eu/commission/priorities/digital-single-market_en .

[2]. PDPO s 8(1)(c) charges the Privacy Commissioner with promoting awareness and understanding of, and compliance with, the provisions of the PDPO, particularly the Data Protection Principles. PDPO Data Protection Principles can be construed widely to include some principles of equity at law such as "mutual

Acting ethically means organizations need to understand and evaluate advanced data-processing activities and their positive and negative impacts on all parties. This approach means organizations will need to be effective data stewards not just data custodians. Data stewards consider the interests of all parties and use data in ways that create maximum benefits for all while minimizing risks to individuals and other parties. They ask whether the outcomes of their advanced data processing activities are legal, fair and just[3]. Legal, fair and just is a proxy for ethical and associated and describable values. In order to determine whether advanced data-processing activities, such as AI and ML, that may impact people in a significant manner and/or that directly impact people, are ethical or fair, organizations should define values that are condensed to core or guiding principles and then are translated into organizational policies and processes including Ethical Data Impact Assessments (EDIAs) and appropriate independent oversight. Ultimately, data stewardship is predominantly driven by organizational policies, culture, and conduct and not technological controls.

What does an appropriate trustworthy accountability framework look like for an ethical data steward?

interests" between parties. W v Registrar of Marriages [2010] HKEC 1518 at 1218 ("The absence of any relevant definition in the Ordinance itself or elsewhere would also support the view that the relevant provisions should be construed in the light of moral, ethical and societal values as they are now rather than as they were at the date of first enactment and that Parliament intended some judicial license."); Consultation Document , 1.06 (The review of the PDPO was guided by (amongst other guiding principles) the principle that ". . . the rights of individuals to privacy . . . must be balanced against other rights, as well as certain public and social interests and with reference to the particular circumstances in which they arise" and "the need to balance the interests of different sectors/stakeholders. For instance, a suitable balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology.")

[3]. IAF, "Artificial Intelligence, Ethics and Enhanced Data Stewardship", September 20, 2017, 5-7. http://informationaccountability.org/wp-content/uploads/Artificial-Intelligence-Ethics-and-Enhanced-Data-Stewardship.pdf .

Ethical Data Stewardship accountability is at the foundation layer.

II. Enhanced Data Stewardship Accountability Elements

In 2009, the accountability principle in the OECD Privacy Principles formed the basis for the Essential Elements of Accountability (Essential Elements).[4] In 2010, the EU Article 29 Data Protection Working Party issued opinion 3/2010 on the principle of accountability.[5] The Office of the Privacy Commissioner of Canada and provincial commissioners in Alberta and British Colombia adopted accountability guidance in 2012.[6] Hong Kong issued accountability guidance in 2014 and updated it in 2018,[7] and Colombia issued accountability guidance in 2015.[8] Now, accountability is the foundation of the General Data Protection Regulation (GDPR).[9]

---

[4]. Essential Elements. http://www.informationaccountability.org

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

[6]. 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 .

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

[8]. 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 .

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

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, 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.[10]

Working with approximately 20 Hong Kong businesses, the Enhanced Data Stewardship Accountability Elements for Data Processing Activities, such as AI and ML, that Directly Impacts People (Enhanced Elements) were drafted. The Enhanced Elements (see Appendix 1 for the complete text) call for organizations to:

1. Define data stewardship values that are reduced to guiding principles and then translated into organizational policies and processes for ethical data processing.
2. Use an "ethics by design" process to translate their data stewardship values into their data analytics and data use design processes so that society, groups of individuals, or individuals themselves, and not just the organization, gain value from the data processing activities, such as AI and ML, and require Ethical Data Impact Assessments (EDIAs) when advanced data analytics may be impactful on people in a significant manner and/or when data enabled decisions are being made without the intervention of people.
3. Use 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 data processing activities are conducted as planned.
4. Be transparent about processes and where possible enhance societal, groups of individual or individual interests; communicate the data stewardship values that govern the data processing activities, such as AI or ML systems developed, and that underpin decisions widely; address and document all societal and individual concerns as part of the EDIA process and design individual accountability systems that provide appropriate opportunities for feedback, relevant explanations and appeal options for impacted individuals.
5. Stand ready to demonstrate the soundness of internal processes to the regulatory agencies that have authority over data processing activities, including AI or ML processes, as well as certifying bodies to which they are subject, when data processing is or may be impactful on people in a significant manner.

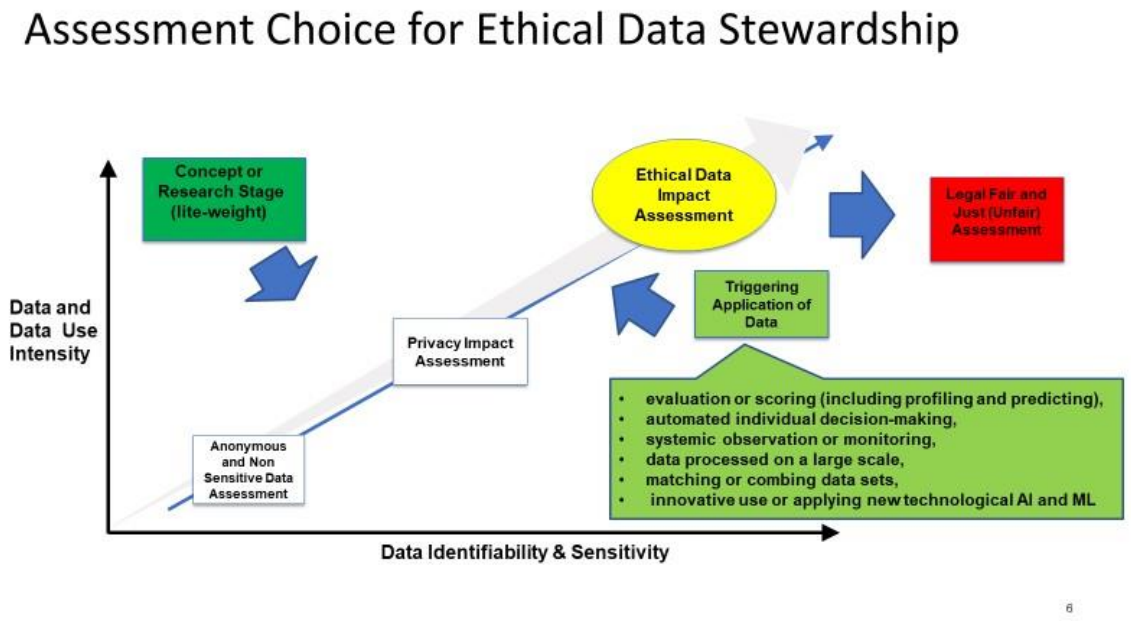
GDPR Article 5(2).

[10]. 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. 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.")

The Enhanced Elements of Data Stewardship are the foundation of trustworthy data intensive activities. They support model Data-Stewardship Values[11] and a Model Ethical Data-Impact Assessment that are further enabled by a Process-Oversight Model.

III. The Model EDIA

A triage process determines the type of assessment necessary for advanced data processing activities.



If data processing is very similar to processing that has been done in the past, no additional assessment may be necessary provided that the appropriate assessment has been conducted already. If the processing is less complex a more simplified Privacy Impact Assessment (PIA) may be more appropriate. At the concept or research stage of a data processing activity a light-weight version of a PIA might be appropriate to identify issues early in the development life-cycle. As data uses get more complex and/or are less obvious to the parties, a more rigorous PIA is likely required. Where the uses are most complex, under either a third-party or an in-house

[11]. See IAF Research Report for an example of Ethical Values.

solution, an assessment that weighs the risks and benefits may be required. It is in these latter situations where an EDIA may be more appropriate in addition to a PIA (if the EDIA does not include all the elements of a PIA).

An EDIA is a process that looks at the full range of rights and interests of all parties in a data processing activity to achieve an outcome 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. An EDIA assists an organization in looking at the rights and interests impacted by the data collection, use and disclosure in data-driven activities. In order to determine whether an EDIA may be necessary, the organization should consider, before the activity begins and when there are any changes that affect the scope of the activity, whether the data processing activity involves **advanced analytics such as: evaluation or scoring (including profiling and predicting), automated individual decision-making, systemic observation or monitoring, data processed on a large scale, matching or combing data sets, innovative use or applying new technological or organizational solutions (such as AI and ML).** If the data processing activity may have an impact on an individual or on a group of individuals that may not be anticipated or easily known, then an EDIA should be considered either at the concept stage or at the service/product/analytical development stage or at both stages. If the data processing activity does not require an EDIA, then only a PIA may need to be completed.[12]

The Model EDIA consists of four sections:

I. **Purpose of the activity**
II. **Data – a full understanding of the data, data use and parties involved**
III. **Impact to parties and in particular individuals**
IV. **Decision – whether an appropriate balance of benefits and mitigated risks supports the data processing activity**.

The very nature of an ethical and values-based assessment requires a careful consideration of the data activity benefits as well as the risks to individuals and society, considering the interests of all the parties who may be part of the activity. While open, structured questions can help, a way to organize the ultimate decision as to whether to proceed can be evaluated by using a well-established risk modeling process where the outcome of the analysis (significance, likelihood and effectiveness of controls) is depicted in a "net benefit/risk heat map". This quantitative portion uses a standardized risk assessment process often found in many organizations Enterprise Risk Management (ERM) programs.

[12]. A PIA Template example can be found at the CNIL. See https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf. The PCPD's PIA information leaflet, https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf, also contains information on how to conduct a PIA. The Office of the Privacy Commissioner for Personal Data, Hong Kong, conducted a Privacy Compliance Assessment Report on the Smart Identity Card System (SMARTICS), https://www.immd.gov.hk/pdf/PCAReport.pdf

Successful implementation of an EDIA assumes and depends on the full implementation of the Enhanced Elements and, in particular, on highly qualified and competent, accountable roles and responsibilities with appropriate separation of duties. For example, EDIAs could be conducted by the privacy group. The structure of the overall Model EDIA and the questions in each section are illustrative, and the Model EDIA should be adapted as appropriate for each organization and/or industry as well as the different data-processing contexts. In particular, in the section that determines and describes how the data-processing could potentially impact the rights and freedoms of individuals, the impact should be assessed against a context-based set of issues. The Omidyar Network and Institute for the Future have established a comprehensive Ethical Framework for Tech–Techonomy organized around "risk zones"[13] that could be used as a reference guide.

The EDIA is broader in scope than the typical PIA; however, the EDIA could be used in conjunction with the PIA. For example, all data are considered in an EDIA and not just personal data. However, to the extent the EDIA can be used to consider and appropriately mitigate the impact of a personal data practice, the EDIA process may supplement (or be woven into) the organization's PIA process. In this regard, the EDIA process may enhance an organization's privacy management program and compliance with its legal obligations under various regulatory frameworks.

An EDIA does not replace a PIA; it is designed to be used in conjunction with PIAs; it is not a complete PIA. Organizations may incorporate the EDIA in whole or in part into their own unique processes and programs so as to supplement or evolve with their PIA processes.

As a Model EDIA, other relevant authorities and/or regulatory bodies may provide input into its content and format. The goal of the EDIA is to encourage ICT innovation and competition by demonstrating that an organization has considered the interests of all parties before deciding to pursue an advanced data-processing activity.

[13]. https://ethicalos.org/

Model Ethical Data Impact Assessment

EDIA Question	Answer/Notes
Section 1: Purpose of the Activity	
A. Business objective and purpose of the data activity	
1. What is the business need/goal/objective for this data activity? *If the purpose of the activity is to solve a question/problem, what particular question/problem is the activity trying to solve? Does the activity fit within a larger theme of work that is currently being contemplated or undertaken?*	
2. Is this activity an expansion of a previous activity? If yes, determine whether a previous assessment has been done. If a previous assessment has been done, what has changed in this data activity and why (refer to previous assessment)? *Does the activity fit within a larger theme of work that is currently being contemplated or undertaken?*	
B. Accountability for the data activity	
1. Who has ultimate decision-making authority for the data activity? *Who else needs to be involved in making the decision regarding the activity?*	
2. Who is accountable for the various phases of the data activity? *Who are the leaders that are responsible for the activity?*	

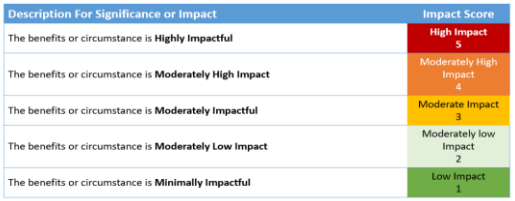
C. Legal and Other obligations regarding data collection, analysis and use(s)	
1. What laws apply to the collection, analysis and use(s) of data?	
2. Does the data activity comply with all organizational policies and self-regulatory commitments?	
3. Are there other legal, cross-border, policy, contractual, industry or other obligations linked to the collection, analysis and use(s) of data?	
4. How will all these obligations be managed and satisfied? *Have appropriate governance and accountability measures and processes been implemented?*	
Section 2: Data – A Full Understanding of the Data, Data Use and Parties Involved	
A. The nature of the data	
1. What specific types of data will be collected, tracked, transferred, used, stored or processed?	
2. Is the data identifiable to a person? *Determine whether there has been data linking of an identifiable individual's data or the data is reasonably linkable to an individual.*	
3. Is the data anonymous? *Determine how and what the anonymizing process was? Is it sufficient? Has the data been aggregated such that it is no longer identifiable personal data? Is reidentification possible? What policy, processes and/or technical measures have been used to minimize the reidentification of the data to an individual*	
4. Are there data elements that are the product of a probability-based process, such as a score?	
5. Is the data or anticipated use of the data sensitive?	

Sensitive categories of data and/or use include Information associated with personal data that is used to decide or discriminate based on race, ethnic origin, religion or philosophical belief, sexual orientation, physical or mental health, information or data that could be used to facilitate identity theft, information associated with personal data that is used to permit access to an individual's account, precise location and/or there is a reasonable expectation the use of the data would be embarrassing to the individual whose data it is. *Would any of the data use be considered sensitive to the individual?*	
B. The sources of the data to be used in the activity	
1. What are all the sources and governance of the data, internal and external? *Determine how the data was originated from each source and whether each source is a legitimate entity? How reliable is the source for the data activity? Is the source data permissible for the purposes of the activity? Who has custody or control over the source data and what are the governance arrangements?*	
2. Determine if the data is provided by the individual (originated in direct action taken by the individual) and whether: • The data is initiated (the product of individuals taking an action that begins a relationship) • The data is transactional (created when the individual is involved in a transaction) • The data is posted (created when individuals proactively express themselves)	
3. Determine if the data is observed (created as the result of individuals being observed and recorded), whether:	

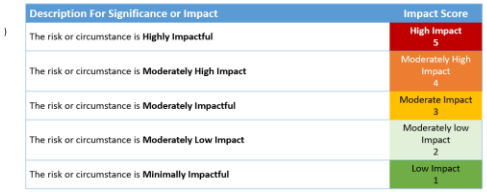
• The data is engaged (instances in which individuals are aware of observation at some point in time) • The data is not anticipated (instances in which individuals are aware there are sensors but have little awareness that sensors are creating data pertaining to the individuals) • The data is passive (instances in which it is very difficult for the individuals to be aware they are being observed and data pertaining to observation of them is being created)	
4. Determine if the data is derived (created in a mechanical fashion from other data and becomes a new data element related to the individual), whether: • The data is computational (creation of a new data element through an arithmetic process executed on existing numeric elements) • The data is notational (creation of a new data element by classifying individuals as being part of a group based on common attributes shown by members of the group)	
5. Determine if the data is inferred (product of a probability-based analytic process), whether: • The data is statistical (the product of characterization based on a statistical process) • The data is advanced analytical (the product of an advanced analytical process)	
C. The accuracy of the data	
1. Is the data accurate enough for the purpose of the activity? *Determine what steps are being taken to determine the accuracy of source data and if the source data will be accurate enough over time? Has consolidation/transformation impacted the data in such a way the accuracy is affected? Are there concerns about the quality of the final data set relative to the purpose of the activity?*	

1. What preprocessing will be done on the data before the analysis and will this affect the accuracy and appropriateness for the data activity? *Determine what work will be done to put the source data used in the analysis in a consistent format? How will the data sources be consolidated for analysis? Will errors and redundancy in the data to be used in the analysis be identified and dealt with during preprocessing? If yes, describe how these errors and redundancies will be identified and addressed.*	
1. Will preprocessing be done with data that is linkable to an individual? Describe how the preprocessing will be done and if there is any impact? *Determine if there are any sensitivity issues or unique data protection issues with respect to the preparation of the data used in the analysis? What security is appropriate for preprocessing of the data? Will the preparation steps be accurate enough over time?*	
D. The governance of the data	
1. Outside of individuals, who are all of the possible stakeholders and parties involved or related to the data activity? What are their interests and potential concerns? *Stakeholders are very broad and apply to any party impacted by the data. A stakeholder for a framework could be a regulator or advocacy organization. Stakeholders for data and data uses include data partners. However, stakeholders can also include those interested in the success of a data use*.	
2. If the data has been collected by, shared with and/or received from others, do those parties have authority to share?	

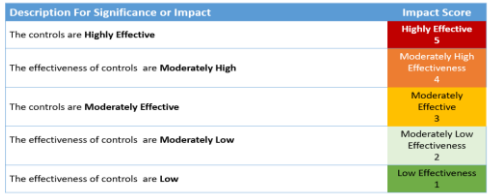
Determine whether the authority of those parties can be relied upon to protect impacted parties.	
3. Are there restrictions on data that would affect the use of the data?	
Section 3: Impact to Parties and in Particular to Individuals	
A. Identify all the impacted parties and the impacts on those parties	
1. During the activity, how will data be used and are there identifiable expectations of individuals, groups of individuals, and society for each use of the data? *For example, could there be an impact (real or perceived) to social or reputation status?*	
2. Could the data be used in a way that may result in a group of individuals being treated differently from other groups of individuals? *Determine what the goal of the difference in treatment is.*	
3. What are the benefits to the individual or groups of individuals? *Determine and describe what the positive impacts on the parties are that are expected to come from the data activity. Consider factors such as: more objective or safer interactions, better product selection and utilization, better access to new products and services, significant discounts, improved service or ease of use, more convenience or improved health and well-being. Improved financial condition, lower cost alternatives or increased availability.*	
4. What are the benefits to society?	

Determine and describe what the benefits are that could be realized by someone beyond the immediate individual whose data is being processed. The processing of data will be more legitimate if the community or society can benefit from the usefulness of the data. Consider factors such as: better/lower cost health care, greater access to health services, or better health outcomes or an improved ability to track and assess health outcomes; more accurate sensors or devices to detect or diagnose health conditions or to improve general wellness; improved education; environmental enhancements such as water conservation, energy cost reduction; infrastructure enhancements; economic improvement; more accessible/usable technology; increased job opportunities; protection of reasonable expectation of privacy, including anonymity; protection of freedom of religion, thought and speech or protection of prohibition against discrimination.	
5. How significant is the benefit? (1-Low; 3-Medium;5-High)	
6. Are the benefits likely to occur? How likely? (1-Low; 3-Medium;5-High)	
7. What are the benefits to the organization? *Consider factors such as increased revenue; lower costs; improved profitability; greater market share; enhanced employee satisfaction; engagement and productivity; enhanced customer relationships; enhanced or maintenance of brand or reputation; assurance of compliance; fraud prevention; enhanced or maintenance of cyber or physical security; new or improved products or services or customer service; improved manner of marketing; improved ability to assess customer preferences; improvements*	

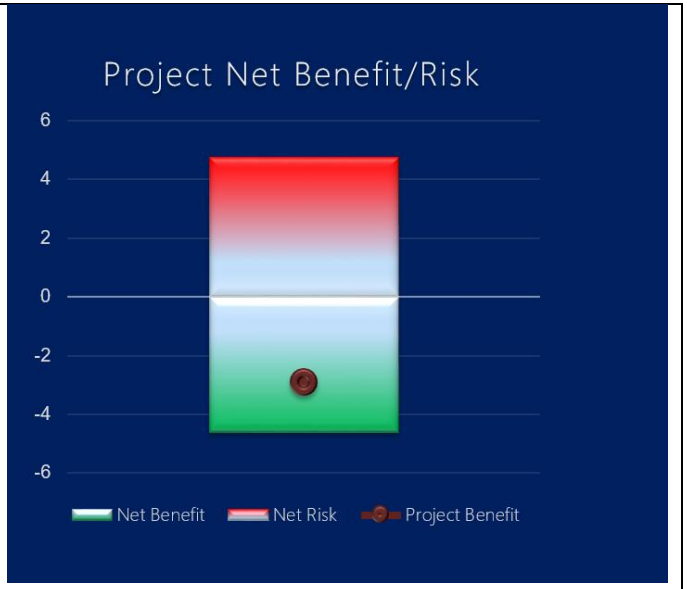
to innovation or enabling greater, faster, more efficient innovation; improved research processes; improved ability to conduct research and find or enroll study subjects or improved efficiency with studies; and innovative ways to conduct research. **NOTE:** *The benefits to the organization are not factored in the numerical assessment of significance and likelihood.*	
8. Considering all the factors relating to the data, the likely data use, the associated data activity, the identifiability and sensitivity of the data and the data activity objective, what are the risks to the individual, groups of individuals, and society? Determine and describe how the data processing could potentially impact the rights and freedoms to individuals. *Consider the risks or increase in risks to the individual whose data is being used and those risks that occur because of the processing being considered. Areas to consider include: physical harm; financial harm; reduced health and well-being or reduced ability to move freely in society; damage to reputation or embarrassment; shock or surprise at the processing activity or the results of the processing; inappropriate discrimination, such as where the discrimination is based on a legally protected class such as race, age, religion or politics; the possibility of inappropriate access to or misuse of data by the company, including sensitive or special categories of data and directly identifiable data; manipulation of needs or desires/wants of the individual (i.e. creation of a need where one previously did not exist); a negative impact of data that are the product of a probability-based process, such as a score; data subjects who may be in a more vulnerable position than the organisation processing the data, such as children or elderly or less-educated or impoverished individuals; larger volume processing (versus a small-scale pilot).*	

9. Is it foreseeable that the potential data analytical insights or the data activity might seem surprising, inappropriate or discriminatory or might be considered offensive causing distress or humiliation? *Would individuals be surprised by the data activity about them? Would the data activity about individuals align with the choices they have provided and the choices they have made? Determine whether there are other sensitivity issues with the potential insights and what aspect of collection/processing/analysis or use of potential insights might be considered unfair to the individual or society.*	.
10. Is the accuracy and/or quality of the data appropriate for the data activity? *Determine the impact of inaccurate data.*	
11. How significant is the risk? (1 – Low; 3 – Medium; 5 – High)	
12. What factors about the activity have the highest impact on the likelihood any of these risks could be realized?	
13. How likely is the risk to be realized? (1 – Low; 3 – Medium; 5 – High)	
14. Are there technical and procedural safeguards (mitigating controls) that could be implemented to prevent and mitigate risks should they occur (e.g. encryption and delinking of data or increased transparency)?	

A mitigating control Is a type of control used to discover and prevent mistakes that may lead to uncorrected and/or unrecorded misstatements that would generally be related to control deficiencies. A mitigating control may help to remedy any elevated risk identified in the analyses above. Determine what risks can be mitigated and how these risks can be mitigated	
15. In the case of analytical driven models, insights or algorithmic decision-making, what is the useful life of each insight for each user? (Periodic recalibration of the insight might be necessary.) Are there appropriate testing and review mechanisms in place? How has the risk of bias in the data activity been addressed? *Determine how long the potential insight might endure and determine whether potential insights could become less useful or valuable over time. Are potential insights progressive and sustainable (repeatable over time) and for how long are potential insights sustainable? Application of potential insights could impact behavior in a manner that could reduce predictive value of insights over time.*	
16. Is there a less data-intensive way to achieve the goals of the data activity (including potential insights)? *Determine whether the minimum possible amount of data has been used in the data activity or to obtain potential insights.*	
17. Have all the stakeholder concerns identified in the Governance of Data section been appropriately addressed?	
18. If data is to be shared with any identified stakeholder have appropriate mechanisms to ensure adherence to data obligations been put in place?	

A PIA should be done even in the case of an EDIA, and core third- party sharing controls should be evaluated for effectiveness.	
19. Does the data activity include mechanisms that explain how data is used, how benefits and risks to individuals are associated with the processing, and how individuals may participate and object where appropriate? *Determine what the transparency and individual accountability mechanisms are and whether they are appropriate for the data activity use.*	
20. How effective are these controls and safeguards in reducing risk (1 – Low; 3 – Medium; 5 – High)	

Description For Significance or Impact	Impact Score
The controls are **Highly Effective**	Highly Effective 5
The effectiveness of controls are **Moderately High**	Moderately High Effectiveness 4
The controls are **Moderately Effective**	Moderately Effective 3
The effectiveness of controls are **Moderately Low**	Moderately Low Effectiveness 2
The effectiveness of controls are **Low**	Low Effectiveness 1

The OUTOME of the assessment of benefits, risks and controls reflected in a Residual BENEFT/RISK HEAT MAP [14]	
Section 4 – Decision: Whether an Appropriate Balance of Benefits and Mitigated Risks Supports the Data-Processing Activity.	
A. Outcome	
1. Are there any other factors that should be considered? Determine whether the interests, expectations and rights of individuals have been effectively addressed and what additional contextual based individual participation and choice factors should be considered. *Consider if the risks are necessary and proportional to the benefits? Have the risks have been mitigated to the extent possible? Are the mitigated risks sufficiently balanced by the benefits?*	
2. Does the purpose of the activity fit within the values of the organization?	

[14]. Net or Residual Benefit/Risk model is for illustration purposes. Individual organizations can develop and modify consistent with their own Enterprise Risk Management system; the illustrative model consists of a numerical assessment of benefits (Significance and Likelihood) – Risks (Significance and Likelihood) = Inherent Risk – Effectiveness of controls = Residual Risk.

3. Does the purpose of the activity fit within the values of society?	
4. After considering all the above factors, is the activity a "go," "no go," or should some aspect of the activity be recalibrated to reduce the residual risk?	
B. Approvals	
1. Have all the individuals described in I.B.1. through I.B.2. above been involved in the decision?	

IV. The Process Oversight Model

Assessments conducted solely by the parts of a business implementing intensive data activities may raise issues of trustworthiness. Where the oversight of the assessment and accountability process is done by the organization itself (versus the accountability or regulatory agency), then the oversight should be conducted pursuant to a common framework.[15] Until such an approach is established, the Process Oversight Model looks at how an organization has translated organizational ethical values into principles and policies and into an "ethics by design" program. It considers how well established internal review processes, such as EDIAs and effective individual accountability systems, have been implemented. It presumes the oversight process is independent from the assessment process. It could be a function performed by, for example, an internal audit group. It may be likened to an assessment of "controls and controls effectiveness" by the internal audit group.

The internal audit group usually is established by the Audit Committee of the Board of Directors or the highest level of the governing body. The Chief Audit Executive reports functionally to the Board, and the internal audit function is independent and objective. The scope of internal audit's responsibilities encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organization's governance, risk management, and internal controls.[16] The Process Oversight Model can be thought of as analogous to a set of control definitions against which the capability and effectiveness of the organization's assessment process is tested. A set of control parameters across functional assessment domains is established and then, through a set of audits, the effectiveness of the relative controls is

[15]. See IAF, Report for Comprehensive Assessment Oversight Dialog: Canadian Ethical Data Review Boards Project, March 31, 2018, 18-24 [IAF Oversight Report]. http://informationaccountability.org/wp-content/uploads/Report-for-the-Comprehensive-Assessment-Oversight-Dialog-Canadian-Ethical-Data-Review-Boards-Project.pdf

[16]. "Model Internal Audit Activity Charter," The Institute of Internal Auditors (rev. 05/2013) https://global.theiia.org/standards-guidance/public%20documents/modelcharter.pdf .

tested. While this oversight could be performed by internal audit, it could also be accomplished by way of an assessment or test conducted by an external resource (e.g. a consulting firm). This sort of audit and testing work is similar to work already performed by these external firms in other domain areas.

The Oversight Model consists of questions in seven sections**:**

I. Accountability for the oversight process
II. Translation of organization values into principles and policies
III. Translation of organizational values into an "ethics by design" program
IV. Utilization of the EDIA
V. Internal review process
VI. Individual accountability system
VII. Transparency of process.

The questions in each section of the Process Oversight Model are illustrative, and the Process Oversight Model should be adapted as appropriate for each organization to oversee the trustworthiness of its assessment process.[17] The Process Oversight Mode is designed to address the ethics part of data stewardship and assumes other internal oversight processes exist to address core elements of privacy programs.

Evidence of oversight is important. Oversight provides rigor to the assessment process and demonstrates that oversight of the EDIA process has occurred. Whether this oversight occurs internally, for example by the audit group, or externally, for example by a consulting firm, it is necessary that documentation exists that demonstrates how the oversight was conducted and that, in fact, it was conducted. The oversight process should measure whether the EDIA process is being conducted with honesty and recognizes the full range of interests of all parties in order to demonstrate that the interests of the organization were not placed in front of the interests of other parties.[18] The organization should stand ready to demonstrate its assessment governance process and individual assessments to regulators with appropriate authority.[19] The Process Oversight Model provides guidance regarding how such oversight should be conducted and documentation that the oversight actually occurred.

[17]. An assessment of the process is designed to be different than a secondary assessment of a specific data-intensive activity.
[18]. IAF Oversight Report p. 21
[19]. Id. pp. 23-24.

The questions in each section of the Process Oversight Model are illustrative and should be adapted as appropriate for each organization to oversee the trustworthiness of its assessment process[20]. The Process Oversight Mode is designed to address the ethics part of data stewardship and assumes other internal oversight processes exist to address core elements of privacy programs. As process oversight models evolve, there may be input and guidance from other relevant authorities and/or regulatory bodies. Such input and guidance will increase the trustworthiness of the EDIA process.

Process Oversight Model

Oversight Question	Answer/Notes
I. Accountability for Oversight Process	
1. Are accountability and responsibility for achieving outcomes established through clearly defined roles throughout the organization? *Are the accountable and responsible roles carried out by competent and capable individuals? Is there a clear separation of duties between data activity roles?*	
II. Translation of Organizational Values into Principles and Policies	
1. Are shared organizational values described and/or articulated and have they been integrated into the organization? *Have the values have been condensed to core and guiding principles that are understood by technical staff? Have they been fully translated into organizational policies and processes? Have they been programmed into data and activity objectives?*	
2. Have the articulated values been aligned to the varied geographic-values across the organization's reach and footprint?	

[20]. An assessment of the process is designed to be different than a secondary assessment of a specific data intensive activity.

Could design choices become international standards or norms?	
III. Translation of Organizational Values into an "Ethics by Design" Program	
1. Does the organization have an "ethics by design process" that is part of its products/service development process? *Determine whether Core or Guiding Principles are understood by staff (in particular by technical staff) and have been programmed into activity objectives and the full product/service development lifecycle.*	
2. Does the product/service development process ascertain whether there is benefit to individuals and society in addition to the organization?	
IV. Use of an EDIA	
1. Does the organization use an EDIA to achieve a principles-based outcome of data? Is the assessment process effective? *Does the organization assess all risks and benefits to an individual, group of individuals, and society? Are the risks effectively mitigated? Does the EDIA process effectively evaluate that data use avoids actions that seem inappropriate or discriminatory, might be seen as generating unequal treatment, might be considered offensive or causing distress or humiliation?*	
2. Does the EDIA process effectively assess the complexity and potential impact of the data and data use? *Does the EDIA process consider all the factors relating to the data, the likely data use, the associated data activity, the identifiability and sensitivity of the data, as well as the potential impact of the data activity?*	

3. Does the EDIA process effectively evaluate if the purpose of the activity fits within the values of the organization and society?	
4. Is there an effective triage process to determine what type of assessment is appropriate? Is this process effectively employed? *A triage process determines the level of review of the process necessary. Where data processing is very similar to processing that has been done in the past and therefore it was concluded no assessment was necessary, only a quick review may be required to confirm those understandings. Where data uses are more complex and/or less obvious to the parties and more rigorous assessments were conducted, a more rigorous review should be required. Where the uses are most complex, an EDIAs that effectively weighs the risks and benefits should be used.*	
V. The Internal Review Process	
1. What kind of periodic assurance reviews will occur over time? *Do the periodic reviews appropriately consider the data and data-use objectives? Is the periodic review process established at appropriate timeframes?*	
2. For intensive data impacting systems, does the review assess that outcomes are as intended with the objectives of the activity and impacts are mitigated as planned, harms are reduced, and unintended consequences are understood? *Determine whether this analysis includes the likelihood of benefits being achieved and risks effectively mitigated. Does the post review include an assessment of if the anticipated outcomes were achieved?*	

3. Have analytic models and insights been tested for their accuracy and predictability? *Is there an ongoing systematic process to ascertain whether analytic models are tested for their consistency with organizational values and principles? Are data-intensive technologies subject to appropriate human direction and control?*	
4. Does the review process include a risk review by senior-accountable leadership? Are higher risk activities approved by senior-accountable leadership? *Is there a formalized, risk-ranked review process where higher impacting data activities are reviewed? Where internal reviewers need external expertise? Is this expertise sought?*	
5. Does the assessment and review process ascertain whether all parties' concerns are assessed and appropriately addressed as part of the data-system lifecycle?	
6. Have systems themselves, and the data that feed those systems, been assessed and protected proportionate to the risks?	
7. Does the review evaluate whether only the minimum data that is needed is used?	
VI. Individual Accountability System	
1. Are there effective systems that provide appropriate opportunities for feedback, relevant explanations, and appeal options for the individuals impacted? *Will individuals have some ability to engage in how their data is used? How will individual situations be remediated, if necessary?*	
VII. The Transparency of the Process	
1. Does the organization have mechanisms that explain how data is used, how benefits and risks to individuals are	

associated with the processing, and how individuals may participate and object where appropriate? *Is the use of the data transparent and effectively made available for all data activities?*	
2. Is the organization ready to demonstrate the soundness of the processes they use so that data and data-use systems are consistent with established values and principles? *Can the organization demonstrate its data stewardship accountability processes?*	

Appendix 1

Enhanced Data Stewardship Accountability Elements for Advanced Data Processing Activities, such as Artificial Intelligence (AI) and Machine Learning (ML), that Directly Impacts People

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.[21] Organizations should be open about their values and principles.
   b) Organizational policies and processes derived from these values should be anchored to clearly defined, accountable individuals within the organization and should be overseen by designated senior executives.
   c) The organization's data stewardship guiding[22] principles should be easily understood by all staff, and in particular by technical staff, and should be capable of being programmed into activity objectives.

[21]. 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.

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

2. 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.
    e) Ethical Data Impact Assessments (EDIAs)[23] 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.
    f) All staff involved in data impacting processing should receive training so that they may competently participate in an "ethics by design" process.
3. 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.[24]
        a) Where data processes begin with analytic insights, those insights should be tested for accuracy, predictability, and consistency with organizational values.
        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.

[23]. See here for A Model EDIA.
[24]. See here for A Model Oversight Assessment.

4. Processes should be transparent and, when possible, should enhance societal, groups of individual or individual interests. The data-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.
5. 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 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.