Decisioning Process, Risk-Benefits Analysis Tool for Data-Intensive Initiatives

Achieving Legal, Fair and Just Use of Data &

Appropriate Individual Engagement

November 2016

Full Range of Interests and Fair Processing For Data Intensive Initiatives

- Privacy law, no matter the location, is increasingly encompassing the objectives of both autonomy and fair processing, covering data collection and use that often goes beyond individuals knowledge and effective consent.
- This concept of fair processing links to the full range of fundamental rights and freedoms defined by charters of human rights.
- These rights and interests can be expressed by a set of Ethical Principles subsuming the data use as **Beneficial, Fair, Respectful, and Just, Transparent and Autonomy Protecting** and performed with appropriate **Accountability** with a **Redress Provision**. (See slide 19.)
- The assessment process discussed here is designed to parse whether the individuals' interests, those of society and those of processors are assessed in a manner that demonstrates legal, fair and just use of data and are risks identified and appropriately mitigated. In addition, the process considers what contextual based individual engagement/participation is appropriate.
- A core objective is to adequately and systematically (operationally) determine interests/impact to stakeholders, including specifically the individual.

Comprehensive Data Impact Assessment (CDIA)

Purpose of this Tool:

Whether the project is a core product review, the broader use of information or a big data analytics project, an assessment process is required to address legal, ethical, fair and other implications of information use. Such robust assessments must expand basic Privacy Impact Assessments to Comprehensive Data Impact Assessment (CDIA), the purpose of which is to aid in the final judgment of whether to proceed or not. A core objective throughout a CDIA process is to adequately and systematically (operationally) determine interests/impact to stakeholders, including specifically the individual.

Using a customizable tool, the CDIA identifies key issues that decision makers in the organization should consider and ways to reduce risk to all stakeholder, but especially to the individual. The tool does not generate answers for users. Rather, decision makers should take into account what they learn from the CDIA and make decisions with integrity. Documentation of the CDIA provides evidence of how decisions were made, including all appropriate mitigations.

The CDIA is both linear, covering a series of definable areas to asses, as well as circular, meaning steps should be repeated to re-investigate impacts of new or different information use and ways to reduce risk. This is particularly important in a big data analytics project where a "discovery" phase that gleans insights is then "actioned". It is also key to repeat the CDIA as new insights and new uses of data are identified and applied.

The CDIA highlights the risks and benefits to all stakeholders, explores mitigation strategies to reduce risks and identifies, when meaningful, context-based participation with individuals is appropriate.

This tool has been modified based on a version developed by the members of the Conference Board Council of Chief Privacy Officers. https://www.conference-board.org/councils/councildetail.cfm?councilid=296 and work published by the Future of Privacy Forum. The modifications have been made by the Information Accountability Foundation. It is a "framework" and should be adjusted to fit the size and complexity of various organizations to fir their specific needs.

Comprehensive Data Impact Assessment (CDIA)
A Risk-Benefits Analysis Tool for Data Intensive Initiatives

Understand and Characterize the Project

Is the project data intensive and/or new? If not, only a PIA is needed.

CDIA involves defining:

- Project Purpose
- Source Data
- Data Preparation
- Legal & Other Obligations
- Expected Project Insights/Outcomes
- Who is accountable

Assess Project Impact

Assess the various aspects of the project. This involves assessing:

- Processes
- Insights

Assess Ethical & Interests Factors

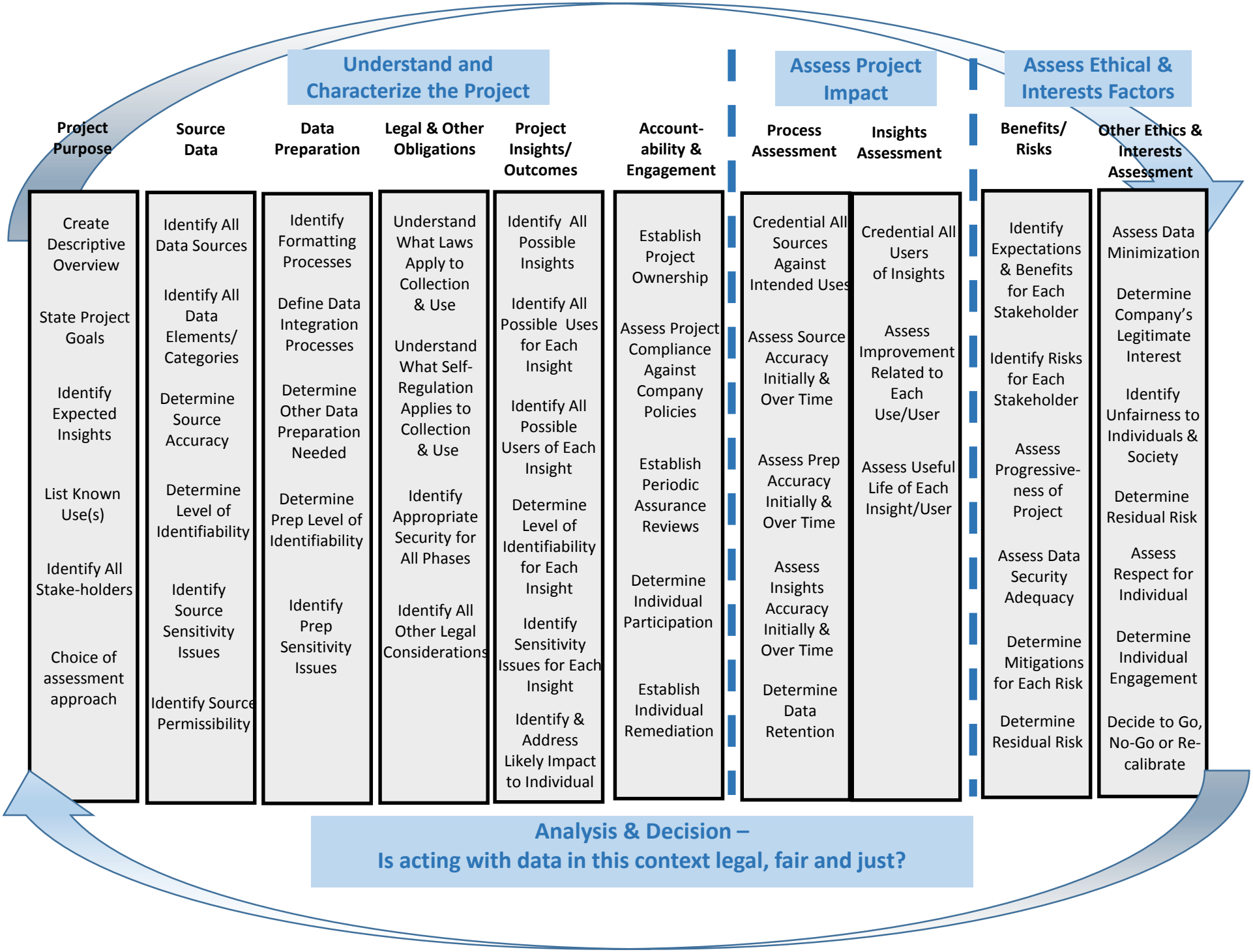
This involves addressing:

- Risks & Benefits
- Other Ethical Considerations

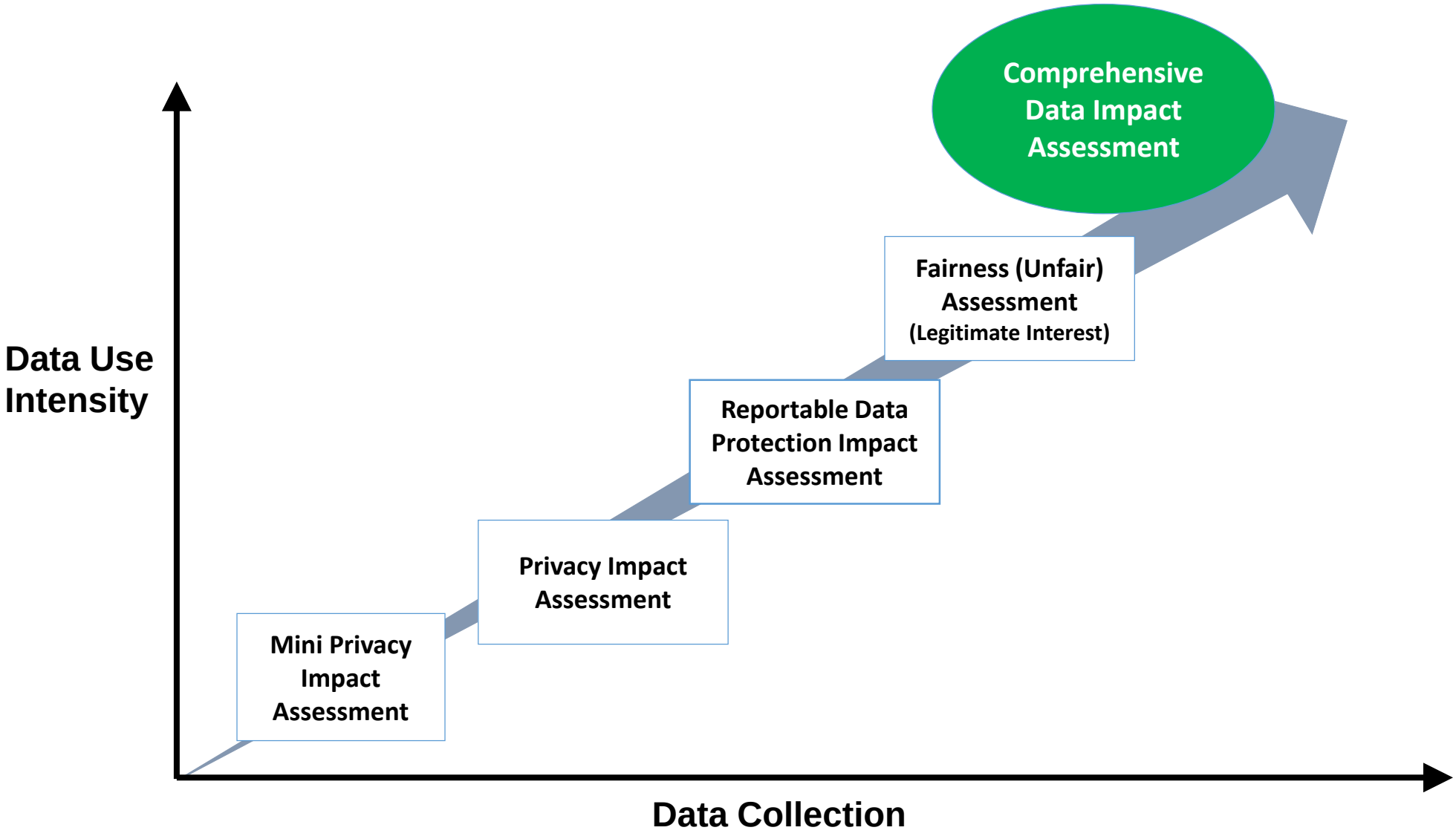
Analysis & Decision - Is acting with data in this context legal, fair and just?

- Identify the stakeholders
- Identify the benefits and mitigations that justify the processing
- Identify the residual risks that the organization is comfortable with
- Identify all individual engagement obligations
- Identify any additional obligations that are required

CDIA for Data Intensive Initiatives



Assessment Choice for Effective Data Protection Governance



Understand and Characterize the Project

Project Purpose

- Create Descriptive Overview
- State Project Goals
- Identify Expected Insights
- List Known Use(s)
- Identify All Stake-holders
- Choice of assessment approach

Project Purpose Notes:

Understanding the purpose, intended outcomes and assessment process for the project.

- Provide a project overview that describes the main purpose(s) of the project.
- State the main goals the project intends to achieve.
- Identify any possible secondary goals.
- Identify the key insights that are expected to be gained.
- List the known use(s) of the insights?
- Identify all the various (initial) stakeholders (internal & external) including individuals and society.
- Choose the proper assessment process based on intensity of the data and use(s).

Mitigations:

Understand and Characterize the Project

Source Data

Identify All Data Sources

Identify All Data Elements/ Categories

Determine Source Accuracy

Determine Level of Identifiability

Identify Source Sensitivity Issues

dentify Source Permissibility

Project Data Sources Notes:

Understand the sources of data to be used in the project.

- What are all the sources of the data?
- What are the actual elements found in the data that will be used?
- Is the source data structured or unstructured or both?
- What is the "quality" of the data (e.g., recency, coverage, element accuracy)?
- Is the data linkable to a particular individual or not? If so, how?
- Are there sensitivity issues with the source data?
- How was the data from each source originated?
- Is the source data permissible for the project?

Mitigations:

Data Preparation

- Identify Formatting Processes
- Define Data Integration Processes
- Determine Other Data Preparation Needed
- Determine Prep Level of Identifiability
- Identify Prep Sensitivity Issues

Data Preparation Notes:

Understand what pre-processing that will be done on the data before the analysis.

- What work will be done to put the source data in a consistent format?
- How will the data sources be consolidated for analysis?
- How will errors and redundancy in the data be identified and dealt with?
- Will the preparation processing be done with data that is linkable to a particular individual or not? If so, how?
- Are there sensitivity issues with the preparation of the data?

Mitigations:

Legal & Other Obligations

Legal & Other Obligations Notes:

Understand What Laws Apply to Collection & Use

Understand What Self-Regulation Applies to Collection & Use

Identify Appropriate Security for All Phases

Identify All Other Legal Considerations

Understand what legal obligations exist with the data, analysis, and use(s).

- What laws apply to your collection/acquisition of the data?
- What laws apply to the analysis of the data?
- What laws apply to the intended use(s) of the data?
- What self-regulation applies to the collection/acquisition of the data?
- What self-regulation applies to the analysis of the data?
- What self-regulation applies to the intended use(s) of the data?
- What security is appropriate for the preparation, analysis and subsequent use(s)?
- Are there other legal, cross border, policy, contractual, industry or other obligations linked to the data or the processing?

Mitigations:

Project Insights/ Outcomes

- Identify All Possible Insights
- Identify All Possible Uses for Each Insight
- Identify All Possible Users of Each Insight
- Determine Level of Identifiability for Each Insight
- Identify Sensitivity Issues for Each Insight
- Identify & Address Likely Impact to Individual

Project Insights/Outcomes Notes:

Understand what insights are expected from the project.

- What are the intended insights from the analysis?
- What are other possible insights that might result?
- What are all known uses for each insight?
- What are other possible uses for each insight?
- Who will use each of the resulting insights?
- Are the insights linkable to a particular individual or not? If so, how?
- Are there sensitivity issues with the insights?
- What is the likely impact to an individual? Is it high or low?
- How different is the data use from a “compatible” use?
- Will there be an impact (real or perceived) to social or reputation status, eligibility decisions to area such as health, education?
- Is the data use likely to be perceived as so “different” additional transparency or choice to the individual should be considered?

Mitigations:

Account-ability & Engagement

- Establish Project Ownership
- Assess Project Compliance Against Company Policies
- Establish Periodic Assurance Reviews
- Determine Individual Participation
- Establish Individual Remediation

Accountability Notes:

Determine how accountability for the project will be handled.

- Who has ultimate project ownership?
- Who all is accountable for the various phases of the project?
- Who are other leaders that are responsible in some way?
- Are all these leaders comfortable with the project?
- Does the project comply with all company policies?
- What kind of periodic assurance reviews will occur over time?
- Will individuals have some ability to engage in how their data is used?
- How will individual situations be remediated, if necessary – e.g., redress options?

Mitigations:

Assess Project Impact

Process Assessment

Credential All Sources Against Intended Uses

Assess Source Accuracy Initially & Over Time

Assess Prep Accuracy Initially & Over Time

Assess Insights Accuracy Initially & Over Time

Determine Data Retention

Process Assessment Notes:

Assess the processes used in the project.

- Is each source provider a legitimate entity?
- Is the source data permissible for the intended use(s)?
- Is the source data accurate enough for the intended use(s)?
- Will the source data be accurate enough over time?
- Will the preparation steps be accurate enough for the intended use(s)?
- Will the preparation steps be accurate enough over time?
- Will the insights be accurate enough for the intended use(s)?
- Will the insights be accurate enough over time?
- How long will the data be retained?

Mitigations:

Assess Project Impact

Benefits/ Risks

Identify Expectations & Benefits for Each Stakeholder

Identify Risks for Each Stakeholder

Assess Progressive-ness of Project

Assess Data Security Adequacy

Determine Mitigations for Each Risk

Determine Residual Risk

Insights Assessment Notes:

Assess the usefulness of the insights from the project.

- Is each downstream user a legitimate entity with a legitimate use for each insight?
- What obligations need to be transferred to each downstream user?
- Does each use of the insight provide a measurable improvement over resulting outcomes that would be achieved without the insight?
- Determine what the useful life of each insight is for each user (periodic recalibration of the insight is necessary).

Mitigations:

Benefits/ Risks

- Identify Expectations & Benefits for Each Stakeholder
- Identify Risks for Each Stakeholder
- Assess Progressive-ness of Project
- Assess Data Security Adequacy
- Determine Mitigations for Each Risk
- Determine Residual Risk

Benefits/Risks Notes:

Assess the benefits and risks associated with the project

- Relist all stakeholders for the project (internal or external to the company, individuals, society, etc.)
- What are the expectations of each stakeholder for each use?
- What benefits will each stakeholder receive for each use?
- Can the benefits be defined?
- What risks does the project pose to each stakeholder for each use?
- Are insights progressive and sustainable (repeatable over time) for each stakeholder?
- Is the data security adequate/proportional to the risks and use(s)?
- What risks can be mitigated and how for each stakeholder?
- What are the residual risks for each stakeholder?

Mitigations:

Other Ethics & Interest Assessment Notes:

Other Ethics & Interests Assessment

- Assess Data Minimization
- Determine Company's Legitimate Interest
- Identify Unfairness to Individuals & Society
- Determine Residual Risk
- Assess Respect for Individual
- Determine Individual Engagement
- Decide to Go, No-Go or Re-calibrate

Assess other ethical aspects of the project.

- What aspect of collection/acquisition/processing/analysis or use of the insights be considered unfair to the individual or to society?
- Is the collection/acquisition/processing/analysis or use of the insights done in a way that is respectful to the individual?
- Has the minimum possible amount of data been used?
- Does the company have a legitimate interest in the processing of the data and the use of the insights?
- After all mitigations have been applied, what is the residual risk to all stakeholders, particularly the individual – have the benefits and risks been effectively balanced?
- Have the interests, expectations and rights of individuals been effectively addressed?
- What additional, contextual based participation and choice (meaningful) with the individual should be considered?
- Is there an effective redress option for the individual impacted? Has this use of data been transparent?
- After considering all of the above factors, is the project a 'go', 'no-go' or should some aspect be recalibrated to reduce the residual risks?

Mitigations:

Analysis & Decision - Is acting with data in this context legal, fair and just?

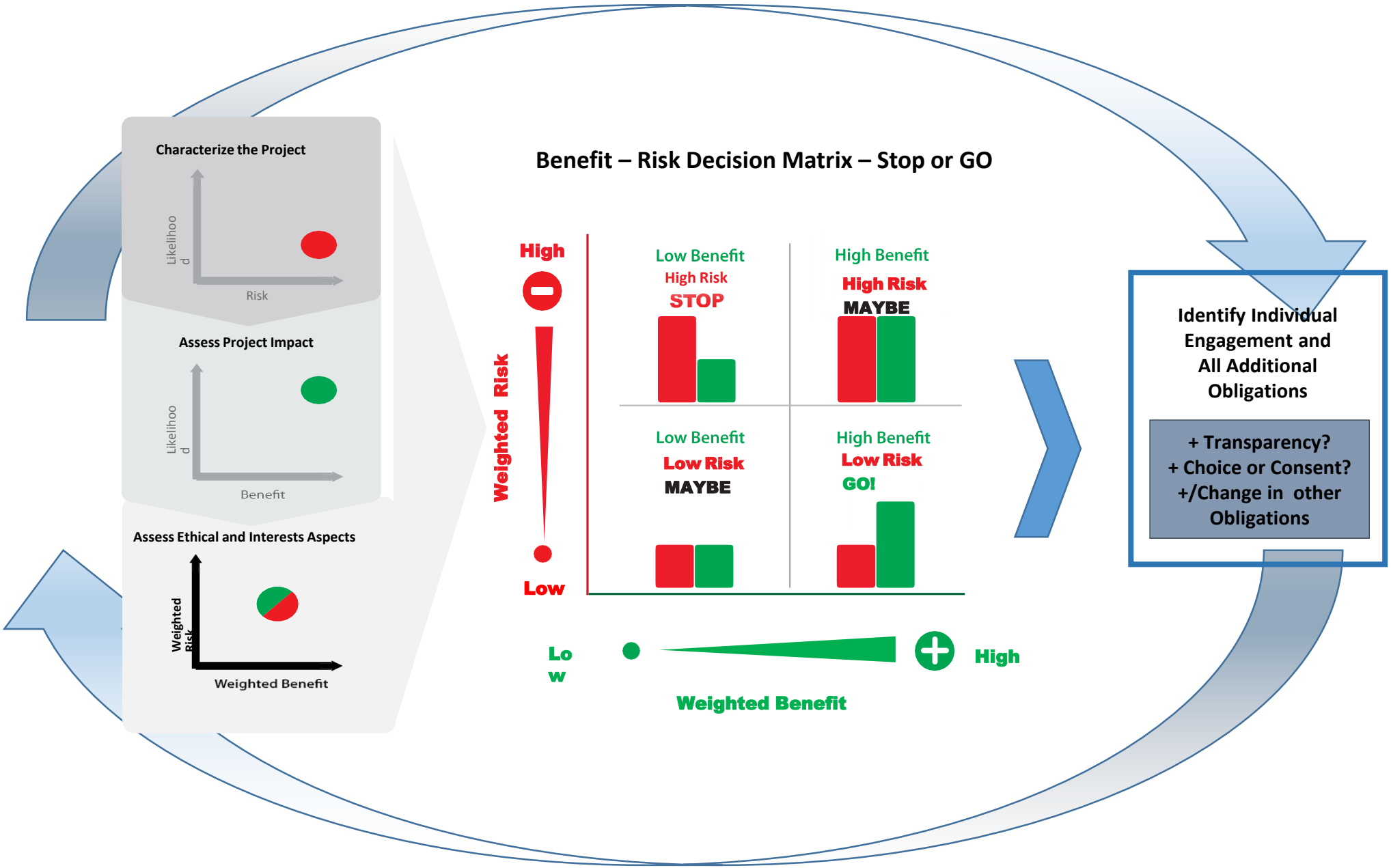
Review & Recalibrate for Maximum Results:

If any where along the way concern is raised about any of the considerations, or over time as the accuracy of insights may fade, adjustments in any of the factors and/or mitigations can be considered to achieve a better outcome. This includes adjustments in source data, data preparation processing, the actual analytics as well as the application of the insights. It may include changes to identifiability, individual engagement, retention, security, accountability or any aspect of the project.

Each pillar of the CDIA should be assessed using the questions as a guide but adding factors relative to the project, industry or product and after mitigations have been developed (as needed), the pillar should be assessed against a "benefit" "risk" and "likelihood" scale. The outcomes including an assessment of where additional engagement with individuals is required and where there any other additional obligations are determined. These should all be documented and a "go/no-go" decision should be made consistent with the Accountable approval process.

The scales for benefits risk and likelihood should be determined based on the organizations or industry's approach to risk (e.g., ERM program). For illustrative purposes, a sample "outcome" chart is shown in the following slide. As new data analysis and new applications of insights can change over time, the process of assessing benefits, risks and changing obligations or individual engagement should be repeated (recalibrated) to achieve acceptable outcomes over time.

Analysis & Decision - Is acting with data in this context legal, fair and just?



Modified based on work published by the Future of Privacy Forum. For n example of assessing benefits and risk in a data-intensive process , see https://fpf.org/2014/09/11/big-data-a-benefit-and-risk-analysis/.

Ethical Data Use Principles

- **Beneficial**
  - Uses of data should provide benefits and value to individual users of the product or service. While the focus should be on the individual, benefits may also be accrued at a higher level, such as groups of individuals and even society as a whole.
  - Where a data use has a potential impact on individual(s), the benefit should be defined and assessed against potential risks this use might create.
  - Where data use does not impact an individual, risks, such as adequately protecting the data, should be identified.
  - Once all risks are identified, appropriate ways to mitigate these risks should be implemented.
- **Fair, Respectful, and Just**
  - The use of data should be viewed by the reasonable individual as consistent, fair and respectful.
  - Data use should support the value of human dignity – that individuals have an innate right to be valued, respected and to receive ethical treatment. Human dignity goes beyond individual autonomy to interests such as better health and education.
  - Entities should assess data use against inadvertent, inappropriate bias or labeling that may have an impact on reputation or the potential to be viewed as discriminatory by individual(s).
  - Data should be used consistent with the ethical values of the entity.
  - The least data intensive processing should be utilized to effectively meet the data processing objectives.
- **Transparent and Autonomy Protection (engagement and participation)**
  - As part of the dignity value, entities should always take steps to be transparent about their use of data. Proprietary processes may be protected but not at the expense of transparency about substantive uses.
  - Dignity also means providing individuals and users appropriate and meaningful engagement and control over uses of data that impact them.
- **Accountability and Redress Provision**
  - Entities are accountable for their use of data to meet legal requirements and should be accountable for using data consistent with the principles of Beneficial, Fair, Respectful & Just and Transparent & Autonomous Protection. They should stand ready to demonstrate the soundness of their accountability processes to those entities that oversee them.
  - Individuals and users should always have the ability to question the use of data that impacts them and to challenge situations where use is not consistent with the core principles of the entity.