Colorado Data Protection Assessment

Lynn Goldstein and Peter Cullen

July 2023

IAF Colorado Data Protection Assessment

I. Introduction

This framework for a data protection assessment (DPA) is organized into XX parts. Parts II – XI, XIV-XVI, XVIII (colored in yellow) are taken directly from the Colorado Privacy Act or the Rules implementing the Colorado Privacy Act (Colorado Rules) which can be found here. Parts XII – XIII, XIX – XX (colored in green) which are taken from:

- IAF's AI Assessment which was developed in consultation with regulators and privacy and data protection professionals and based on IAF's 10+ years of experience in developing big data and complex analytics assessments such as to be used with AI, and which can be found here, and
- IAF's model legislation, the FAIR and OPEN USE ACT which was drafted by Marc Groman based upon input from IAF strategists and membership and which can be found here.

Part XIV.B. (colored in pink) is taken from Ethical OS, the Omidyar Ethical Framework for Tech.

The Colorado Privacy Act and other State privacy laws require that a DPA identify and weigh the benefits that may flow to the controller, consumer, other stakeholders, and the public, against the potential risks to the rights of consumers as mitigated by safeguards employed to reduce those risks. The weighing required by these state privacy laws is different from the weighing required by privacy laws anywhere else in the world. For example, the EU General Data Protection Regulation (GDPR) data protection impact assessments (DPIAs) only call for an assessment of the risks to the rights and freedoms of natural persons. The GDPR DPIA is a tool for managing risks to the rights of data subjects and typically is enforced against a narrower set of data protection rights; other fields manage the risks to society and organizations. EDBP Guidelines, p.17.

The Colorado Rules go even further than the State privacy laws in setting forth 11 risks to consumers that may be considered, six of which are in the IAF's FAIR and OPEN USE ACT, identifies mitigating measures and the timing of when DPAs should be conducted, and requires a DPA for Profiling if the Profiling presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on Consumers,
- Financial injury to Consumers,
- Physical or other intrusion upon the solitude or seclusion or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person, or
- Other substantial injury to Consumers.

The Colorado Rules set forth the content of the DPA for Profiling, **including** an explanation of the training data and logic used to create the Profiling system and a plain language description of the outputs secured from the Profiling process and how they are or will be used and how the Profiling system is evaluated for fairness and disparate impact and the results of any such evaluation.

The Colorado Rules and most risk taxonomies do not address risks to society or large groups of individuals. The IAF believes these types of risk are key and has added some examples from the Ethical OS to consider in the risk portion of the DPA.

The actions to be taken required by the Colorado Rules are demanding; most of them are not mechanical and call for more than a translation of the Colorado Rules into a compliance checklist. To meet the regulations explicit and implicit requirements, we believe organizations will have to adopt new governance processes and procedures (see XIX). Required actions call for open ended multi-dimensional weighing, with the expectation multiple internal stakeholders will be involved. In addition to supplementing the requirements of the Colorado Rules with IAF's prior work, the IAF has developed an impact analysis which takes into account all of the stakeholders and weighs the benefits/interests against the risks/harms using a 1,3, 5 scale and showing the results in two different ways: math determined and visual depiction.

IAF's multi-dimensional weighing is unique. It factors in as many stakeholders, benefits, and risks as are relevant to the processing being assessed. It is capable of weighing each of the stakeholders vis-à-vis each of the other two factors. It can demonstrate the results mathematically or visually or both.

The DPA required by the Colorado Rules is used only when there is a heightened risk of harm to consumers (i.e., when risky processing is conducted, including Profiling). Because of the IAF's additions to the DPA, the IAF version of the DPA can assess Artificial Intelligence (AI) where AI goes beyond Profiling. Getting the DPA right is good for business. The weighing of the risks and benefits to the numerous stakeholders will be worthwhile only if it done competently and with integrity. The IAF version of the DPA enables business to weigh the risks and benefits of AI competently and with integrity.

II. Timing of the DPA

- The Controller must conduct and document the DPA before initiating a Processing activity that Presents a Heightened Risk of Harm to a Consumer (i.e., risky processing). Examples of risky processing are:
    - Targeted advertising
    - Profiling that presents a reasonably foreseeable risk of unfair or deceptive treatment or disparate impact
    - Financial, physical, or reputational injury
    - Intrusion upon seclusion offensive to a reasonable person
    - Sensitive data

- The Controller must review and update the DPA as often as appropriate considering the type, amount, and sensitivity of Personal Data Processed and level of risk presented by the Processing, throughout the Processing activity's lifecycle in order to: 1) monitor for harm caused by the Processing and adjust safeguards accordingly; and 2) ensure that data protection and privacy are considered as the Controller makes new decisions with respect to the Processing.
- DPAs containing Processing for Profiling in furtherance of Decisions that Produce Legal or Similarly Significant Effects Concerning a Consumer must be reviewed and updated at least annually and include an updated evaluation for fairness and disparate impact and the results of any such evaluation. –
- A new data Processing activity is generated when existing Processing activities are modified in a way that materially changes the level of risk presented. When a new data Processing activity is generated, a DPA must reflect changes to the pre-existing activity and additional considerations and safeguards to offset the new risk level. Modifications that may materially change the level of risk of a Processing activity may include, without limitation, changes to any of the following:
    - The way that existing systems or Processes handle Personal Data
    - Processing Purpose
    - Personal data Processed or sources of Personal Data
    - Method of collection of Personal Data
    - Personal Data recipients
    - Processor roles of Processors
    - Algorithm applied or algorithmic result, or
    - Software or other systems used for DPAs Processing
    - DPAs are required for activities created or generated after July 1, 2023. This requirement is not retroactive.

III. Retention of the DPA

DPAs, including prior versions which have been revised when a new data Processing activity is generated, must be stored for as long as the Processing activity continues, and for at least three (3) years after the conclusion of the Processing activity. DPAs must be held in an electronic, transferable form.

IV. Triggers for a DPA

Processing that presents a "heightened risk of harm to a consumer" including the following:

(a) Processing Personal Data for purposes of targeted advertising or for Profiling if the Profiling presents a reasonably foreseeable risk of:
1. Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
2. Financial or physical injury to consumers;

3. A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
4. Other substantial injury to consumers;

(b) Selling Personal Data; and
(c) Processing Sensitive Data.

Profiling means any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

Triggers for a DPA for Profiling

Controllers must conduct and document a DPA for Profiling if the Profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of, or unlawful disparate impact on Consumers
2. Financial or physical injury to Consumers
3. A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or
4. Other substantial injury to Consumers.

Controllers should consider both the type and degree of potential harm to Consumers when determining if Profiling presents a reasonably foreseeable risk of "other substantial injury" to Consumers."

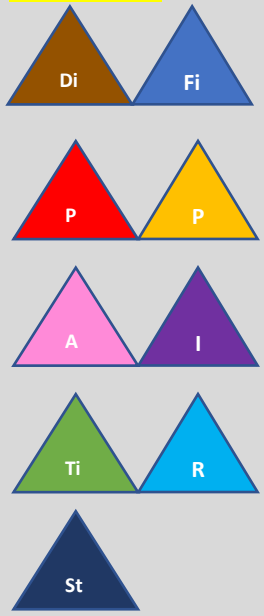
Profiling covered by DPA obligations includes Profiling using Solely Automated Processing, Human Reviewed Automated Processing, and Human Involved Automated Processing

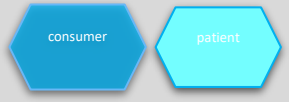
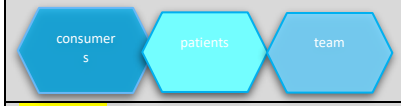
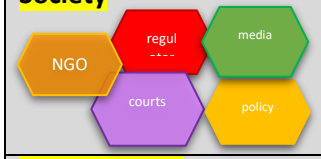
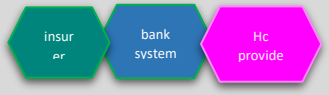
V Scope	A. A DPA must be a genuine, thoughtful analysis of each Personal Data Processing activity that presents a heightened risk of harm to a Consumer that: 1) identifies and describes the risks to the rights of consumers associated with the processing; 2) documents measures considered and taken to address and offset those risks; 3) contemplates the benefits of the Processing; and 4) demonstrates that the benefits of the Processing outweigh the risks offset by safeguards (controls) in place.

	B. The depth, level of detail, and scope of the DPA should take into account the scope of risk presented, the size of the Controller, amount and sensitivity of Personal Data Processed, Personal Data Processing activities subject to the assessment, and complexity of safeguards applied. C. A "comparable set of Processing operations" that can be addressed by a single DPA is a set of similar Processing operations including similar activities that present heightened risks of similar harm to a Consumer.
VI Purpose (summary business need/goal/ objective for this data use scenario)	A short summary of the Processing activity and the context of the Processing activity, including the relationship between the Controller and the Consumers whose Personal Data will be Processed, and the reasonable expectations of those Consumers
VII Benefits	The core purposes of the Processing activity, as well as other benefits of the Processing that may flow, directly and indirectly to the Controller, Consumer, other expected stakeholders, and the public.
VIII Data Involved (is any sensitive data included)	The categories of Personal Data to be Processed and whether they include Sensitive Data, including Personal Data from a known Child.
IX Nature and Operational Elements of the Processing Activity	In determining the level of detail and specificity to provide, the Controller must consider the type, amount, and sensitivity of Personal Data Processed, the impacts that operational elements will have on the level of risk presented by the Processing activity, and any relevant unique relationships. Relevant operational details may include: a. Sources of Personal Data; b. Technology or Processors to be used; c. Names or categories of Personal Data recipients, including Third Parties, Affiliates, and Processors that will have access to the Personal Data, the processing purpose for which the Personal Data will be provided to those recipients, and categorical processes that the Controller uses to evaluate that type of recipient; d. Operational details about the Processing, including planned processes for Personal Data collection, use, storage, retention, and sharing e. Specific types of Personal Data to be processed

X Sensitive Data	The details of the process implemented to ensure that Sensitive Data and Sensitive Data Inferences are not transferred and are deleted within 12 hours of the Processing activity.
XI Profiling	If a Controller is Processing Personal Data for Profiling, a DPA of that Processing activity must include the following: 1. The specific types of Personal Data that were or will be used in the Profiling or decision-making process 2. The decision to be made using Profiling 3. The benefits of automated processing over manual processing for the stated purpose 4. A plain language explanation of why the Profiling directly and reasonably relates to the Controller's goods and services 5. An explanation of the training data and logic used to create the Profiling system, including any statistics used in the analysis, either created by the Controller or provided by a Third Party which created the applicable Profiling system or software; 6. If the Profiling is conducted by the Third-Party software purchased by the Controller, the name of the software and copies of any internal or external evaluations sufficient to show the accuracy and reliability of the software where relevant to the risks described below 7. A plain language description of the outputs secured from the Profiling process 8. A plain language description of how the outputs from the Profiling process are or will be used, including whether and how they are used to make a decision to provide or deny or substantially contribute to the provision or denial of financial or lending services, housing, insurance, education, enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services 9. If there is human involvement in the Profiling process, the degree and details of any human involvement 10. How the Profiling system is evaluated for fairness and disparate impact, and the results of any such evaluation .
XII Other Governance Requirement Byproducts	**Over and above the requirements in the DPA relating to Profiling, since the Colorado Rules refer to terms/issues that are not defined, such as "Test for fairness, negative inferences, adversarial use/attacks, unconscionable treatment, creation of anxiety, embarrassment, fear or other mental trauma, over collection, surveillance or use beyond what a reasonable consumer would expect," the following DPA topics also should be considered. These topics lead to the need to create governance/control processes and questions that would appear in the functional part of a PIA. Question themes found in an Artificial Intelligence Assessment (AIA), which includes**

	Profiling, are set forth below. Examples of questions are in an AIA can be found here.
XIIa Lifecycle	The project plan should account for each stage of the Model lifecycle: Plan and Design Model, Collect and Process Data, Build and Use Model, Verify and Validate Model, Deploy and Use Model, Operate and Monitor Model, Assess Impacts of Model
XIIb Fairness	The term "fairness" has been described, and steps are in place to measure and test for achieving fairness.
XIIc Traceability	Traceability can be maintained across data, experiments, model versions and usage. Performance can be captured against success criteria.
XIId Training	The quality of training data has been assessed. There were enough total training samples? The samples were representative of different social groups based on – race, gender, color, age, income, etc.
XIIe Model Testing	The performance of the model was tested. The model was well-trained and analyzed through different metrics – Precision, Recall, F1Score, Accuracy, Bias, Robustness & Sensitivity training, etc.
XIIf Equal treatment	All users are treated equally. If not – and your algorithms and predictive technologies prioritize certain information or sets prices or access differently for different users – describe, how would you handle consumer/user demands or government regulations or contractual requirements that require all users be treated equally, or at least transparently unequally. The criteria for conducting Bias Audits under the Final Rule implementing New York City Local Law 144 may be helpful in determining whether a decision or other action is discriminatory.
XIIg Third Parties	If your organization obtained models or datasets from a third party, describe how the risks of using third parties are assessed and managed and what the documentation requirements of using the third parties are.
XIIh End user	Describe how end-users or other subjects are made aware adequately that a decision, content, advice, or outcome is the result of an algorithmic decision?
XIII Other Governance Requirements	In addition to the DPA for Profiling, the Colorado Rules also contain requirements regarding transparency, opting out, and consent. Describe the additional governance processes put in place to address these additional requirements.

XIIIa Governance Controls	Describe the governance controls in place that will enable a consistent, robust, repeatable development/implementation process. Describe how all project team members' roles have been established and communicated.
XIV Impact Analysis **A The DPA must involve all relevant internal actors from across the Controller's organizational structure and, where appropriate, relevant external parties, to identify, assess and address the data protection risks to consumers.** 	Describe how the benefits of the Processing outweigh the risks as mitigated by the safeguards. This description includes the sources and nature of risks to the rights of Consumers associated with the Processing activity posed by the Processing activity. The source and nature of the risks may differ based on the Processing activity and type of Personal Data processed. Risks to the rights of Consumers that a Controller may consider in a DPA include, for example, risks of: a. Constitutional harms, such as speech harms or associational harms; b. Intellectual privacy harms, such as the creation of negative inferences about an individual based on what an individual reads, learns, or debates; c. Data security harms, such as unauthorized access or adversarial use; d. Discrimination harms, such as a violation of federal antidiscrimination laws or antidiscrimination laws or any state or political subdivision thereof, or unlawful disparate impact; e. Unfair, unconscionable, or deceptive treatment; f. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services. g. Financial injury or economic harm; h. Physical injury, harassment, or threat to an individual or property; i. Privacy harms, such as physical or other intrusion upon the solitude or seclusion of the private affairs or concerns of Consumers, stigmatization or reputational injury; j. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or k. Other detrimental or negative consequences that affect an individual's private life, private affairs, private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that Personal Data or other data will not be collected, observed, or used. l. Inconvenience or expenditure of time m. Disruption and intrusion from unwanted commercial communications or contacts n. Loss of autonomy through acts or practices that are not reasonably foreseeable by an individual and that are intended to materially: I. Alter that individual's experiences

	II. Limit that individual's choices III. Influence that individual's responses, or IV. Predetermine results or outcomes for that individual	
B Risks to Society/Large Groups of Individuals	• Overuse of technology (e.g., TikTok by teenagers) • Utilization of Disinformation and Propaganda • Economic and Asset Inequalities - Who will and won't have access to technology • Utilization of technology by Surveillance State • Utilization of online tools by Hateful and Criminal Actors • Algorithmic bias in technology • Who controls consumer data and who monetizes it • Loss of consumer trust	
Stakeholders (examples shown – not complete)	**Benefits/Interests**	**Risks/Harms**
Individual 		
Groups Of Individuals 		
Society 		
Organization: 		

Other		
Other		

XV Additional Mitigators

a. The use of De-identified Data; b. Measures taken pursuant to the Controller duties, including an overview of data security practices the Controller has implemented, any data security assessments that have been completed, and any measures taken to comply with the consent requirements of the Colorado Rules; c. Measures taken to ensure that Consumers have access to the rights provided in the Colorado Rules; d. Contractual agreements in place to ensure that Personal Data in the possession of a Processor or other Third Party remains secure; or **e.** *Any other practices, policies, or trainings intended to mitigate Processing risks.*

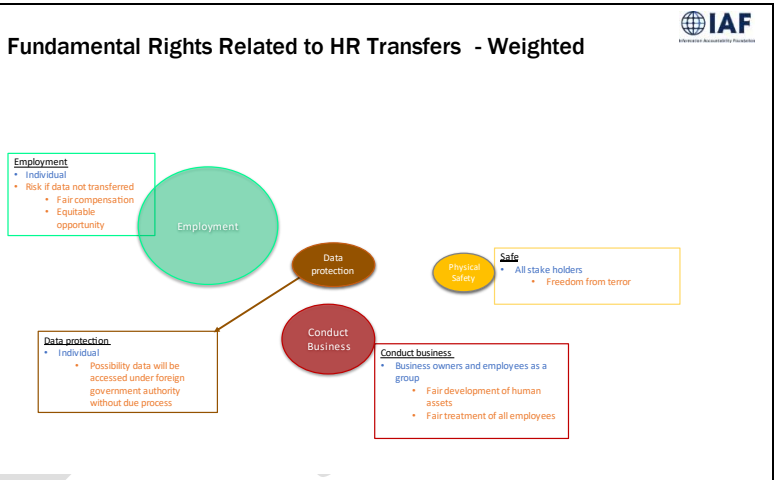
If Profiling is being assessed, safeguards used to reduce the risk of harms identified and safeguards for any data sets produced by or derived from the Profiling must be assessed. Include a description of any other practices, policies, or trainings intended to mitigate Processing risks

XVI Summary of Weighted Balance (Include Heat Maps or other "Weighing" criteria)

A description of how the benefits of the Processing outweigh the risks identified, as mitigated by the safeguards identified.

DPAs MUST IDENTIFY AND **WEIGH** THE BENEFITS THAT MAY FLOW, DIRECTLY AND INDIRECTLY, FROM THE PROCESSING TO THE CONTROLLER, THE CONSUMER, OTHER STAKEHOLDERS, AND THE PUBLIC AGAINST THE POTENTIAL RISKS TO THE RIGHTS OF THE CONSUMER ASSOCIATED WITH THE PROCESSING, AS MITIGATED BY SAFEGUARDS THAT THE CONTROLLER CAN EMPLOY TO REDUCE THE RISKS. THE CONTROLLER MUST FACTOR INTO THIS DPA THE USE OF DE-IDENTIFIED DATA AND THE REASONABLE EXPECTATIONS OF CONSUMERS, AS WELL AS THE CONTEXT OF THE PROCESSING AND THE RELATIONSHIP BETWEEN THE CONTROLLER AND THE CONSUMER WHOSE PERSONAL DATA WILL BE PROCESSED.

Two examples of Multi Dimensional/Stakeholder Balancing Output – one with a math determined balancing (weighing) and one visual depiction of the balancing.	



XVII Decision – Go /No-Go (Approver)

How effective are the mechanisms that facilitate the Processing activity auditability (e.g., traceability of the development process, the sourcing of training data and the logging of the Processing system's processes, outcomes, positive and negative impact)? Could the AI system be audited by independent third parties?
What are the additional requirements surrounding the Processing activity? Are there other legal, cross-border, policy, contractual, industry or other obligations linked to the collection, analysis, and use(s) of data? Have these all been addressed?
If the Processing involves Profiling, does the assessment effectively address the reasonably foreseeable risk of: Unfair or deceptive treatment of, or unlawful disparate impact on Consumers; 2. Financial or physical injury to Consumers; 3. A physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of Consumers if the intrusion would be offensive to a reasonable person; or 4. Other substantial injury to Consumers.
Is it foreseeable that the potential application of Profiling might seem surprising, inappropriate or discriminatory or might be considered offensive causing distress or humiliation?

How effective are the overall controls and safeguards in reducing risk?
Decision – Do benefits and mitigated risks support proceeding with the processing activity? Are there any other factors that should be considered? Have the interests, expectations and rights of stakeholders been effectively addressed. Are potential risks to Consumers sufficiently mitigated??
If the Attorney General requested a copy of the DPA, is the organisation comfortable in sharing?
XVIII Signatories **Names, Titles, and Signatures of all Decision Makers:** **Relevant internal actors and external parties contributing to the DPA:** **Any internal or external audit conducted in relation to the DPA, including the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process:** **Dates the DPA was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval of the DPA:**

XIX Assumptions/Caveats/Implications

- The organization has in place a privacy impact assessment (PIA) process that helps the organization determine whether the requirements in the Colorado Rules (e.g., Transparency, Consent, Access, Portability) have been met.
- The DPA required by the Colorado Rules will be added to the organization's already existing PIA.
- Organizations will use a set of "triggering" questions to determine if a DPA, including for Profiling will be needed. Practically speaking, ALL projects will likely have to go through an initial risk assessment to determine if a DPA will likely be required. This process reinforces the likelihood of having to design an iterative, multistage assessment more aligned with an AI development lifecycle.
- Capitalized terms used in the DPA and the DPA for Profiling have the meaning given them in the Colorado Revised Statutes and the Code of Colorado Regulations.
- Most of the IAF's listed adverse impacts are contained in the Colorado Rules. Those that are not, are listed in red.
- The explicit, implied aspects of the law and regulations coupled with issues that are not defined suggest the need for enhanced governance controls processes. Many of these are more associated with Responsible AI governance.

- Since the Attorney General can ask for any DPA, it is likely the AG's office would ask for details on processes and controls associated with key mitigators. Therefore, a demonstrable governance program, likely including new elements should be considered, and in some cases, the Colorado Rules so require.

XX Definitions and Context

XXa Sensitive Data/Data Use - *Sensitive categories of data and/or use include Information associated with personal data that is used to decision 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 or be considered sensitive to the individual whose data it is.*

XXb Benefits – Determine and describe:

What are the benefits to the defined impacted other stakeholders? Could the use of this data be used in a way that may result in a specific stakeholder or group of stakeholders being treated differently in a positive way from other groups of individuals? Can the benefits obtained by various stakeholders be measured? Determine and describe the positive impacts on the various stakeholders that are expected to come from the application of this technology/data activity. Determine what the potential positive goal of the difference in treatment is (if any). Are areas of interest such as Integrity of the person, autonomy, respect for private life, liberty and security, or education access affected in a positive way?

Are there benefits for society as a whole? Consider factors such as increased revenue, lower costs, improved efficiency, enhanced employee satisfaction, engagement and productivity, enhanced citizen (or workforce) relationship, enhancement or maintenance of brand or reputation, assurance of compliance, fraud prevention, enhancement or maintenance of cyber or physical security, new or improved public services or citizen 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, innovative ways to conduct research. Do the benefits of having the model and/or data use in production outweigh the costs of maintaining it? Are there any social interests served with the deployment of the Processing activity? How does the Processing activity contribute to or increase well-being? How will the Processing activity contribute to human values?

XXc Risks:

Considering all the factors relating to the data, metric or measure, the likely use, the associated activity, the identifiability and sensitivity of the information and its use, what are the risks (real and/or perceived) to the identified stakeholders/users? Could any metric of measure be used in a

way that makes a decision on a specific user and/or creates a profile on them (real or perceived)? Have all the key factors listed in the Colorado Rules been considered?

Consider the risks or increase in risks (real or perceived) to the identified stakeholder as the information is or may be used. Areas to consider include: real or perception of data about them being used in an impactful way; an impact to their employee relationship, reduced status and/or well-being; financial loss or physical harm/threats; psychological harm; excessive expenditure of time; damage to reputation or embarrassment; shock or surprise at the processing activity or the results of the processing; inappropriate discrimination, the possibility of inappropriate access to or misuse of information by the company, including sensitive 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 the information through a probability-based process, such as a score; who will and who will not have access to this information? Will stakeholders who do not have access to this information suffer a setback compared to those who do? What does that setback look like? What new differences will there be between the "haves" and the "have-nots" of this information?

What factors about the activity have the highest impact on the likelihood any of these risks could be realized?

XXd Additional Mitigators:

Are there technical and/or procedural safeguards (mitigating controls) that could be implemented to prevent and mitigate risks should they occur (e.g., increased transparency, additional suggestions/guidance to the customer, more choice, etc.)?