DATA INNOVATION RISK ASSESSMENT TOOL

Part 4: Communication about your project

4.1 Transparency

Transparency is a key factor in helping to ensure accountability, and is generally encouraged. Transparency can be achieved via communication about your project (including providing adequate notice about the data use, as well as the principles and policies governing the data use). Making the outcomes of your data innovation project public can also be important for innovation.

Note, that making data (produced as an output of your project) open is an element of transparency. If you decide to make a data set open, you must conduct a separate assessment of risks, harms and benefits. In this case, you may also want to provide transparent notices on the process and applicable procedures for making the data set open.

Did or will you communicate about the data use (publicly or to other appropriate stakeholders)?

- ☐ Yes
- ☐ No
- ☐ Don't Know
- ☐ Not Applicable

Comments:

4.2 Level of transparency

Being transparent about data use (e.g., publishing data sets, publishing an organization's data use practices, publishing the results of a data project, etc.) is generally encouraged when the benefits of being transparent are higher than the risks and possible harms. Also note, that level of detail (e.g., the level of aggregation) in a data set that is being made open should be determined after a proper assessment of risks and harms.

Particular attention should be paid to whether, for example, publishing non-sensitive details about a project or making non-identifiable datasets open can cause a mosaic effect with another open datasets. Accidental data linking or mosaic effect can make an individual(s) or group(s) of individuals identifiable or visible, thus exposing the individual(s) or group(s) of individuals to potential risks of harms.

Are there any risks and harms associated with the publication of the collected data or resulting reports and are they proportionately high compared to the benefits?

- ☐ Yes
- ☐ No
- ☐ Don't Know
- ☐ Not Applicable

Comments:

Part 5: Third Parties

5.1 Due diligence in selecting partner third parties (e.g., research partners and service providers, including cloud computing providers, etc.).

Frequently, data related initiatives require collaboration with third parties-data providers (to obtain data); data analytics companies (to assist with data analysis); and cloud or hosting companies (for computing and storage). It is therefore important that such potential collaborators are carefully chosen, through a proper due diligence vetting process that also includes minimum check points for data protection compliance, the presence of privacy policies, and fair and transparent data-related activities.

It is also important to ensure that third party collaborators are bound by necessary legal terms relating to data protection. These may include: non-disclosure agreements and other agreements containing appropriate terms on data handling; data incident history; adequate insurance, data transfer and data security conditions among other matters.

Cloud hosting. Many projects may use cloud or other hosting services, meaning that your organization does not maintain security of the hardware. It is important to ensure that your chosen cloud or hosting provider, and the data center in which they operate, have appropriate standards of security. Security certifications could be good evidence of your cloud provider's security compliance. When considering cloud storage and computing, take into account where the data will be actually located to understand potential vulnerabilities, compliance with laws, the special status of an implementing organization, including their privileges and immunities, where applicable, or rules concerning trans-border data flows.