Is your use of the data compliant with (a) applicable laws and (b) the terms under which you obtained the data?

□ Yes
□ No
□ Don’t Know
□ Not Applicable

Comments:

3.5 Data quality

Data experts as well as domain experts should be consulted, if necessary, to determine the relevance and quality of data sets. Data accuracy must be checked for biases to avoid any adverse effects, including giving rise to unlawful and arbitrary discrimination.

Is your data adequate, accurate, up to date, reliable and relevant to the purpose of the project?

□ Yes
□ No
□ Don't Know
□ Not Applicable

Comments:

3.6 Data Security

Taking into account the available technology, cost of implementation and data type, robust technical, organizational safeguards and procedures, including efficient monitoring of data access and data breach notification procedures, should be implemented to prevent any unauthorized use, disclosure or breach of data. Embedding principles of privacy by design and employing privacy enhancing technologies during every stage of the data life cycle is recommended as a measure to ensure robust data protection. Note that proper security is necessary in every stage of your data use.

In considering security, special attention should be paid when data analysis is outsourced to subcontractors. Data access should be limited to authorized personnel, based on the need-to-know principle. Personnel should undergo regular and systematic data privacy and data security trainings. Prior to data use, the vulnerabilities of the security system (including data storage, way of transfer etc.) should be assessed.

When considering the vulnerability of your security, consider the factors that can help you identify "weaknesses" - such as intentional or unintentional unauthorized data leakage: (a) by a member of the project team; (b) by known third parties who have requested or may have access, or may be motivated to get access to misuse the data and information; or (c) by unknown third parties (e.g., due to the data or information release or publication strategy).

It is generally encouraged that personal data should be de-identified, where practically possible, including using such methods as aggregation, pseudonymization or masking, to help minimize any potential risks to privacy. To minimize the possibility of re-identification, de-identified data should not be analyzed or otherwise used by the same individuals who originally de-identified the data.
It is important to ensure that the measures taken to protect the data do not compromise the data quality, including its accuracy and overall value for the intended use.

Have you employed appropriate and reasonable technical and administrative safeguards (e.g. strong security procedures, vulnerability assessments, encryption, de-identification of data, retention policies, confidentiality/non-disclosure, data handling agreements) to protect your data from intentional or unintentional disclosure, leakage or misuse?

□ Yes
□ No
□ Don't Know
□ Not Applicable

Comments: