DATA CONSIDERATIONS				
Sustainable growth & development	*Purpose & fairness*	*Transparency & explainability*	*Security & safety*	*Assurance & accountability*
Engage in activities that can contribute to inducing inclusive growth, sustainable development, and wellbeing.	*Respect the rule of law, human rights, and democratic values throughout data lifecycle activities,*	*Commit to responsible disclosures to provide information to foster stakeholders' understanding of data use.*	*Ensure traceability and apply systematic risk management approaches to mitigate, among others, safety and security risks.*	*Be accountable for the proper functioning of data systems and for the respect of data roles and the data context.*
• Consolidate research networks and collaborative platforms for data reduction. • Enable, guide, and foster access to, use and re-use of, data and evidence. • Reduce the potential environmental impact of data infrastructure. • Avoid the proliferation of unnecessary, redundant, or overlapping datasets. • Manage and reduce dark data volume. • Monitor and control the quality, suitability, sustainability, and impartiality of data	• Conduct human rights impact assessments, where appropriate, to analyse effects of data input activities on rights-holders. • Employ initiatives to reduce bias that may feature in data. • Protect privacy over data lifecycle. • Ensure the availability of diverse teams collaborating around data projects to help mitigate biases. • Publish data governance and management policies, practices, and procedures.	• Disclose information about historical and future use of data. • Involve expected data users to allow adjustments to data needs for successful scaling of data projects. • Reuse data based on assessment of existing data assets to increase efficiency over time. • Gather and record information on data system(s) functioning over time for evaluation. • Assess quality of data inputs.	• Maintain records of data characteristics for traceability. • Adopt and uniformly apply standards, guidelines, codes for data procurement. • Perform regular and random data audits to assess data input quality and if data is fit for purpose. • Identify and assess data risks through risk management approaches. • Communicate residual risks, data accuracy, & serious data incidents.	• Adopt clear terms of who should be held responsible for data and in which circumstances. • Establish a system for "check and balances" of decisions on spending on data and related technologies. • Establish independent oversight bodies to audit the use of data and data practices. • Use tools and processes to document data system decisions and to ensure accountability. • Establish codes of ethical conduct and

inputs by defining and deploying data management rules and practices. • Deploy communication tools to help facilitate engagement of appropriate stakeholders, or representatives, as and when appropriate.	• Be user-driven and place users' needs and their concerns at the core of data project design, implementation, and monitoring. • Communicate to relevant stakeholders, or representatives, about the use of data and its focal purpose. • Protect privacy of legacy data. • Protect right to freedom of expression, association, and personal autonomy. • Avoid the emergence of new forms of "digital exclusion" in the workplace, communities, and society. • Protect whistle-blowers reporting wrongdoing.	• Define a formal process for relevant parties to challenge the use of data. • Be transparent, open, and clear about data inputs and machine / human processes that led to final decisions. • Ensure the processing of personal, personal sensitive or community data by third parties in the context of public-private partnerships is transparent and comply with and adhere to applicable policy and legislation.	• Establish compliance measures where appropriate. • Agree on trustworthy data management practices across departments. • Identify user, intended data use and reasonably foreseeable data misuse (hazard identification). • Adopt impact mitigation planning (IMP) for social & environment impacts. • Track efforts to reduce and address risk(s) from data use. • Manage digital security risks and the safety of connected products and services.	practical technical tools for data use. • Acknowledge that the type and use-context of data determine the relevant principles, rules and norms bearing on its use. • In the case of a negative outcome, take action to ensure a better future outcome. • Articulate the value proposition for all data projects, above a certain size. • Understand potential sanctions to intended or unintended data abuse and mismanagement. • Create safe havens for reporting data misuse, negative outcomes, and early warnings.

SOURCE: Author created. The data considerations are adapted from the following source documents: OECD, "Good Practice Principles for Data Ethics in the Public Sector", (2020); OECD, "The State of Implementation of the OECD AI Principles Four Years On", October (2023); OECD, "Common Guideposts to Promote Interoperability in AI Risk Management", November (2023); and OECD, "Recommendation of the Council on Digital Government Strategies", (2014), respectively.