



Guide to data practices

Foundations for an open,
trustworthy data ecosystem.



The data practices

This guide is an introduction to a set of data practices devised by the ODI. We believe that these practices should underpin the collection, use and sharing of data.

In the first instance, we have looked at how these practices can help organisations become **more trustworthy**. Trust is an essential foundation for a strong data ecosystem. Without it, it is impossible to create the conditions for data collection, use and sharing that deliver social, economic and environmental value.

The practices have been designed to:

- Fill the gap between strategic aims and the real world data collection, use and sharing.
- Complement – not duplicate – what others are doing in the data assurance market.
- Be understood by everyone, enabling them to describe what data practices ‘look like’ for them.



Why we need common data practices

There are many frameworks that seek to stratify the components of good data infrastructure. The majority of these are focused on considering the technical implementation and measurement of data activities.

We believe that there is a significant gap between these technical aspects and the strategic business environment of an open, trustworthy data ecosystem.

The data practices devised by the ODI – and set out in this document – are designed to fill the gap. They build on the ODI’s previous work in data assurance and more than ten years of research.

“The process or set of processes that increase confidence that data will meet a specific need, and that organisations collecting, accessing, using and sharing data are doing so in trustworthy ways.”

– **The ODI definition of data assurance**

We welcome ideas and input from those with an interest in the data practices. Please send your feedback to dataassurance@theodi.org.

Developing the data practices

- The ODI's founding mission is to build an open, trustworthy data ecosystem. The data practices define what we believe is the best foundation for this ecosystem.
- The ODI has researched data ecosystems for more than ten years. The data practices pull together all the insights and learning from that work into an organised structure. They are the factors that we conclude are most commonly present in ecosystems – and organisations – that demonstrate best practices with data.
- We are initially using the data practices to look at organisations' trustworthiness. Trust is a key element within the ODI Strategy 2023–28. In principle 3 we say that “for data to work for everyone it needs to work across borders – geographic, organisational, cultural and political. For this to happen... there needs to be trust – trust in data and trust in those who share it.”
- While our starting point was an attempt to define the features of an open, trustworthy data ecosystem, we believe that these features also need to be present in the organisations – and amongst individuals – that exist in that ecosystem. So our work progressed to what we hope is a useful framework of practices against which organisations can evaluate themselves.
- We intend the framework to provide a bridge between the strategic articulations of best practice in the data ecosystem, and the embedding of important, core activities.



Helping leaders understand nine key organisational data practices.

Accountability

Open and transparent oversight and accountability structures with clear roles and responsibilities for data.

Privacy

Open and transparent processes for handling and sharing personal information legally.

Security

Open and transparent processes for handling and sharing information securely.

Standardisation

Open and transparent processes outlining why and how data is collected, used and shared.

Resourcing

Open and transparent plans and funding for the ongoing management and maintenance of data.

Capability

Open and transparent ability to implement data processes, including both technological and human.

Engagement

Open and transparent approaches to engagement and participation with data providers and users.

Ethics

Open and transparent processes that outline how data is handled in accordance with a defined ethical framework.

Permissions

Open and transparent processes for managing the permissions under which data is consumed and shared.

Accountability

Open and transparent oversight and accountability structures with clear roles and responsibilities for data.

Definition

“The fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens.”

When considering whether they are practiced in accountability, C-Suite leaders might ask themselves:

How can I show that my organisation recognises the importance of data?

Accountability indicators

- There are named data steward roles and people.
- Data accountabilities are identified in all job descriptions and personal and corporate objectives.
- Data collection, use and sharing decision-making processes are in place.
- There is a data issue escalation path to accountable leaders.
- The organisation has a clear data strategy.

Privacy

Open and transparent processes for handling and sharing personal information legally.

Definition

“Someone’s right to keep their personal matters and relationships secret.”

When considering whether they are practiced in privacy, C-Suite leaders might ask themselves:

How can I show that my company understands the law around privacy and personal data?

Privacy indicators

- A data protection role is identified and filled, with clear accountabilities.
- Appropriate training is given on privacy laws.
- Data collection, use and sharing processes contain privacy considerations.
- The organisation clearly complies with the law and regulations.
- Data is classified as potentially containing personal information.
- There is a clear process for responding to privacy enquiries.

Security

Open and transparent processes for handling and sharing information securely.

Definition

“Protection of a person, building, organisation, or country against threats such as crime or attacks by foreign countries.”

When considering whether they are practiced in security, C-Suite leaders might ask themselves:

How can I show that my company understands how to handle data securely when it is being collected, used and shared?

Security indicators

- A data security role is identified and filled, with clear accountabilities.
- Data collection, use and sharing processes contain security considerations
 - And clearly comply with the law and regulations.
- The organisation has undertaken and passed a formal assessment, for example, Cyber Essentials.
- The technology used by the organisation is compliant with security requirements:
 - Encryption
 - Access controls
 - Data loss prevention software
- A process is in place for identifying data security incidents.
- Procedures are in place for secure transfer of data where required.

Standardisation

Open and transparent processes outlining why and how data is collected, used and shared.

Definition

“The process of making things of the same type all have the same basic features.”

When considering whether they are practiced in standardisation, C-Suite leaders might ask themselves:

How can I show that my company has a structured approach to the data that it collects, uses and shares and we understand what it is suitable to be used for?

Standardisation indicators

- The organisation has data quality standards for key data and data is measured against them, including:
 - Completeness
 - Timeliness
 - Consistency
 - Validity
 - Accuracy
 - Resolution
- The organisation provides metadata with information about how data has been created or collected to an appropriate standard.
- It operates and maintains appropriate data management software and tools.
- There is transparency around how data is processed (for example, algorithms, models used).
- There are processes for archiving and deleting data.

Resourcing

Open and transparent plans and funding for the ongoing management and maintenance of data.

Definition

“Resourcing is the process of giving money, workers, skills, etc., to a particular job or piece of work.”

When considering whether they are practiced in resourcing, C-Suite leaders might ask themselves:

Do we have a budget or funding for the ongoing management, maintenance and sharing of data?

Resourcing indicators

- There is a budget in place for data-related activities – collection use and sharing – and services.
- There is a process in place for identifying and mitigating financial risks.
- The organisation has a strategic business plan for future data management requirements.
- There is a commitment to funding in the long term.

Capability

Open and transparent ability to implement data processes, including both technological and human.

Definition

“The ability to do something.”

When considering whether they are practiced in capability, C-Suite leaders might ask themselves:

How can I ensure that my organisation has the necessary tools, and our employees have the skills to collect, use and manage data in a trustworthy manner?

Capability indicators

- The organisation makes data requirements part of all job descriptions, appropriate to the specific role.
- There is an understanding of skills gaps in the organisation, and a plan for ensuring that they are being met – through a programme of continuous development.
- A training programme is in place, and skills are regularly updated to ensure people and processes remain relevant.

Engagement

Open and transparent approaches to engagement and participation with data providers and users.

Definition

“The process of encouraging people to be interested in the work of an organisation, etc.”

When considering whether they are practiced in engagement, C-Suite leaders might ask themselves:

How can I ensure that internal and external stakeholders understand and have a chance to contribute ideas to the ways we operate with data?

Engagement indicators

- The organisation has a good understanding – and documentation – of stakeholders for key data including:
 - Employees
 - Customers
 - Suppliers
 - Partners
- It gathers views from its stakeholders to understand their data needs and concerns.
- The organisation has clear routes for reaching and engaging with data owners/suppliers – to ensure they know how their data is being used.
- It maintains clear and understandable documentation about its data practices.

Ethics

Open and transparent processes that outline how data is handled in accordance with a defined ethical framework.

Definition

“The study of what is morally right and wrong, or a set of beliefs about what is morally right and wrong.”

When considering whether they are practiced in ethics, C-Suite leaders might ask themselves:

How can I show that in addition to complying with the law my company takes the ethical use of data seriously?

Ethics indicators

- The organisation has a published ethical use of data statement.
- It has processes in place to understand, assess, manage and mitigate ethical considerations around data collection, use and sharing in line with that statement.
- The organisation has resources and training available for staff to help them understand ethical data use.
- It has clear escalation routes for decision-making around ethical data use.

Permissions

Open and transparent processes for managing the permissions under which data is consumed and shared.

Definition

“The act of allowing someone to do something, or of allowing something to happen.”

When considering whether they are practiced in permissions, C-Suite leaders might ask themselves:

How can I make sure that when we acquire data from – or share it with – others we all understand what we can and cannot do?

Permissions indicators

- The organisation has a clear and transparent approach to data licensing.
- It has a standard, and documented approach for responding to requests for data.
- Clear and readable licence terms and permissions are provided alongside data.
- The organisation has a risk assessment process for permission to collect, use and share data that is well documented and available.
- It has a clear understanding of the legal ownership of the data it is collecting, using and sharing.
- It has appropriate legal and licensing support.

Now, improve your data practices...

Being a ‘responsible steward of consumer data is a strategic necessity for building an effective business in the digital era’.*

The nine data practices provide a framework for organisations to demonstrate the trustworthiness of their data practices.

Our new tools, the Data Practices Assessment Tool and Data Sharing Risk Assessment, will help organisations to evaluate data practices and unlock value.

But we want to go further. Help us continue to improve these tools so they work best for organisations.

Get in touch with us at dataassurance@theodi.org to get involved.

*Forbes, (2023), ‘[Ethical Marketing Innovation in The Age of AI and Big Data](#)’.



More information about how the ODI can support your data needs:

- Consulting services
- Research and policy
- Membership
- Training

Open Data Institute

Kings Place
90 York Way
London N1 9AG
United Kingdom

info@theodi.org

+44 (0)20 3598 9395

