ODI

OPEN FOR FEEDBACK

Designing trustworthy data institutions

Open Data Institute

Contents

About

This report has been researched and produced by the Open Data Institute, and was published in April 2020. The lead authors are Rachel Wilson and Olivier Thereaux, with contributions from Sonia Duarte, Renate Samson, Jared Robert Keller, Jack Hardinges and Jeni Tennison.

If you would like to send us feedback, please get in contact with us at research@theodi.org.

OPEN FOR FEEDBACK

How can it be improved? We welcome suggestions from the community in the comments.

Executive summary

In spring 2019, the Open Data Institute (ODI) released pilot reports concluding that data trusts – new organisational structures providing independent stewardship of data – could be useful in increasing access to data while retaining trust. Data trusts are one example of a broader range of data institutions.

Data institutions are organisations whose purpose involves stewarding data on behalf of others, often towards public, educational or charitable aims. For these institutions to achieve this purpose, they need to be both trustworthy and trusted. Some data institutions, however well intentioned, could fail to operate in an effective and trustworthy way, possibly causing harm. In addition, data contributors and other stakeholders need to assess whether they should work with a particular data institution or not.

There are some things that a data institution *must* do, for example to comply with laws and regulations, but there are others that, while not mandated, will help a data institution build and maintain trust.

A trust framework, combined with an understanding of the ecosystem of trust surrounding a typical data institution, can give a clear understanding of what is expected of a data institution, and what mechanisms are available to assess and to demonstrate its trustworthiness.

Many mechanisms and tools are available for data institutions to adopt. And much that is needed to design a trustworthy data institution can be derived from exemplars in organisational design and governance elsewhere. Other mechanisms, such as certification programmes for data institutions, need to be developed, tested and integrated in the ecosystem.

This exploratory research from the ODI ran in parallel to a related project on designing *sustainable* data institutions[1]. Both projects have highlighted that trust and sustainability are deeply connected, requiring strong governance and ongoing community engagement. This report does not presume to have all the answers to what makes a *good* data institution, but it provides a way of thinking that will both guide new data institutions, and form a basis for future work in this field.

[1] Open Data Institute (2020), 'Sustainable data institutions', https://theodi.org/project/sustainable-data-institutions

Introduction

Data stewardship involves collecting, maintaining and sharing data, and, in particular, determining who has access to it, for what purpose and to whose benefit.

How data is stewarded is important, as it affects what it can be used for and how it may bring benefit or cause harm. Data institutions are organisations whose purpose involves stewarding data on behalf of others, often towards public, educational or charitable aims. At the ODI, we have been exploring the role of data institutions in increasing access to data.

Data trusts are one type of data institution. They provide independent, fiduciary stewardship of data.[2] With data trusts, one party authorises another to make decisions about data on their behalf, for the benefit of a wider group of stakeholders. The independent person, group or entity stewarding the data takes on a fiduciary duty, which is considered the highest level of obligation that one party can owe to another.

Some data institutions will follow a similar pattern, whereby an organisation, or group of organisations, entrusts them to share data with others. Other data institutions will play different roles, such as combining or linking data, and providing benchmarks and other insights to the organisations that have contributed to them.

Setting up institutions to steward data can create benefits for organisations, people and communities through data being used more widely. But data contributors need to be able to determine whether they should share data with or through the data institution; data users need to know whether to use data from it; and people, organisations and communities affected by the data institution need to assess whether to support its operation or campaign against it. These judgements rest on the question: is this data institution trustworthy?

To explore this topic, the ODI carried out desk research into trust and trustworthiness, and the ways existing institutions make themselves trustworthy and trusted. We also reviewed and built upon our earlier research on data trusts and data institutions. This was complemented by interviews with representatives from the following data institutions:

- **Higher Education Statistics Agency (HESA)[3]**: an official body which collects, analyses and publishes data about higher education in the UK. HESA collaborates with higher education providers, such as universities, to collect and curate higher education data sources. Its products are used by researchers and policymakers for transparency, retaining public trust and decision making.
- **Research Organization Registry (ROR)[4]**: a community-led project working to produce a unique, open, usable and sustainable identifier for every research organisation in the world.

[2] Open Data Institute (2020), 'Data trusts in 2020', https://theodi.org/article/data-trusts-in-2020/

[3] Higher Education Statistics Agency (n.d.), https://www.hesa.ac.uk/

[4] Research Organization Registry (n.d.), https://ror.org/

- **HiLo Maritime Risk Management**[5]: a not-for-profit joint industry initiative providing analysis of shipping data to make the industry safer. Shipping companies share safety-related data from vessels and HiLo runs it through a risk algorithm, and shares insights with the companies.
- **OpenCorporates**[6]: the world's largest open database of information about companies. All of the data on OpenCorporates comes from primary public sources, and is used by individuals, journalists, non-governmental organisations (NGOs) and companies.
- **MusicBrainz**[7]: a project to create a collaborative database about artists, songs and albums. Any user can contribute and release the music metadata under open licences.

This report presents the results of our initial exploratory research and provides an overview for those designing or running data institutions about what to consider in order to be trustworthy, how to build and maintain trust, and how to avoid potential breakdowns of trust.

We start by introducing a framework that describes how trust tends to operate. Using this framework, we can better understand how different mechanisms for building trust are designed to work and what aspects of trustworthiness and trust they try to address.

We then describe what a data institution will be expected to do to achieve its objectives, that is, what makes it worthy of trust. These are primarily related to processes, capability or legal compliance that are, in the main, directly under the control of the institution itself. We also describe what a data institution can do to demonstrate its trustworthiness to other parties, and how to close the gap between being *trustworthy* and being *trusted*.

There are various legal, procedural and technical mechanisms that can be used to provide assurances of trustworthiness throughout a data institution's lifecycle. We describe some of these mechanisms in this report. Some of these mechanisms are things a data institution *must* do, while others are things a data institution *should* do.

We hope this research will lead to the development of further guidance to support the effective adoption of trustworthy practices by new and existing data institutions, and to demonstrate their trustworthiness to those who want to use their services.

[5] HiLo Maritime Risk Management (n.d.), https://hilomrm.com/
[6] OpenCorporates (n.d.), https://opencorporates.com/
[7] MusicBrainz (n.d.), https://musicbrainz.org/

An ecosystem of trust

“Companies do not exist in isolation. To succeed in the long term, directors and the companies they lead need to build and maintain successful relationships with a wide range of stakeholders.”[8]

Trust is inherently about relationships and communication between people and organisations. There are many actors interacting with a data institution who need to know whether it is trustworthy. A data institution needs to demonstrate its trustworthiness to these different people and organisations, and, in turn, needs to trust those people and organisations.

The role of a data institution will differ depending on its mission; the needs of the ecosystem and community; the number of data contributors and users; the countries it operates in; and the sensitivity of the data being managed.[9]

Some data institutions may focus their activities on governing access to data provided by data contributors. But other institutions may be more actively involved across the lifecycle, including collecting, processing, managing and transforming data. These all entail different relationships and commitments.

What is a data institution trusted to do?

The different people, communities and organisations that interact with a data institution will have different expectations of it, depending on the role that they play.

Data contributors (including individuals mentioned in the data if it contains personal data) need to trust the data institution to govern access to the data, such that it is shared and used in accordance with the rules defined by the data institution. This might include taking into account consent and preferences, keeping data secure, safeguarding privacy, protecting the reputation of data contributors, and creating value and impact from the data.

Data users, and the **decision makers** who use the tools and services created from institution-stewarded data, need to trust the data institution to deal with their data-access requests fairly and equitably, and to supply data in a timely and reliable way. They need to trust that the data institution is stewarding the most appropriate data to meet intended uses, in line with the data institution’s purpose, and is being open about its limitations. They also need to trust that the data institution is not going to expose them to legal or reputational risks when it provides them with access to the data.

[8] Financial Reporting Council (2018), ‘UK Corporate Governance Code’, https://www.icaew.com/technical/corporate-governance/codes-and-reports/uk-corporate-governance-code

[9] Open Data Institute (2019), ‘Data trusts: lessons from three pilots’, p48, https://theodi.org/article/odi-data-trusts-report/

Those people, organisations and communities that might be affected by the sharing and use of data need to trust: that the institution will only share data with those who will advance the institution's purpose; and that data is used to benefit them, or at least to do them no harm. They might also trust it to maintain proactive engagement with them, and listen and respond to their views.

Funders tend to support data institutions with the aim of encouraging healthy data ecosystems, pursuing philanthropic goals or as part of performing their public function. Therefore they need to trust the data institution to maximise the economic, societal or environmental value of the data it stewards, as defined by the data institution's purpose.

Data institutions as trust intermediaries

Some of a data institution's trustworthiness will depend on other people and organisations, including data contributors and data users; it is therefore a trust intermediary.

A data institution needs to assess and demonstrate the trustworthiness of one party on behalf of others to be confident that it can be trusted itself, since a failure to do so can affect its own reputation. This is especially important if any parties are legally liable for any negative outcomes or harmful behaviour. A data institution can increase the trustworthiness of these stakeholders in several ways, such as by providing tools and training, or through binding their behaviour through formal contracts.

Data users need to be trusted to accurately declare what they are intending to do with the data and not to cause harm through their use of it. Data users can be monitored to ensure they are keeping to the terms of any data-sharing agreements. This could include assurances that data is only accessed by those authorised to do so; that data is not shared with unauthorised people; and that data is kept secure if it is transferred between sites.

Data contributors, be they organisations or community volunteers,[10] need to be trusted to provide continued access to good quality-data that is of trustworthy provenance and is useful to the purpose of the data institution.

People represented in the data need to trust the data institution – as a representative of the data contributors – to: collect only the required data; hold the data securely; and delete the data when it is no longer needed.

A data institution will often store data and mediate interactions using technology, so it needs to ensure the trustworthiness of its suppliers, technical solutions, products and services – including algorithms[11].

Finally, the people, organisations and communities affected by potential uses of the data need to trust the data institution – as a representative of the data users and decision makers – not to cause them harm.

[10] Open Data Institute (2019), 'Collaborative data patterns', https://collaborative-data.theodi.org
[11] Harvard Data Science Review (2020), 'Should we trust algorithms?', https://hdsr.mitpress.mit.edu/pub/56lnenzj

The external ecosystem

The trust ecosystem also extends to actors beyond the immediate environment of the data institution: this wider ecosystem includes legislators, regulators, oversight bodies, journalists, certifying bodies, insurers, and external bodies offering both oversight and redress[12].

Despite best intentions, sometimes things go wrong. These external bodies provide assurance that data contributors, data users and the people, organisations and communities affected by the use of data will be protected. Trust in the external environment – such as in the effective enforcement of data protection law – gives stakeholders confidence to place trust in a data institution. This is one of the ways that trust can be established even when there is little prior evidence for the behaviour of a data institution, for example when it is newly established.

Assurance might come from an agreement with the data institution, such that it will accept liability or provide redress (see box below), or from the surrounding environment, such as the ability to take legal action to recover costs or reputation. Mechanisms such as relevant insurance policies help to provide assurance that the data institution will be able to satisfy any financial commitments this entails.

Throughout this report, we refer to the actors who interact with data institutions collectively as stakeholders, to differentiate them from communities who may be impacted by the use and sharing of data.

Accountability, liability and redress

An important expectation of a data institution is that it should protect all of its stakeholders from harm. A data institution will be responsible and accountable for incidents, whether harms or errors arise intentionally or unintentionally. This can mean being legally liable or enacting redress mechanisms.

Liability or redress don’t intrinsically make data institutions more trustworthy, but they provide confidence that undesirable or damaging situations will be remedied if trust is misplaced or something goes wrong. That assurance might come from agreements with the data institution that it will accept liability, or from an oversight body or authority that is external to the data institution.

Accountability, liability and redress have different legal definitions:[13]

Accountability means being available to give an account, rationale or explanation for an action or state of affairs. Sources of accountability can be

[12] In ways similar to the Financial Services Compensation Scheme (FSCS) for financial institutions. Financial Services Compensation Scheme (n.d.), https://www.fscs.org.uk/

[13] Cornock M (2011), ‘Legal definitions of responsibility, accountability and liability’, https://www.deepdyve.com/lp/royal-college-of-nursing-rcn/legal-definitions-of-responsibility-accountability-and-liability-zkI79QFMtC

legislative, organisational, contractual or informal.[14] Systems of accountability provide reassurance that the behaviour of an organisation is being monitored and controlled.[15] Such systems must be well designed, so as not to introduce perverse incentives.[16]

When legislation or a contract means that a party is legally answerable to another party, we say they are **liable**. Failure of a person or entity to meet that responsibility can result in a court judgment.

The standard contractual penalty is financial damages. However, there are situations where damages are not sufficient, and it may be necessary to compel or stop a certain action. These are called 'equitable remedies' or '**redress**', and require clauses to be written into contracts or agreements. Redress functions as a restorative force in the ecosystem if something goes wrong, similar to an insurance policy.

Remedies include:

- monetary compensation, similar to contractual damages
- correcting public information, for example, to restore someone's reputation
- deletion of data shared by a data institution
- re-running processes that were affected by procedural flaws or bias.

The ability to seek redress should be easily accessible, responsive, not be unduly expensive or time-consuming, and be understandable. Appropriate redress for those affected by technology-driven harms is still developing. Doteveryone's ongoing research into better online redress has three recommendations that are relevant to data institutions:[17]

- Define meaningful outcomes for redress, where not all harms are financial.
- Develop new structures of redress fit for the scale and pace of online services.
- Make it easier for people to navigate digital complexity.

[14] McGrath S, Whitty J (2018), 'Accountability and responsibility defined', https://www.researchgate.net/publication/324582377_Accountability_and_responsibility_defined

[15] O'Neill O (2018), 'Assessment, public accountability and trust', https://www.cambridgeassessment.org.uk/images/126032-baroness-onora-o-neill.pdf

[16] O'Neill O (2002), 'Reith Lectures 2002: Lecture 3: Called to account', http://downloads.bbc.co.uk/rmhttp/radio4/transcripts/20020417_reith.pdf

[17] Doteveryone (2019), 'Seeking redress in the online world – the current challenges', https://www.doteveryone.org.uk/2019/12/seeking-redress-in-the-online-world-the-current-challenges

Being trustworthy and being trusted

The degree to which we trust a person or organisation determines the agreements we are willing to enter into with them, and how we act and behave towards them.

There are various frameworks for describing trust, trustworthiness and what it means to be trusted. These frameworks attempt to distil trust into a few components like "credibility, reliability, intimacy and self-orientation"[18], "honesty, competence and reliability"[19], or "rigorous logic, authenticity and empathy"[20].

Each trust framework starts from the same premise: that trust involves communicating and meeting expectations. This can be paraphrased as: 'I want to be trusted *to do X*, and I will attempt to demonstrate to others that I am trustworthy. I trust another *to do Y*, and will attempt to assess that my trust is well placed'.

For this report, we have drawn especially on a framework[21] developed by Dr Kieron O'Hara at the University of Southampton. It is a useful basis for our research because it describes trust using components that scale well from interpersonal to institutional contexts, while sidestepping debates about human nature and the role of authorities. [22] The framework also explains how being trustworthy is different from being trusted, and how the two must be aligned to avoid a breakdown of trust, and offers a useful way to reason about where trust can break down.

This section uses the ecosystem of actors introduced in the previous section to summarise and expand on the framework developed by O'Hara. After introducing a number of useful concepts and vocabulary, we examine a range of ways that trust between parties operates and can break down.

As the nature of trust is relational, in this section we have used named people ('Alice' and 'Ben') to help demonstrate the relationships.

A framework for trust

O'Hara's framework for trust starts with the notion of trustworthiness. Within his framework, a person or organisation is **trustworthy** if they do what they have committed to do. More specifically, they are trustworthy if they are **able**, **willing** and

[18] Trusted Advisor (n.d.), 'Understanding the trust equation', https://trustedadvisor.com/why-trust-matters/understanding-trust/understanding-the-trust-equation

[19] O'Neill O, Bardrick J (2017), 'Trust, trustworthiness and transparency', https://www.thebritishacademy.ac.uk/sites/default/files/Trust-Trustworthiness-Transparency.pdf

[20] Frei F (2018), 'How to build (and rebuild) trust', https://www.ted.com/talks/frances_frei_how_to_build_and_rebuild_trus t

[21]O'Hara K (2012), 'A general definition of trust', https://eprints.soton.ac.uk/341800/1/ohara_trust_working_paper_aug_2012.pdf

[22] Mouritz T (2010), 'Comparing the social contracts of Hobbes and Locke', https://www.murdoch.edu.au/School-of-Law/_document/WA-jurist-documents/WAJ_Vol1_2010_Tom-Mouritz---Hobbes-%26-Locke.pdf

motivated to act or behave in such a way that makes good on their commitments. Furthermore, they are able, willing and motivated to behave this way in specific **contexts,** and to the benefit of a particular **audience**, which can include themselves, but will usually be others.

The framework further distinguishes between being *trustworthy* and being *trusted*. The main difference is that **being trusted** is relational and involves an assessment by another party. For example, 'Ben' must believe 'Alice' to be trustworthy before he **places his trust** in her. He must judge Alice's ability, willingness and motivation to do as he expects her to do; the two need a common understanding of the boundaries of the context in which Alice operates and the audience she intends to benefit from her actions; and he needs to correctly interpret all her behaviours as ultimately benefiting that same audience.

If Alice is unable to adequately demonstrate to Ben that she is trustworthy, or if Ben is unable to adequately assess whether Alice can indeed be trusted, then trust might not be given when it is deserved. Or trust might be given when it is not warranted, for instance if Alice is not as trustworthy as she claimed or if Ben doesn't accurately assess her trustworthiness. As we will describe later, trust can also break down after it is given.

Components of trust

O'Hara's framework describes the components of trust; here we summarise how they apply to data institutions.

Ability, willingness and motivation
Alice's ability to do as she claims is fundamental to her trustworthiness. But in order to act, as well as being favourable to an idea, she also needs an intrinsic or extrinsic reason or incentive.[23] For example, if Alice is a medical researcher, she may be *able* and *willing* to share her research findings, but until she is *motivated* by the prospect of collaboration, she will delay doing so.

A data institution's *ability* to steward data on behalf of others depends on its access to technology, resources and funding. It must also be *willing* to steward data on behalf of others, by having it as part of its vision or mission. It may also have a mix of positive and negative *motivations,* such as contributing towards a societal goal, or a legal compulsion.

Context
People are not equally able, willing or motivated in all circumstances. Instead, Alice's context is the specific circumstances in which she claims to be trustworthy, for example teaching mathematics, providing advice during office hours, or carrying out research into heart disease. Context might be extremely precise, such as described in a contract. Or it might be informally assumed through social norms, or have to be clarified over time, for example through case law.

A data institution's context will depend on its role within the ecosystem, the type

[23] Bénabou R, Tirole J (2003), 'Intrinsic and extrinsic motivation', https://www.princeton.edu/~rbenabou/papers/RES2003.pdf

of data, and the domain. It could include aspects of data management, and control of how data is used. The limits and expectations of the circumstances in which a data institution should be trustworthy are broadly defined and still evolving.

Audience
Alice's audience are those who she anticipates will benefit from her trustworthiness. Her promises will sometimes be precisely targeted to certain individuals or groups. At the very least, Alice's audience would reasonably expect not to be harmed as a result of her behaviour.

The target audiences for a data institution's trustworthiness will include all the actors within its ecosystem, as well as those using the insights, products and services that it enables; and people, organisations and communities affected by the sharing and use of the data it stewards. The diversity of these audiences adds complexity to the challenge of being trustworthy and trusted.

Actions, behaviours, claims and commitments
Alice may make claims or commitments about how she is willing, able and motivated to behave to serve the interests of the audience she is targeting. These might be open-ended or quite precise claims.

These claims may be open to interpretation. For example, a data institution may be very precise about the goal it is working towards, but it may give itself leeway in how it achieves this.

As claims become more explicit, they begin to resemble a contract. But it may be that expectations of behaviour are defined by unwritten, implicit social norms; being a 'good steward' implies a lot of things and raises a lot of expectations, but is very open-ended.

A data institution represents itself as being willing, able and motivated to carry out stewardship duties on behalf of others. How it is expected to behave may be defined in contracts, but there will also be an implicit expectation that their operation will not cause harm to their audience.

How trust breaks down

The trust framework outlined above is a useful way of pinpointing and describing the various components of trust and the calculations that often go into determining whether or not a person or organisation can be trusted to do what they have committed themselves to do. Crucially, the framework also offers a means of analysing the different ways that trust can be lost, broken or diminished.

Misrepresentation

It may be that Alice makes a **misrepresentation** (of her ability, willingness, etc). This is where we look for evidence to root out bad actors, dishonesty, incompetence or unreliability. But it might also be that Alice underestimates her own abilities and is more trustworthy than she declares. Whether positive or negative, intentional or unintentional, misrepresentations mean that Ben’s trust in Alice is misaligned with what is warranted.

An example of **misrepresentation** of a data institution’s ability might be if it provides data contributors with assurances about data protection, but does not have good security measures in place, which comes to light when it suffers a data breach.

Misunderstanding

It may be that Alice and Ben have a **misunderstanding**. This arises when there is a failure of communication such that Alice and Ben have different interpretations of the context, audience or expected behaviour. Again, misunderstandings can mean that Ben places the wrong level of trust (too much or too little) in Alice.

A **misunderstanding** of the audience could arise when a data institution claims to have a social benefit purpose, such as improving healthcare, and furthers that purpose by sharing data with private sector organisations, such as pharmaceutical companies. The data institution may see their purpose at a system level, and the development of new drugs as ultimately contributing to better healthcare. But data contributors may have a narrower view, and see companies making profit through using data about them as unacceptable.

Inability to determine

It may be that Ben is **unable to determine** sufficient evidence to decide how much trust to place in Alice. This lack of evidence may raise the risk for Ben, of both misrepresentations and misunderstandings, such that he errs on the side of caution. If Alice is indeed trustworthy, this results in an opportunity cost of not entering into an agreement that could otherwise have been mutually beneficial. It is therefore important for Alice to produce sound evidence of her ability, willingness and motivation (reducing the risk of misrepresentation), and clarity about her context, audience and expected behaviour (reducing the risk of misunderstanding).

A stakeholder might be **unable to determine** how much to trust a data institution if it cannot get access to information about the sources of the data it stewards, or the process through which requests for access are granted.

Failure to communicate changes

It may be that Alice **fails to communicate changes in circumstances**. Her ability may be hindered, or Alice’s context or audience – and therefore behaviour – changes in ways Ben is unaware of or didn’t expect. Ben’s expectations may no longer be aligned with Alice’s reality. It is important that Ben is given the opportunity to re-evaluate how much trust to place in her, and revise any agreements he has entered into with her.

A **failure to communicate a change in circumstances** might arise if a data institution is absorbed into, or spun out of, another organisation and this is not communicated clearly; or if new data contributors or data users enter into agreements with the data institution, particularly if those organisations have poor reputations.

Being trustworthy with data

"The trustworthiness of a data institution is a product of the people, systems and processes that enable and support trustworthy stewardship of data."[24]

Being trustworthy with data is not the same as being trusted with data. When we talk about the trustworthiness of data institutions, we are primarily looking at internal processes, capabilities or legal compliance related to how a data institution will reliably deliver on what it promises.

When we talk about a data institution being trusted, on the other hand, we are looking at what a data institution can do to demonstrate its trustworthiness to other parties, to ensure those parties are able to assess its trustworthiness and so decide whether they can trust it to steward important data.

The following two sections of this report examine these two related topics, starting with how to be trustworthy with data. This section ends with a discussion of things a data institution *should* or *may* do, but we start with what a data institution *must* do in order to be trustworthy with data.

A system of rules

As a foundation, a trustworthy data institution is expected to follow a system of rules. Rules such as laws, regulations or codes of practice define the **behaviours** expected of a data institution. In some cases, the rules stipulate what the data institution is *not* allowed to do. As well as motivating a data institution to act in a trustworthy way, this system of rules provides a base set of criteria that defines what it *means* to be trustworthy with data, against which we can judge whether a data institution has done what it must do.

These rules may be mandated by the data institution's environment, stated by the data institution itself, or may be implicit because of social or industry norms.

Laws and regulations

Laws and regulations define the **behaviours** expected of a data institution by an authorising body. Some laws and regulations are principle based, rather than being proscriptive, and therefore are intended to encourage or stimulate, rather than proscribe. The promise of rewards (such as tax breaks) or the threat of penalties or punishments can increase a data institution's **motivation** to comply.

[24] Paraphrased from UK Statistics Authority (2018), 'Code of Practice for Statistics', https://www.statisticsauthority.gov.uk/code-of-practice

Data institutions should have a good understanding of the duties and powers set out in legislation and regulation, and ensure these are applied in its governance and management. Referring to specific legislation and oversight bodies in terms and conditions, and policy statements both informs stakeholders of their rights, and demonstrates that the data institution is aware of, and is adhering to, legislation. Legislation relevant to data institutions in the UK includes:

- **Data Protection Act 2018:**[25] includes the General Data Protection Regulation (GDPR) and is applicable to a data institution stewarding personal data.
- **Consumer Rights Act 2015:**[26] includes rights for the consumer regarding digital content, including in relation to services provided for free.
- **Equalities Act 2010:**[27] mandates against discriminatory practices so that a data institution provides equal access to users.
- **Protection of Freedoms Act 2012:**[28] relevant to data institutions collecting data such as CCTV footage.
- **Digital Economy Act 2017:**[29] addresses data sharing across government including statistical information and a range of media, internet and mobile phone laws. Outlines some of Ofcom's (Office of Communications) oversight requirements.
- **UK Copyright and Rights in Databases Regulations 1997:**[30] describes intellectual property rights in databases and other content.

Contracts

Legally enforceable contracts help align different parties' expectations in several respects: they define expected **behaviour**, clarify the bounds of the **context** of a data institution, and may specify its **audience**. Contracts greatly reduce the risk that these aspects will be misunderstood by parties. Penalties for breaking the terms of a contract increase a data institution's **motivation** to follow the rules it agreed to.

Penalties

The threat of penalties, sanctions, fines and punishments gives us confidence that a person or organisation will be **motivated** to comply with rules because they will incur a sufficient cost if they do not. It is, however, necessary to trust in the external enforcement system, whether that be legal, regulatory or reputational. Whereas penalties are supposed to dis-incentivise harmful behaviour, redress is designed to provide recompense to any harmed parties. See 'Accountability, liability and redress' above.

Legal agreements and laws define expected behaviour that has the backing of an external enforcement authority. However, there are other voluntary rules defining trustworthy behaviour that have been developed for self-guidance, to meet a need, or that codify community expectations.

[25] UK Parliament (2018), 'Data Protection Act', http://www.legislation.gov.uk/id/ukpga/2018/12
[26] UK Parliament (2015), 'Consumer Rights Act', https://www.legislation.gov.uk/id/ukpga/2015/15
[27] UK Parliament (2010), 'Equalities Act', http://www.legislation.gov.uk/id/ukpga/2010/15
[28] UK Parliament (2012), 'Protection of Freedoms Act', https://www.legislation.gov.uk/id/ukpga/2012/9
[29] UK Parliament (2017), 'Digital Economy Act', https://www.legislation.gov.uk/id/ukpga/2017/30
[30] Cooley Go, 'What you need to know about UK database rights', https://www.cooleygo.com/what-you-need-to-know-about-uk-database-rights

Standards

Standards are documented, reusable agreements that are used for consistency, to enable processes to be replicated, to make comparisons, or to reach a shared understanding.[31] They include technical definitions,[32] data formats,[33] specifications for quality standards and management processes.[34] If we know something complies with a standard, we can be confident how it will **behave**.

In some industries, compliance with some standards will be expected, if not mandated by regulation. In other cases, implementing a standard may be voluntary as a way of improving an internal process, or to make it easier for others to interact.

An accredited body can certify compliance with a standard as a measure of assurance, although it is not always necessary.

Policies, processes, principles and codes

Developing and publishing policies, codes of conduct, or lists of principle or values signal a data institution's **willingness** to **behave** in a particular way. Examples include:

- ORCID's[35] organisational principles set out its ways of working to create a trustworthy, sustainable data infrastructure.
- Council of Europe's 12 Principles of Good Governance[36] describe the responsible conduct of public affairs and management of public resources.
- The Code of Practice for Statistics[37] aims to 'provide the framework to ensure that statistics are trustworthy, good quality and valuable'.
- The Chartered Institute of Auditors' codes of professional conduct and ethics [38] aim to raise the professionalism of internal auditing.

Norms

Norms are implicit or 'unwritten rules' of **behaviour** typically determined by social or cultural convention. Sometimes norms become codified[39] as guidelines, standards or codes, especially in growing communities[40] where new members need to learn the community's norms in order to participate successfully.

Examples of norms include user experience (UX) practices; vocabulary; what is meant by terms like 'respectful' or 'doing the right thing'; and what might be considered proportionate or fair use of data.

[31] Open Data Institute (2018), 'Open standards for data', https://standards.theodi.org

[32] Wikipedia (2020), 'USB standard', https://en.wikipedia.org/wiki/USB

[33] Office for National Statistics (2020), 'Data standards', https://www.ons.gov.uk/aboutus/transparencyandgovernance/datastrategy/datastandards

[34] International Organization for Standardization (2020), 'ISO-27001: Information security management', https://www.iso.org/isoiec-27001-information-security.html

[35] ORCID (2011), 'Our principles', https://orcid.org/about/what-is-orcid/principles

[36] Council of Europe (2020), '12 principles of good governance and ELoGE', https://rm.coe.int/12-principles-brochure-final/1680741931

[37] Office for Statistics Regulation (2018), 'Code of Practice for Statistics', https://www.statisticsauthority.gov.uk/code-of-practice

[38] Chartered Institute of Auditors (2020), 'Our standards and ethics', https://www.iia.org.uk/about-us/our-standards-and-ethics

[39] Kalkman S, et al (2019), 'Responsible data sharing in international health research: a systematic review of principles and norms', https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-019-0359-9

[40] Open Data Commons (2020), 'Community norms', https://opendatacommons.org/norms/odc-by-sa.1.html

Because norms are usually unwritten and can evolve over time, they make it difficult to establish or determine trustworthiness. It is easy to unintentionally make a mistake or misinterpret others, especially for those new to a community or domain. Although the 'penalties' for not following established norms are likely to be social or reputational, rather than legal or financial.

Ethical design

Rules define explicit, externally defined and enforced expectations of a data institution, but many of the expectations of how a data institution should steward data are informal and implicit[41]. The rapidly changing context in which a data institution operates – in particular with regard to increasing capability of technology, availability of data, and awareness of potential harms caused by data misuse – makes it hard to determine fixed rules.

Just as the rules and regulations recommend that organisations working with data should build in privacy and security by design,[42] data ethics should be built in by design into every organisation stewarding data, typically through the publication of ethical principles, and embedding those principles into processes and practice.

Ethical principles and values outline how an organisation ideally **wishes** to **behave**, and what it is not **willing** to do, often to protect specific **audiences**. Publishing principles and values could be taken as a sign of intrinsic **motivation**.

Ethical principles should be developed collaboratively so that they capture the expectations of a data institution's audiences. Once published, they can be used to hold the data institution to account.[43]

However, what people perceive to be ethical and unethical use of data is rapidly evolving, and codes of practice are likely to quickly go out of date. This means data ethics principles need to be practical, and need to evolve.

Principles and values can also be difficult to put in practice: they can be too vague to offer clear guidance for day-to-day decisions.

Practical ethical systems and processes can be developed early in the organisation's lifecycle, and embedded into organisational design, governance practices and processes, and the way the data institution develops products and services.[44]

Many practical data ethics tools exist, including Doteveryone's Consequence Scanning[45], the Data Ethics Self Assessment tool[46] by the UK Statistics Authority and

[41] Open Data Institute (2020), 'Building trust in how you handle data: a hierarchy', https://theodi.org/article/building-trust-in-how-you-handle-data-a-hierarchy

[42] For example, Information Commissioner's Office (2018), 'Data protection by design and default', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default

[43] Raji I, et al (2020), 'Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing', https://arxiv.org/abs/2001.00973

[44] NowNext Design (2017), 'Ethical design sprints', https://www.cennydd.com/ethical-design-sprint-schedule

[45] Doteveryone (2019), 'Consequence scanning', https://www.doteveryone.org.uk/project/consequence-scanning

[46] UK Statistics Authority (2019), 'Ethics self-assessment',

the ODI's Data Ethics Canvas[47]. Most of these tools include guidance on identifying who may be affected by the stewarding or use of data, and recommend engagement with stakeholders and those affected by the use of data, particularly in the event of something going wrong.

Organisational design

Organisational design is the process of aligning the structure of an organisation with its objectives, with the aim of improving efficiency and effectiveness.[48] It includes, for example, the business model,[49] revenue model, and legal and corporate structures.

A data institution needs to ensure sustainable organisational and financial **ability** to implement good governance and deliver on its purpose. Certainly "crises of financial sustainability (or challenges of expansion) for these organisations are often coupled with or lead to a crisis in governance and/or community trust".[50]

All five of the experts we interviewed for this report highlighted the relationship between trust and organisational sustainability. Issues of trustworthiness that they associated with sustainability included fitness of technical systems; data protection; creating high-quality and useful data; and building a sense of community. For example, the representative from MusicBrainz said, "[A culture of honesty] builds trust, and this trust builds sustainability".

In some cases, the structure of an organisation expresses **willingness** and **motivation** to act in its stakeholders' interests over and above a profit motive. For example, after several years of operation, OpenCorporates created the OpenCorporates Trust[51] to oversee their public interest purpose: "[our corporate structure] ensures we'll always be independent and always act in the public interest and follow the rules that we've set ourselves".

Legal forms, such as trusts, charities, community interest corporations, and industrial and provident societies,[52] are organisational structures that legally enshrine social objectives rather than financial duty to shareholders. But it is not as simple as choosing a not-for-profit structure. For some data institutions, a commercial or profit-driven business model might interfere with the types of value they are trying to deliver, whereas for others, a commercial focus might enable them to invest more in, and maximise the value from, their services.[53]

https://www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/data-ethics/self-assessment-2

[47] Open Data Institute (2019), 'The data ethics canvas', https://theodi.org/article/data-ethics-canvas

[48] University of Southampton (n.d.), 'Organisational development & design explained', https://www.southampton.ac.uk/hr/services/od-explained/index.page

[49] Osterwalder A, Pigneur Y (2010), 'Business model generation: a handbook for visionaries, game changers, and challengers', https://www.wiley.com/en-gb/Business+Model+Generation%3A+A+Handbook+for+Visionaries%2C+Game+Changers%2C+and+Challengers-p-9780470876411

[50] Bilder G, Lin J, Neylon C (2015), 'Principles for open scholarly infrastructure', https://wiki.lib.sun.ac.za/images/f/f6/2015-principle-for-open-scholary-communication-infrastructures.pdf

[51] OpenCorporates (2018), 'Announcing the OpenCorporates Trust', https://blog.opencorporates.com/2018/06/11/announcing-the-opencorporates-trust

[52] GOV.UK (2011), 'Legal forms for social enterprise: a guide', https://www.gov.uk/government/publications/legal-forms-for-social-enterprise-a-guide

[53] Open Data Institute (2020), 'Designing sustainable data institutions', https://theodi.org/project/sustainable-data-institutions

Considering different audience's ethical expectations could affect the organisational design and governance of the data institution. Kieron O'Hara's paper 'Data trusts: ethics, architecture and governance for trustworthy data stewardship' explains: "Not all [audiences] can be pleased all at once. The purpose of the data trust should realistically be to benefit one or two of these [classes of audience]. The rules and ethical principles of the trust should be tailored to create the optimal signals of trustworthiness to those classes."[54] For example, an organisation designed primarily to be trusted by data contributors might emphasise corporate structures that enable independent stewardship; whereas one designed to primarily create trust among individuals mentioned in the data might de-emphasise business models that depend on sharing data with third parties.

Independent stewardship is necessary for some data institutions such as data trusts, [55] to ensure trustworthy decisions about data access. They can demonstrate their independence by screening out conflicts of interest; recruiting a diverse board; and choosing a funding model that doesn't override the data institution's purpose.

The ODI's research into sustainable data institutions[56] identified tensions in relation to some common institutional goals that would influence the organisational structure and funding. For example, charging data users to access data creates tension by incentivising the data institution to share data with more users in order to secure greater revenue. Resolving these tensions is necessary to align the expectations of different stakeholders, without which there is risk of losing their trust.

Organisational governance

Governance practices attempt to align the interests of stakeholders[57] and define which **audiences** benefit from the data institution's operation and how. Publishing governance materials, such as charters or terms of reference, provides clarity and transparency about the activities and behaviours that stakeholders should expect.

Good governance helps a data institution be more trustworthy by setting rules for itself and designing internal structures and processes to ensure those rules are followed, usually in a way that is transparent to stakeholders. As such, governance assures, controls and communicates a data institution's **behaviour**; as well as its **ability** and **willingness** to act towards its stated purpose.

A data institution's governance model needs to be appropriate to its operating context and for whom it needs to build trust. Research from Nesta suggests two axes [58] that could influence governance models for data institutions stewarding personal data. One axis represents how much control or choice the individual has in determining how data is shared and used; and the other is whether value from using the data is public (benefiting everyone) or private (benefiting data users).

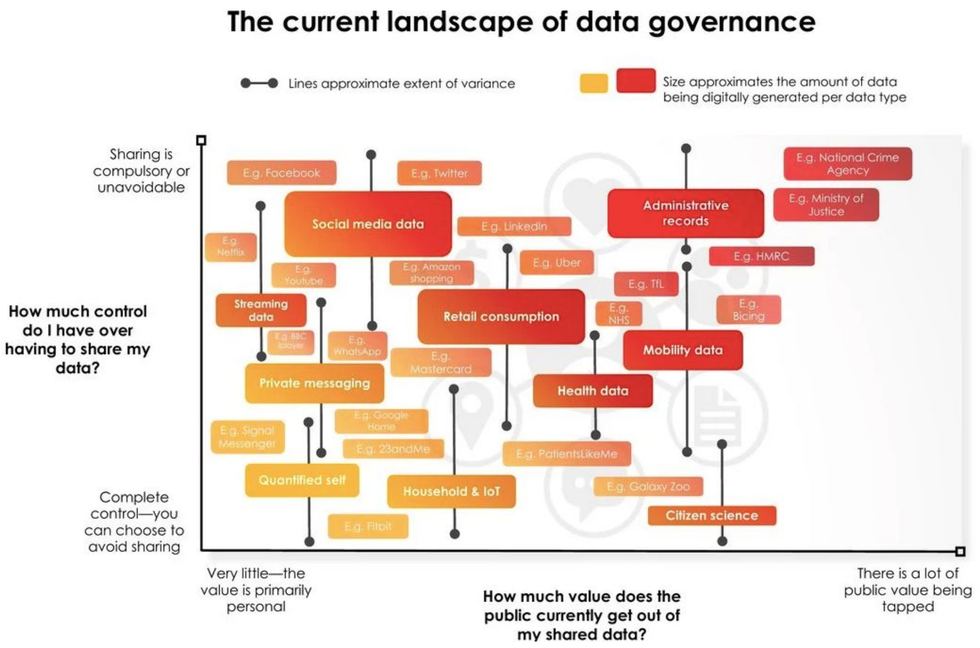
[54] O'Hara K (2019), 'Data trusts: ethics, architecture and governance for trustworthy data stewardship', https://eprints.soton.ac.uk/428276

[55] Open Data Institute (2019), 'Data trusts: lessons from three pilots', https://theodi.org/article/odi-data-trusts-report

[56] Open Data Institute (2020), 'R&D: Sustainable data institutions' https://theodi.org/project/sustainable-data-institutions

[57] Organisation for Economic Co-operation and Development (2004), 'G20/OECD principles of corporate governance', http://www.oecd.org/corporate/principles-corporate-governance

[58] Nesta (2019), 'The new ecosystem of trust', https://www.nesta.org.uk/blog/new-ecosystem-trust



Source: Nesta | The new ecosystem of trust

Where a data institution sits on these two axes determines its institutional governance. For example, a data institution that stewards data where individuals have little control over data sharing – and the data should benefit everyone – will require people in accountable roles who can explain why particular data sharing choices are made. In contrast, data institutions that create both public and private value, and where control is by individual consent, may better suit governance with networked trust relationships and collective decision-making similar to a co-operative.[59]

Guidance for publicly run organisations,[60] such as the UK Corporate Governance Code,[61] covers themes related to trust and is therefore relevant to data institutions. In terms of the trust framework we have built on in this report, the guidance talks about how to:

Establish the data institution's *context*, and how its *behaviour* in this context contributes to its objectives
for example, by aligning company culture with a clear purpose and strategy, and explaining the rationale for actions the company takes with consistency.

Enable *ability* to maintain long-term sustainable success and achieve wider objectives
for example, by recruiting an effective board, and ensuring they have the necessary time, resources and information available for the company to meet its objectives.

Demonstrate *willingness* and *motivation* to be trustworthy
for example, by ensuring and publicising how workforce policies and practices are consistent with the company's values.

[59] Hafen E (2019), 'Personal data cooperatives – a new data governance framework for data donations and precision health', https://link.springer.com/chapter/10.1007/978-3-030-04363-6_9
[60] Department for Transport (2018), 'Ports good governance guidance', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684839/ports-good-governance-guidance.pdf
[61] Financial Reporting Council (2018), 'UK Corporate Governance Code', https://www.icaew.com/technical/corporate-governance/codes-and-reports/uk-corporate-governance-code

Give wide-ranging consideration to diverse *audiences*, including those who should benefit from, and those affected by, use of data
for example, by establishing a board with diverse perspectives and giving regard to the interests of, and relationships with, employees, suppliers, customers, the wider community and the environment.

Enable stakeholders to make *informed judgements* about the data institution's trustworthiness
for example, by setting high standards of transparency, and by using a variety of engagement approaches to communicate meaningfully and consistently with stakeholders.

To be trustworthy, data governance and oversight should also extend beyond internal processes and data access to include how the data is used.[62] It will almost certainly extend to the way in which data users use and onwardly share the data that has been shared with them. Depending on the design and function of the data institution, it may also extend to how data contributors manage, use and share data themselves. Technology has some role to play in monitoring adherence to the rules created by the data institution.

The role of technology

Technology is mainly used to bolster a data institution's **ability** to keep to its data security commitments. Anonymisation techniques, for example, can help reduce the risk of re-identification[63] of data subjects. Security techniques, access control and logging mechanisms help restrict and monitor access to data.

The methods of data access and data formats should be reliable, sustainable and non-prohibitive in terms of cost and complexity to be considered trustworthy by those data users who are permitted access.

> *Because trust is embedded in our social relationships and our relationships with technological systems, these are the areas policymakers must pay more attention to, in addition to data privacy and security issues.*[59]

Research from the University of Manchester cautions against viewing new digital services simply as new means of providing the same personal service.[64] It suggests that we broaden the conversation around trust in technology beyond issues of privacy, security and data sharing, and consider its potential to disrupt the trusted

[62] Tzovaras B (2019), 'Alternative personal data governance models', https://osf.io/preprints/metaarxiv/bthj7

[63] Open Data Institute (2019), 'Anonymisation and open data: an introduction to managing the risk of re-identification', https://theodi.org/article/anonymisation-report

[64] Ribeiro B (n.d.), 'Beyond privacy and security: opening-up 'trust' in digital healthcare', https://policyatmanchester.shorthandstories.com/on-digital-trust/index.html#group-Trust-in-Healthcare-RDrtklFazP

relationships between people. For example, in the relationships between patients and caregivers, technology can change how and where care takes place, producing new forms of communication and attributing responsibility to new points of contact.

Complex social issues like this mean data institutions might need to make efforts to be trusted in new ways. The next section discusses measures and mechanisms to mediate some of the relationships inherent in trust.

Being trusted with data

As we saw in the section ‘How trust breaks down’, there are several ways stakeholders’ trust in a data institution can be undermined. Many mechanisms have been developed to help people and organisations overcome these potential failures, and to bridge the gap between the understanding of those involved in a data institution and those who are trying to judge whether that institution can be trusted.

Some of these mechanisms are intended to help people or organisations be more trustworthy, such as by undergoing training; some are designed to help people or organisations be more trusted, for example by publishing the minutes of meetings where decisions are made. Often mechanisms have a dual function, for example studying for an exam both teaches someone the material, and demonstrates to others that they have attained a certain level of qualification.

Some of the measures will be implemented by the data institution itself, such as performance monitoring or drafting data sharing agreements; others are carried out by external actors to provide assurance, such as auditing and certification.

Different mechanisms will address potential misunderstandings or misrepresentations for different components in the framework. For example, interviews are a way to interrogate someone’s abilities; drafting licences is a way to avoid misunderstandings about how data can be used in different contexts; and kitemarks help people determine how a data institution should behave in accordance with which quality standards.

Understanding how these mechanisms relate to the trust framework, as introduced in the previous section of this report, can help data institutions use them more effectively to strengthen trustworthiness and build trust.

Mapping trust mechanisms

Drawing on our desk research and interviews, we identified a number of common mechanisms used by and between organisations to demonstrate or assess trustworthiness. We conducted a mapping exercise taking these various mechanisms and distributing them across a matrix with (i) the specific elements of trustworthiness (ability, willingness, etc) on one axis; and (ii) the possible ways trust can break down (misrepresentation, misunderstanding or the failure to communicate in times of change) on the other axis. The result of the mapping exercise is presented in Appendix B: Map of trust mechanisms.

While the mapping exercise is not authoritative or comprehensive, it reveals a number of insights. The main one is that **there are gaps where no standard mechanism exists**; the gaps suggest areas where trust can easily break down. For example, it is not easy to prove one’s motivations.

The second insight is that **there is no panacea:** we did not find any mechanism which would help prevent all possible ways trust can break down, nor did any mechanism appear to cover all the elements of the trust framework. Most mechanisms address one or two potential failure points.

A notable exception is the use of contracts, which define expectations of behaviour, context and, in some cases, how benefit is to be distributed to the intended audience. Audits also address several aspects: defining and verifying a data institution's ability or behaviours, and acting as evidence: if a data institution passes an audit, you can expect them to meet a certain standard of ability or behaviour.

Communication and transparency

A further insight surfaced by the mapping exercise was a lack of standard communication mechanisms. Although many mechanisms are designed to root out misrepresentation, a significant proportion of breakdowns of trust are caused by failures of communication – either to align understanding or to communicate changes. But we identified very few standard mechanisms to address this type of problem.

Some mechanisms such as contracts or reports are themselves forms of communication. But effort to align understanding is particularly important between parties that aren't covered by contracts or other more formal mechanisms. In these cases, proactive communication is vital.

We can learn from the case of data sharing between the Royal Free Hospital and DeepMind. The Royal Free Hospital shared patient data with artificial intelligence (AI) company DeepMind, which was developing an app to help detect patients with acute kidney injury. The Information Commissioner's Office ordered an audit of the app after widespread concerns from patient groups about the scale and scope of the project – in other words, the **context** and **behaviours** were not what the patients expected. In response, DeepMind resolved to increase and improve communication around future work.[65]

> “ *Explanations are a positive opportunity to communicate, not an onerous obligation.*[66]

A data institution needs to consider communication in several respects:

- Demonstrate it has considered and addressed all the ways it needs to prove its trustworthiness.
- Ensure all parties have a shared understanding of the data institution's context or purpose; of how behaviours and activities relate to the purpose of the data institution; and who will benefit from those activities.
- Explain changes to circumstances that may change that shared understanding.

[65] DeepMind (2017), ‘The Information Commissioner, the Royal Free, and what we've learned’, https://deepmind.com/blog/announcements/ico-royal-free
[66] Financial Reporting Council (2018), ‘UK Corporate Governance Code’, https://www.icaew.com/technical/corporate-governance/codes-and-reports/uk-corporate-governance-code

Intelligent transparency

Transparency is common to many mechanisms where sharing or publishing evidence helps others make informed judgements. For example, publishing a record of decisions made by a data access board helps others determine if decisions are being made in the interest of the expected audience.

Onora O'Neill[67] cautions against transparency for transparency's sake, since "increasing transparency can produce a flood of unsorted information and misinformation that provides little but confusion unless it can be sorted and assessed".

Instead, O'Neill advocates for 'intelligent transparency' and says that information should be:

- accessible – people should be able to get at it
- comprehensible – people should be able to understand it
- useable – it should suit their needs
- assessable – interested parties should, if necessary, be able to examine the workings and assess its quality.

This view is echoed by David Pozen,[68] who also cautions that "transparency mandates hold complex processes to unrealistic standards" and "there is nothing incoherent about transparency policies yielding positive outcomes in certain settings and negative or even opposite outcomes in other settings".

Pozen advises careful consideration of transparency's relationship to governance goals, such as constructive deliberation, and advises implementing the means of transparency in service to each goal.

Mechanisms throughout a data institution's lifecycle

Being trustworthy and being trusted both need to function over time. In our previous project to pilot data trusts,[69] we proposed a simple lifecycle that describes the stages of setting up and running a data institution.

[67] O'Neill O (2002), 'Reith Lectures 2002: Lecture 4: Trust and transparency', http://downloads.bbc.co.uk/rmhttp/radio4/transcripts/20020427_reith.pdf

[68] Pozen D (2019), 'Seeing transparency more clearly', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3478005

[69] Open Data Institute (2019), 'Data trusts: lessons from three pilots', https://theodi.org/article/odi-data-trusts-report

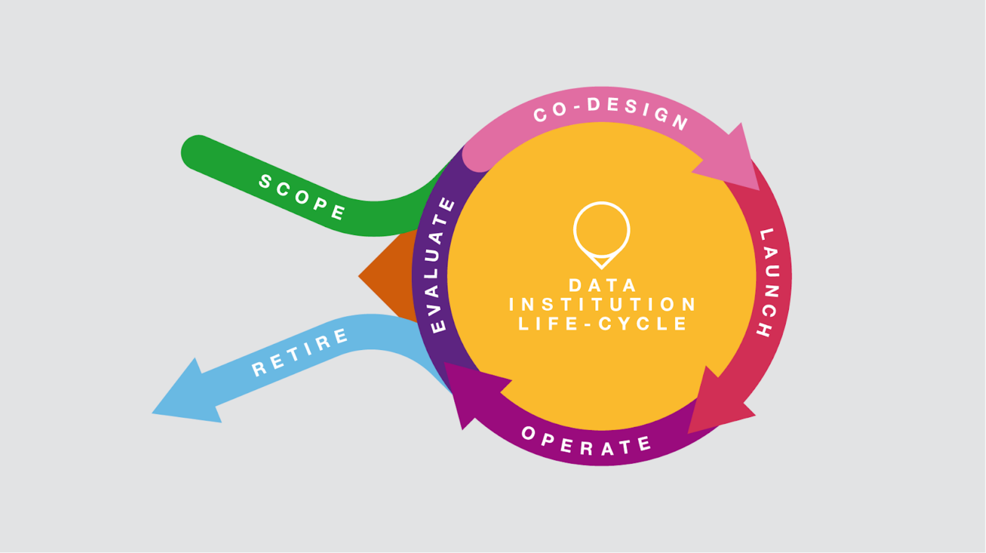


Image source: Open Data Institute

Different mechanisms will be more appropriate in different phases in the lifecycle of a data institution. For example, use cases, ecosystem maps[70] and empathy maps[71] are more likely to be used to create shared understanding in the scoping and co-design phases, while the context and audiences for the data institution are being defined. Whereas after launch, a data institution might use mechanisms of transparency such as decision logs or financial reporting to help stakeholders make accurate assessments of the data institution's trustworthiness.

Third party trust

People and organisations can make claims about trustworthiness on another's behalf. This is one of the ways that trust can scale. We cannot know everyone personally, so we rely on recommendations from organisations we trust, in turn to understand the trustworthiness of others.

As we discussed previously, a data institution will need to act as a trust intermediary. Using this framework, we can see this role as providing assurances around another person or organisation's **ability** to supply data that is of a particular quality, or to hold data securely. It may need to provide evidence that helps people decide whether to trust each other, or in some cases provide incentives that **motivate** stakeholders to behave as they claim.

Other trusted people or organisations may also make claims about the trustworthiness of a data institution. For example, by being involved in the data institution, data contributors implicitly indicate that they trust it. More explicit claims of trustworthiness may be made by auditors or certifiers.

[70] Open Data Institute (2018), 'Mapping data ecosystems', https://theodi.org/article/mapping-data-ecosystems
[71] XPLANE (2017), 'Updated empathy map canvas', https://medium.com/the-xplane-collection/updated-empathy-map-canvas-46df22df3c8a

Assessing trustworthiness

Audits and certifications are assessments that can be conducted internally by a data institution to improve its own trustworthy operation, or externally by a third party. That third party could be a direct stakeholder – such as a prospective data contributor or user performing due diligence – or a trusted independent assessor, whose assessments are then used by prospective stakeholders.

Audits

Audits are tools for interrogating complex processes, often to determine whether they comply with company policy, industry standards or regulations.[72] In this way, audits assess a data institution's **behaviours** and **ability** to deliver on expectations.

External audits typically examine the finances of an organisation; whereas internal audits consider the effectiveness of governance, risk management and control processes, and even wider issues such as the organisation's reputation, growth and impact on the environment.[73]

A data institution will need to demonstrate to auditors that it is "delivering on its purposes, has effective processes for promoting beneficial use and mitigating harm, is appropriately assessing its non-financial impacts, is achieving an equitable balance between the needs of different stakeholders, and so on".[74] Assessment mechanisms might include stakeholder surveys and interviews, public research, and stress-tests of a data institution's processes and policies.

A data institution may pose challenges to traditional audits, however, due to the need for auditors to understand the operational and data contexts. There may eventually be the need to find auditing approaches that are specific to data institutions, for example, processes to determine compliance with declared **willingness** to uphold ethical principles.[75]

Certification

Certification is a process where a third-party authoritative body verifies that a non-authoritative person, process, product or organisation meets standardised criteria. A certification will have a target audience such as customers, shareholders or regulators. If successful, the non-authoritative entity is allowed to signal compliance using mechanisms such as kitemarks. The certifying authority usually acts as an auditor to verify ongoing compliance, as well as having powers to enact redress mechanisms.

We can trust certifying bodies by ensuring there is oversight of them by accreditors.

[72] Liu J (2012), 'The enterprise risk management and the risk oriented internal audit', https://www.researchgate.net/publication/272673574_The_Enterprise_Risk_Management_and_the_Risk_Oriented_Internal_Audit

[73] Chartered Institute of Internal Auditors (2020), 'What is internal audit?', https://www.iia.org.uk/about-us/what-is-internal-audit

[74] Open Data Institute (2019), 'Data trusts: how decisions are made about data sharing', https://theodi.org/article/data-trusts-decision-making-report

[75] Raji I, Smart A, White R(2020), 'Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing', https://arxiv.org/abs/2001.00973

Accreditation confirms that the process of certification is carried out correctly. For example, the UK Accreditation Service and the International Accreditation Service.

Certification is a special type of mechanism because it is designed to incorporate other mechanisms. For example, to meet ISO-9001 requirements, an organisation must *train staff* with adequate abilities, and define *acceptance criteria* for product behaviour.

As such, certification serves many purposes: guidance; monitoring; independent accountability; and as a signal to others that an organisation has been through a rigorous process, which others may consider when deciding whether to trust it.

Existing certifications that are likely to be relevant for data institutions include:

- **Technical expectations** such as technical or security adequacy. For example the National Cyber Security Centre's Cyber Security certification,[76] which "helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security".
- **Organisational processes** for example ISO-9001, which aims to ensure the quality of products and services by establishing a rigorous quality management system.[77]
- **Organisational structure and mission** for example B-Corp, which verifies whether a company meets "standards of social and environmental performance, public transparency, and legal accountability to balance profit and purpose".[78]
- **Comprehensive certification** such as CoreTrustSeal's Trustworthy Data Repositories[79] certification, which certifies repositories that have an explicit mission to provide access to and preserve data. It covers matters of preservation, licences, financial and technical sustainability, ethics, organisational structure, guidance, data quality and integrity, evaluation, documentation, data discovery, enabling data reuse, technical infrastructure, and security.

The costs of formal certification, which include employee training and auditors' fees, need to be balanced against the value it brings in terms of the standard achieved and the signal of trustworthiness it produces. HESA told us it had let its ISO-9001 certification lapse having "decided in the last few years that the benefits didn't justify the costs involved [...] but we do still follow the procedures that were set up internally to comply".

Certifications need to be renewed and so are not a permanent guarantee. For example, OpenCorporates preferred to use irs organisational structure and governance processes to assure its public interest mission rather than certification because of the "overhead" involved and because the certification doesn't provide protection: "there's no guarantee the owners won't sell to someone else the day after tomorrow and you'll no longer be a B-corp after that".

[76] National Cyber Security Centre (2020), 'Cyber essentials', https://www.cyberessentials.ncsc.gov.uk
[77] British Assessment Bureau (2018), 'Quality management systems explained', https://www.british-assessment.co.uk/insights/what-is-a-quality-management-system
[78] Certified B Corporation (n.d.), 'About B Corps', https://bcorporation.net/about-b-corps
[79] CoreTrustSeal (2019), 'CoreTrustSeal Trustworthy Data Repositories Requirements', https://www.coretrustseal.org/why-certification/requirements

A certification of trustworthiness?

Certifications often have specific requirements, for example, 'product and service quality' or 'corporate responsibility'. At the time of writing, there is no known comprehensive 'certification of trustworthiness with data' that considers all aspects necessary to demonstrate trustworthiness and align trustworthiness and trust in a rigorous way. However, we suggest the CoreTrustSeal Trustworthy Data Repositories would make a good basis.

A certification of trustworthiness might ask to what extent the data institution has:

- communicated the quality and coverage of appropriate mechanisms, including laws and regulations, codes and standards
- communicated the context, audience and behaviours to avoid misunderstandings throughout a data institution's lifecycle
- a plan to re-communicate and re-consent if one or more of the context, audience, behaviours or abilities were to change during the lifetime of the data institution.

There are two options for such a certification:

- An all-encompassing certification that would assess all aspects necessary to demonstrate trustworthiness and align trustworthiness and trust in a rigorous way.
- Several focused certification bodies that assess separate aspects. In this case, the data institution may make use of advisory and consultancy services to create coherent coverage.

Earlier research from Oxford Insights into certification for data trusts[80] recommended the discovery, prototyping and testing of potential certification models with stakeholders. The ODI intends to follow these recommendations in a future phase of our research and development.

Signals such as kitemarks or trustmarks may have limitations with some audiences. Doteveryone carried out extensive research into trustmarks for technology[81] and found that they would take significant investment to establish, and with limited benefit. Requirements for a trustmark in the face of fast-changing technology services, and lack of consumer levers and interest in a domain where choices are already complex, led Doteveryone to conclude that a more effective solution would be to work with businesses to introduce a more flexible, value-based approach to ensure the trustworthiness of their processes and products. This could be coupled with lightweight accountability and enforcement, without the cost and scale of a full standards body or certification authority.

[80] Oxford Insights (2019), 'Exploring data trust certifications', https://theodi.org/article/data-trusts-will-certification-work-report

[81] Doteveryone (2019), 'Why we haven't made a trustmark for technology', https://www.doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas

Trusting others

In the section ‘An ecosystem for trust’, we discussed how a data institution needs to assess the trustworthiness of those parties it depends on or represents. It can do that using the same mechanisms described in the previous section.

For example, when hiring staff, it may assess their ability through interviews, professional certification and exams; and data access panels within a data institution will assess whether prospective data users will behave in accordance with agreed criteria.

But trust isn’t merely transactional; it is relational. Collaboration requires mutual trust. And for the relationships to be mutually beneficial, a data institution also needs to trust its stakeholders.

Invest in capability to take collective decisions

A data institution will have to make many decisions throughout its lifecycle. For example, what types of data users should have access to, what services to provide and what business model to adopt.

Research into decision making for data trusts – by Communication Chambers and Involve and commissioned by the ODI – states: “Deliberative decision-making [...] is important for data [institutions], given wider societal mistrust and uncertainty around data sharing and use. A data [institutions]’s legitimacy – and, by extension, the trust of stakeholders – comes from its capacity to enable, encourage and benefit from collective discussion, reasoning and decision-making.”[82]

Before a data institution is willing to open its processes to external influence, it will need to trust that its stakeholders are invested in shared problems. By investing in stakeholders’ capability and skills to understand complicated issues, a data institution will have the confidence to act on the feedback and perspectives they provide.

Many data institutions will have a broad stakeholder group with a range of economic and data literacy. True engagement requires sustained, iterative effort to produce accessible materials and develop a shared vocabulary that is meaningful to both sides of the conversation;[83] and necessary for aligning understanding and trust.

Even so, many organisations report positive experiences and successful engagement programmes[84] involving diverse groups with a range of data literacy, such as the Royal Society’s public dialogue work on machine learning[85]. The Ada Lovelace

[82] Involve (2019), ‘Data trusts: how decisions are made about data sharing’, https://theodi.org/article/data-trusts-decision-making-report

[83] O’Hara K (2019), ‘Data trusts: ethics, architecture and governance for trustworthy data stewardship’, https://eprints.soton.ac.uk/428276

[84] University of Manchester (2020), ‘We need to re-think health data sharing and public trust’, https://www.manchester.ac.uk/discover/news/we-need-to-re-think-health-data-sharing-and-public-trust-says-pub

[85] Royal Society (2017) ‘Public views of machine learning’,

Institute reports: “When engaged in a way that fosters critical democratic scrutiny, publics are capable of discussing the use of data in a sophisticated manner… [supporting] policymakers and regulators to broaden the conversation on the use and governance of data.”[86]

Be fearless, be honest

Inevitably, even for trustworthy actors events don’t always go to plan or new information comes to light. By investing in stakeholder’s capability and skills to understand complicated issues, a data institution can trust in their discernment enough to be honest with them if something goes wrong.

Data institutions that are not open with their stakeholders, or try to manage messaging, risk being misinterpreted as untrustworthy; as Onora O’Neill points out, deception is the real enemy of trust[87]. O’Hara expands on this idea saying, “Even if the organisation has done everything it could and is not to blame for a breach, an ill-thought-out communication strategy gives an impression of a cover up.[...] At best, it means that the organisation is focused on its own problems of liability, and not on the harms to its stakeholders”.[88]

There are good examples of frank apologies[89], reparations[90], open post-mortems[91] and incident reports[92] that have prevented a technical or procedural mishap from escalating into an issue of mistrust and damaging relationships.

Honesty is the foundation on which to rebuild trust. If a data institution has built and maintained a relationship with its stakeholders using the techniques described in the rest of this report, they may be supportive.

https://royalsociety.org/-/media/policy/projects/machine-learning/publications/public-views-of-machine-learning-ipsos-mori.pdf

[86] Ada Lovelace Institute (2020), ‘Rethinking data’, https://www.adalovelaceinstitute.org/our-work/rethinking-data

[87] O’Neill O (2002), ‘Reith Lectures 2002: Lecture 4: Trust and transparency’, http://downloads.bbc.co.uk/rmhttp/radio4/transcripts/20020427_reith.pdf

[88] O’Hara K (2019), ‘Data trusts: ethics, architecture and governance for trustworthy data stewardship’, https://eprints.soton.ac.uk/428276

[89] Gitlab (2019), ‘Important updates to our terms of service and telemetry services’, https://gitlab.com/gitlab-org/gitlab/issues/34833

[90] DeepMind (2017), ‘The Information Commissioner, the Royal Free, and what we’ve learned’, https://deepmind.com/blog/announcements/ico-royal-free

[91] Google Cloud Platform (2020), ‘Fearless shared postmortems’, https://cloud.google.com/blog/products/gcp/fearless-shared-postmortems-cre-life-lessons

[92] Cloudflare (2020), ‘Post Mortem’, https://blog.cloudflare.com/tag/postmortem

If you want to go far, go together

“The failure on the part of policy and industry organisations to open up the conversation to the wider public has moved the current discourse on data out of step with people’s expectations and attitudes.”[93]

Trust is dynamic. It is built, and must be nurtured over time. The relationship between data institutions and the communities that surround and support them is one of mutual interaction and influence. A change or evolution of either of these is bound to have an impact on, or bring about changes in, the other. Over the life of a data institution, this changing relationship can present a number of challenges to the understanding between a data institution and its stakeholders.

Stakeholder engagement is a means to continually align understanding, for example through open processes where external parties are able to influence outcomes through consultation, dialogue, negotiation, compromise and relationship building.

Specialist engagement skills are required to identify stakeholders, incentivise participation, design events, facilitate and mediate, and summarise and feed back recommendations into existing processes. The complexity[94] of the task should not be underestimated. A data institution will need access to people with the right skills, either in house or by working with specialist agencies.

There are many engagement approaches appropriate to the message being communicated, the purpose of the engagement, and the needs of the group, including:

- interviews and dialogues[95]
- roundtables
- citizens’ juries[96]
- advisory committees
- public forums[97]
- consultation on specific subjects or projects[98]
- open annual meetings

[93] Ada Lovelace Institute (2020), ‘Rethinking data’, https://www.adalovelaceinstitute.org/our-work/rethinking-data

[94] MIT Sloan Management Review (2005), ‘Managing stakeholder ambiguity’, https://sloanreview.mit.edu/article/predicting-customer-choices-2

[95] Royal Society (2017) ‘Public views of machine learning’, https://royalsociety.org/-/media/policy/projects/machine-learning/publications/public-views-of-machine-learning-ipsos-mori.pdf

[96] Ada Lovelace Institute (2019), ‘The Ada Lovelace Institute supports Wellcome Trust to undertake citizen juries on fair data sharing in the NHS’, https://www.adalovelaceinstitute.org/the-ada-lovelace-institute-kicks-off-citizen-juries-on-fair-data-sharing-in-the-nhs

[97] Involve (2020), ‘21st century town meeting’, https://www.involve.org.uk/resources/methods/21st-century-town-meeting

[98] UK Biobank (2020), ‘Public consultation’, https://www.ukbiobank.ac.uk/public-consultation

For example, ROR has established a community advisory group composed of domain experts with whom they convene regular stakeholder prioritisation sessions. A steering group with experts and leaders from non-profit and academic institutions brings a wealth of expertise to ROR, lending it a sense of authority and trust.

The following are occasions when two-way engagement is particularly appropriate to aligning trustworthiness and trust.

Provide opportunities to re-evaluate following new information

A data institution's circumstances can change such that the foundations on which trust was built may shift. The trigger for change can be internal, for example, staffing or business models change; or caused by external forces, for example, new information comes to light, or regulations change.

In seeking to evolve, scale and adapt to changing circumstances, however, it is important that data institutions assess whether they will be changing in ways that will upset or alienate members of their current stakeholders, community or ecosystem.

For example, as a data institution grows and evolves, it may need to evolve its business model, possibly by offering new services or by welcoming new data contributors, users or decision makers to the ecosystem.

HESA described to us how its business model has adjusted over time. It wanted to move away from commercialisation of data resources towards commercialisation based on expertise, such as data analysis and data visualisation. Its board of directors has always been careful to ensure that HESA's commercial activities are not in conflict (or perceived by stakeholders to be in conflict) with HESA's core functions.

The ODI's Data Ethics Canvas guidance recommends organisations regularly revisit their ethics assessment, for example, quarterly, or at project milestones. Similarly, if the conditions under which trust was originally given change, stakeholders and those affected by the use of data should be given the opportunity to review new information and re-evaluate any agreements they have entered into.

Stakeholders' views can change

As a data institution grows, the community around it is likely to grow as well, and the needs, motives and expectations of that community are almost certain to evolve.

Engagement can help a data institution identify any changes in public perception or changes in how trustworthiness and trust is aligned, giving the data institution the opportunity to make any necessary changes.

For example, OpenStreetMap has corporate sponsors who provide funding and are increasingly involved in the project by contributing data, open source code and other resources. Their contributions represent their evolving sense of what is important to the project. These contributions help make the project more sustainable, but have raised concerns from the existing community about the ease with which those organisations could shape the future of the project.

Data institutions as centres of debate

The Ada Lovelace Institute observes: “The failure on the part of policy and industry organisations to open up the conversation to the wider public has moved the current discourse on data out of step with people’s expectations and attitudes.” This misalignment is fertile ground for the breakdown of trust.

Previous ODI commissioned research[99] found that data institutions could play a role in defending the interests of parties who:

- cannot negotiate effectively because they are too dispersed, for example, the public
- lack sufficient information about other parties’ incentives
- are invested in the social and non-financial benefits.

Data institutions could be a centre for debate: bringing together and enabling data scientists, data subjects and other stakeholders to interact, debate and refresh mutual understanding of what constitutes trustworthy behaviour.[100]

[99] Open Data Institute (2019), ‘Data trusts: how decisions are made about data sharing’, https://theodi.org/article/data-trusts-decision-making-report

[100] O’Hara K (2019), ‘Data trusts: ethics, architecture and governance for trustworthy data stewardship’, https://eprints.soton.ac.uk/428276

Conclusion and next steps

This report summarises an initial exploratory study to help understand the factors that contribute to the creation of trustworthy data institutions.

Data institutions are a relatively new type of organisation, and it is important that they are designed and operated in a trustworthy way, such that they establish and maintain the trust of their stakeholders.

Adopting the language and concepts of formalised trust frameworks can help us understand the evolving ecosystem of trust around a data institution. A trust framework can also be used to understand the rules governing the activities of data institutions, and to organise our knowledge of the many mechanisms which they and others can use to either assess trustworthiness, or try to demonstrate it to create richer and more resilient networks of trust.

Trust can be conferred to data institutions by third parties. By providing audit and certification, already-trusted members of the data ecosystem can help bolster trust in new data institutions, as earlier research into certification for data trusts suggests[101].

Mapping these mechanisms reveals where there are gaps: trust is often undermined when there is a failure to communicate around change; and there is only so much kitemarks and principles can help in those cases. Most importantly, our work has highlighted how trust is dynamic: it can only be built over time, through demonstration of trustworthiness, and honest, open engagement across the ecosystem.

To conclude, we identify some areas for further research and provide some initial recommendations for those currently scoping, designing and running data institutions.

Areas for further research

We plan to apply the framework introduced in this report to support further analysis of the ways data institutions ensure their trustworthiness and help others decide to trust them.

There are several areas that merit further work, including:

- Developing a more comprehensive review of the mechanisms adopted by different types of data institutions across sectors, and, in particular, exploring some who have suffered from breakdowns of trust.

[101] Oxford Insights (2019), ‘Exploring data trust certifications’, https://theodi.org/wp-content/uploads/2019/04/Report_-Exploring-Data-Trust-Certification.pdf

- Further work to understand whether a combination of trust mechanisms would create an effective certification programme, and to understand how such a programme would affect the ecosystem of trust.
- Developing and testing practical tools, for example, a canvas, using the trust framework as a basis to help support data institutions in developing trustworthy practices and aligning understanding.

Suggestions for those scoping, designing and running data institutions

While our exploratory research was not intended to produce a comprehensive survey of the many data institutions that exist across sectors, through our desk research and interviews we have identified some common issues and challenges in aligning trustworthiness and trust.

Based on those insights, we offer some initial suggestions for those currently scoping, designing and running data institutions, to help them navigate trustworthiness and trust.

Being trustworthy: reliably deliver on promises

- **Define explicit expectations and boundaries.** Everything a data institution does should be constrained by its context – its purpose – to benefit some audiences and not cause harm through its actions. It should understand its role in the ecosystem: the relationships and dynamics in which it operates, including data flow and funding that could affect its purpose. It should understand its own abilities, limitations and where it should cooperate, and it shouldn't overstep those boundaries.
- **Surface implicit expectations.** Some expectations of a data institution will be implicit. Seek to understand the expectations of all those who have an interest in the operation: from regulators and direct stakeholders, to those who may be affected by using the data being stewarded.
- **Implement trustworthy practices.** Follow the rules set by the data institution itself, and by its environment. Practise ethical design with special consideration to any implicit expectations. Establish an organisational structure, governance practices and organisational processes that are aligned with the declared values and principles, and that enable the people in the organisation to deliver on expectations. Hire employees with the right skills. Be fearlessly honest.

Building and sustaining trust: close the perception gap

- **Demonstrate** that the data institution has implemented trustworthy practices.
- **Communicate** the data institution's own expectations and boundaries clearly.
- **Engage people with empathy.** Build mutually beneficial relationships. Understand how the data institution and its employees are perceived. Internalise the understanding gained in surfacing implicit expectations. Meet people where they are. Use language they understand. Demonstrate trust in the data institution's stakeholders.

- **Adapt and evolve collaboratively.** Circumstances change and new information comes to light, and organisations need to adapt – but trust that was placed in the data institution in one set of circumstances may or may not endure in a new set. Explain changes to stakeholders and give them the opportunity to re-establish trust on new terms. Open up the data institution's processes to influence and evolve together.

We plan to apply these recommendations as we continue to work with a range of organisations that are establishing new data institutions. As our research and practical work continues, we will revisit, revise and expand these recommendations.

Appendix A: Methodology

To inform this exploratory research project, we conducted broad desk research into concepts of trustworthiness relevant to the context of data institutions. We then defined a set of criteria to select different types of data institutions we would look at in more details. We conducted desk research about these institutions and, where possible, interviewed representatives of the data institutions.

The brief timeframe of this research resulted in several limitations, including:

1. Limited number of interviews.
2. Potential sector bias – our desk research has been informed significantly by our prior knowledge of specific institutions.
3. Focus on one trust framework.

Research questions

Main research question
What mechanisms exist to assess (and verify) the trustworthiness of people, products and institutions, and which ones may be relevant in the context of data institutions?

Supplementary research questions:

1. What laws and regulation currently affect data institutions?
2. What mechanisms do organisations use to prove their trustworthiness?
3. Which groups of people or organisations do the data institutions aim to prove their trustworthiness to?

Desk research

Our desk research covered academic and professional literature on trust and trustworthiness, accountability, certification and accreditation, and data governance models. We also reviewed and built on our earlier research on data trusts and data institutions.

Interviews

We complemented the information gathered through desk research with interviews with representatives of data institutions. We interviewed representatives from five organisations covering some of the following criteria:

1. Type of data institution:
    a. Organisations that steward data on behalf of a community
    b. Organisations that steward digital resources or a platform on behalf of a community
    c. Organisations that steward a physical resource on behalf of a community or set of stakeholders
2. Life stage of the data institution:
    a. Organisations in scoping or co-design stage
    b. Organisations that are operational but relatively young
    c. Well-established or 'successful' institutions
    d. Organisations that tried to set up a data institution but could not overcome the challenges

We interviewed representatives from the following data institutions:

- **Higher Education Statistics Agency (HESA)**[102]: an official body which collects, analyses and publishes data about higher education in the UK. Its products are used by researchers and policymakers for transparency, retaining public trust and decision making.
- **Research Organization Registry (ROR)**[103]: a community-led project working to produce a unique, open, usable and sustainable identifier for every research organisation in the world.
- **HiLo Maritime Risk Management**[104]: a not-for-profit joint industry initiative providing analysis of shipping data to make the industry safer. Shipping companies share safety-related data from vessels, HiLo runs it through a risk algorithm and shares insights with the companies.
- **OpenCorporates**[105]: the world's largest open database of information about companies. All of the data on OpenCorporates comes from primary public sources, and is used by individuals, journalists, non-governmental organisations and companies.
- **MusicBrainz**[106]: a project to create a collaborative database about artists, songs and albums. Any user can contribute and release the music metadata under open licences.[107]

The questions asked during the one-hour interviews covered themes related to sustainability[108] and trustworthiness, specifically:

- Revenue streams
- What sustainability looks like
- Alignment of business models with data institutions' core goals
- Mechanisms for ensuring trustworthiness
    - Laws or regulations that help prove or improve trustworthiness
    - Used or planned to use mechanisms to prove trustworthiness
    - Mechanisms for redress if trust is broken
    - Ways of demonstrating trustworthiness to different groups of people.

[102] Higher Education Statistics Agency (n.d.), https://www.hesa.ac.uk/
[103] Research Organization Registry (n.d.), https://ror.org/
[104] HiLo Maritime Risk Management (n.d.), https://hilomrm.com/
[105] OpenCorporates (n.d.), https://opencorporates.com/
[106] MusicBrainz (n.d.), https://musicbrainz.org/
[107] MusicBrainz (n.d.), 'About: Data license' https://musicbrainz.org/doc/About/Data_License
[108] Open Data Institute (2020), R&D: Sustainable data institutions, https://theodi.org/project/sustainable-data-institutions

Appendix B: Map of trust mechanisms

This appendix presents a map of mechanisms that can be used or called upon by data institutions or others in their ecosystem. The table below presents those mechanisms mapped against the element of trust in the framework in the section 'A framework for trust', with columns mapping the ways trust can break down presented in the section 'How trust breaks down'.

The map is not intended to be comprehensive, but indicative of the kind of mechanisms considered during our research.

	Avoid misrepresentation	Avoid misunderstanding	Avoid being unable to determine	Communicate changes
Ability	● Exams ● Interviews ● Performance monitoring ● Audit ● Certification ● Professional certification ● Accreditation ● Oversight eg regulatory ● Peer review	● Quality standards eg ISO-9000	● Exams ● Interviews ● Performance monitoring ● Audit ● Certification ● Training ● Quality standards eg ISO-9000 ● Privacy technologies	
Willingness	● Interviews		● Principles ● Codes of ethics ● Codes of conduct	
Motivation			● Penalties ● Redress ● Values	
Context		● Contracts ● T&Cs ● Licences ● Data sharing agreements ● Citizens' juries		● Re-issuing T&Cs
Behaviour	● Data access panels ● Audit ● Review boards ● Minutes of Meetings ● Certification	● Laws ● Regulation ● Contracts ● T&Cs ● Licences ● Sharing agreements ● Data standards ● Ethics assessments ● Citizens' juries	● Audit ● Data standards ● Principles ● Codes of ethics ● Codes of conduct ● Kitemarks	● Re-issuing T&Cs
Audience	● Financial reporting ● Decision logs	● Contracts ● T&Cs ● Licences ● Register of interests ● Ecosystem map ● Empathy map		● Re-issuing T&Cs