August 2017

A Path to Social Licence

Guidelines for Trusted Data Use

DATA FUTURES PARTNERSHIP

Introduction

The Data Futures Partnership wants New Zealand to embrace the opportunities presented by data. For this to happen, organisations must work with personal information in ways that are trusted.

Many people understand the benefits of data use, but have key questions they expect to be answered before they are comfortable sharing their personal information. These draft Guidelines set out these questions and provide advice to organisations on the kinds of answers New Zealanders are likely to find acceptable.

In some cases, simply providing the answers to the key questions will not be enough. Organisations using data for a novel purpose or in ways that affect communities with a low level of trust will need to do more to achieve community acceptance. We have set out the situations in which organisations may need to proactively engage with affected communities.

Being transparent about how data is being used is a crucial step towards community acceptance – what we refer to as social licence. We look forward to working with organisations across New Zealand to test and revise the Guidelines over the coming months as we build a consensus between communities, organisations and New Zealanders on data use.

Who the guidelines are for

Companies, government agencies and non governmental organisations

For New Zealand organisations seeking to use personal data, the Guidelines promote practices that will improve the levels of comfort and trust among those individuals providing data as well as within the wider community.

The Guidelines list the eight questions that matter most to New Zealanders. The Guidelines include guidance on how to answer those questions in a manner that is best suited to building trust. The Guidelines also provide advice on when organisations may need the additional step of active community engagement.

New Zealanders

For New Zealanders, the Guidelines are a tool to help them decide on their level of trust and comfort with an organisation's proposed use of their data.

The Guidelines list the eight questions New Zealanders should expect to have answered by organisations seeking to use personal data. The Guidelines give guidance on what transparent and reasonable answers look like. The Guidelines also give people an idea of when they should expect an organisation to consult more actively on a proposed data use.

However, every person needs to decide for themselves if a data use provides enough **Value, Protection** and **Choice** for them to be comfortable.

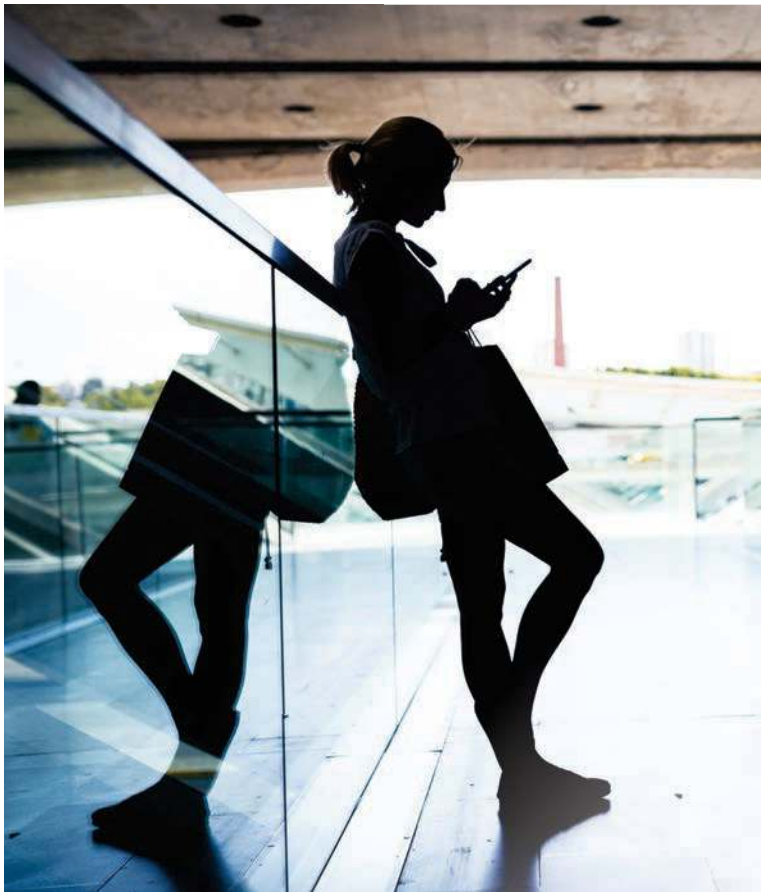
What the Data Futures Partnership is

The Data Futures Partnership is an independent group appointed and funded by the Government. We are working with all New Zealanders to create the right systems, settings and conditions to allow New Zealander's data to be put to work, maximising its benefits and making New Zealand a better place. Our overarching objective is to:

Create a competitive advantage by positioning New Zealand as a high-value, strongly inclusive, high-trust, and high-control data-sharing ecosystem.

The Guidelines are part of our wider work programme to maximise the benefits of data for the public, companies, government agencies, and non-governmental organisations. A background document, including our research and engagement with New Zealanders, is available from our website.

www.trusteddata.co.nz



Relationship of the Guidelines to the Treaty of Waitangi

Some data may be seen as a taonga by Māori. Therefore, governance of data should recognise the Treaty of Waitangi, where appropriate, and include arrangements for partnership, participation and protection. These arrangements should involve whānau, hapū, iwi and Māori communities. Further guidance on this will be provided in a companion document that is being developed about trusted use of iwi/Māori data.

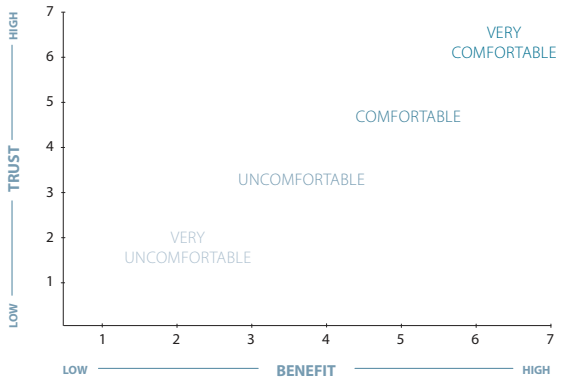
What 'social licence' is

These Guidelines encourage data use practices that will build acceptance. This acceptance is referred to as **social licence.** Our work towards social licence is underpinned by an ongoing conversation with New Zealanders to understand their feelings and perspectives on data use.

New Zealanders' attitudes to how personal data is used

To find out about attitudes to data use and sharing, we asked thousands of people across New Zealand to consider different data use scenarios. People were asked to say how much benefit they could see in each scenario and to describe their level of trust in the way data was being collected, used and shared. In our workshops, people discussed what would make them move from a low level of trust to a high level of trust.

Trust in data use is an important part of social licence: when people trust that their data will be used as they have agreed and accept that enough value will be created, they are likely to be more comfortable with its use.



Eight key questions

Our engagement with New Zealanders told us what features of data use matter most. For people to feel comfortable about a proposed data use, they first need good information on the eight key questions that we have grouped under the headings Value, Protection and Choice.

VALUE

1. What will my data be used for?
2. What are the benefits and who will benefit?
3. Who will be using my data?

PROTECTION

4. Is my data secure?
5. Will my data be anonymous?
6. Can I see and correct data about me?

CHOICE

7. Will I be asked for consent?
8. Could my data be sold?

Transparency is central

The data landscape is changing rapidly, so highly prescriptive guidelines would quickly become dated. In such an environment, we believe that transparency is central. That is why the Guidelines are organised around the eight key questions that New Zealanders want answered.

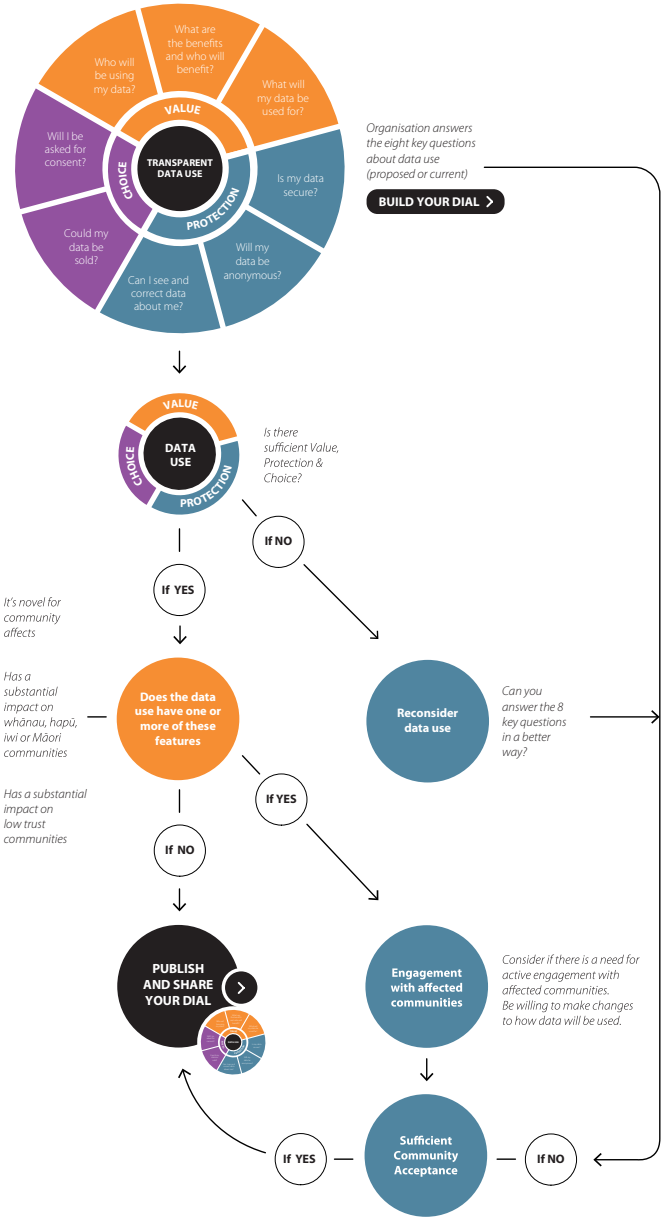
The answers that organisations provide to these questions will determine how comfortable people feel about the use to which their data is proposed to be put.

Displaying the answers to the eight key questions

The Transparent Data Use dial focuses on the eight key questions and provides an easy way for organisations to display (online or on paper) information and for people to engage with it. Each segment should be able to be "clicked through" (or opened up, if a paper version is used) to reveal the answers from the organisation for the particular data use being considered. Where an organisation uses data in only one way or in very similar ways over time, completing the dial once may be sufficient. Organisations using a variety of data sources for varying purposes should complete the dial for each distinct use of data, including new uses.

If presented as an online tool, this form of presentation allows people to choose what they are interested in and drill down as needed to access second and even third layers of information. At each layer they receive more in-depth information about each specific aspect of the data use.

How organisations should use the Guidelines



When to proactively engage with the community

Trust in a data use may be more difficult to obtain where that use is novel for the community that it will affect. If an organisation makes a significant change to the types of data it collects, how data is collected or how data is used, providing the answers to the eight key questions may not be enough – even if the answers comply with these Guidelines.

Proactive community engagement needs to be genuine and involve not just those people whose data is being used, but the broader communities who might be indirectly affected by the proposed new data use.

Organisations need to listen to what the community has to say about its proposed data use and to make changes if the community is not comfortable.

Building acceptance – social licence

Trusted data use is specific to a situation and context: it needs to be considered each time a new data use is proposed, and it needs to be maintained over time.

Organisations need to use their own judgement to decide whether active engagement is needed to achieve trust. However, if a planned data use has one or more of the following features, the need to engage should be carefully considered. The features are that the data use will:

- be novel for the community it will affect
- have a substantial impact on whānau, hapū, iwi or Māori communities
- have a potential impact on Pasifika
- have a disproportionate impact on people from small communities or people identifying as disadvantaged
- have an impact on vulnerable groups such as minors
- have the potential to have a serious impact on people's lives (for example, decisions about access to social housing or mortgages)
- involve sensitive information
- be proposed by an organisation starting from a low level of trust (for example, following a serious breach of data security).

The communities of interest may be wider than just those people who are providing their data. For example, information gathered from a group could be used to formulate policy affecting a much larger section of the community.

If the people affected have concerns, you should be willing to make changes to your proposed data use.

Most organisations will already have mechanisms to engage with communities and stakeholders. Ways to engage with communities include:

- establishing a panel of community representatives who provide ongoing checks on data use
- using existing stakeholder engagement channels, including social media and digital platforms.

Guidelines on answering the eight key questions

1. What will my data be used for?

People expect to be clearly informed about the purpose of collecting data in *specific* and *detailed* terms, including a list of the data being collected, a description of any algorithms used, and disclosure of any possible future uses. In general, people tend to be more comfortable when data is used in context, as a necessary part of delivering a product or service.

Purpose

Explain clearly the use to which the data collected will be put, for example:

We will collect only the data that is necessary to deliver the service we offer, and no more.

We will make your medical records accessible online to specialists and hospitals. This will provide them with access to your medical history if you need treatment, including in an emergency.

We will use your information to target marketing to you. We will also share it with the companies in our loyalty programme, and they will use your information to target marketing material to you by email.

We will provide your information to charities so they can approach you for support.

Provide further detail with concrete examples for people who are interested. Examples might include ways you have used research to improve services in the past.

Provide, if you can, the more detailed information as a click or drill-down option so that it can be skipped by people who are interested in only more general statements about purpose.

Where the data is sensitive, or some client groups are likely to have a low level of trust in your organisation, explain why it isn't possible to achieve the purpose in any other way (for example, by using anonymous instead of personally identified data).

Data being collected

List what data you are collecting in each of the following three categories:

Data you are requiring as a condition of supplying the service or product.	In most cases this should only be the data that is strictly necessary for the service.
Information beyond what is strictly needed for service delivery, but authorised under legislation.	Describe the purpose and state the authorisation clearly. Be explicit about any consequences of not providing this additional information.
Information beyond that needed for service delivery or authorised under legislation (eg for marketing or research).	Describe the purpose. Be explicit about any incentives you are offering in exchange for gaining the right to use customer/ client information.

Algorithms

If you use algorithms (formula-based decision tools) to make decision e.g. to determine whether to grant loans, what interest rate to charge, or as part of a recruitment process:

- Explain how these work and which pieces of data are used
- Advise clients of other inputs to your decision processes (e.g. does a staff member review applications?)
- Offer the applicant the right to contest the decision, including the data that was used in the algorithm.

Future uses

State clearly if the data might be used for other purposes in the future and, if so, what other purposes.

If it isn't possible to be precise about possible future uses, assure the person that they will be asked to give consent to that use before it occurs.

2. What are the benefits and who will benefit?

People want to know what the benefits are from a particular data use and who benefits. When data will be used as a product in its own right for commercial gain, organisations should explain what the person is gaining in exchange and what the business is gaining.

Benefits

Explain what personal benefits the individual or their family can expect. Also explain any wider benefits (for example, to the organisation, an iwi or society).

Be specific and provide evidence about how the proposed data use will lead to the benefits claimed.

Proven outcomes are the best way to demonstrate benefits. Provide an example of a similar data use and the resulting benefits or a concrete example of an expected benefit from the proposed use.

Marketing

Where personally identifiable data is collected to target people for direct marketing and advertising, the benefit accrues mainly to the company as profit. Therefore, people's level of comfort is likely to be less, and people may expect to receive significant personal benefit.

Explain what benefits are being offered in exchange for the use of personal data (for example, free services or access to services at a lower charge).

Explain whether other organisations are benefiting from the personal data, including which organisations and how they are benefiting.

Give people the ability to opt out of direct marketing and advertising that uses their data. Make information about this option easy to find and make it easy to opt out.

3. Who will be using my data?

People want to know who will be using or sharing their data.

Data on individuals can be matched across datasets to give a larger, richer set of information (for example, for research or statistical purposes). Data can also be linked to enable personal identification of an individual, and, therefore, the ability to approach individuals for a variety of purposes such as with offers of services, advertising or requests for donations.

Linking or sharing data

State clearly if you will or will not be linking the data with any other datasets or sharing the data with other organisations.

Identify any dataset that will be linked, what other dataset it will be linked with, and for what purposes the data will be linked.

Identify any data that will be shared with other organisations – which organisations and for what purposes.

4. Is my data secure?

People want to know that organisations that will use and share their data have rules and controls to minimise the risk that the data is mishandled.

Data security

Build data protection safeguards into your products and services from the earliest stages of development.

Outline the measures you have to keep data secure and measures taken by the agencies that you will share data with. Where data is sensitive and personally identified, include:

- which types of personnel will have access to the data and their credentials (for example, their training, that there were referee checks, and that they have signed declarations of confidentiality)
- the access rules and protocols in place and the consequences for staff who break them
- security arrangements that prevent unauthorised access to the data.

Tell people what you will do if there is a data breach. Ideally, you should inform the people affected as soon as possible to give them the best opportunity to protect themselves.

5. Will my data be anonymous?

In many cases, data must be personally identified in order to achieve the purpose of delivering a service or product. Personally identified data is one in which the names or addresses (or other identifying information) of the person can readily be established. People are willing to have their personally identified data shared in a limited way when they can see significant benefits from the data use and have trust in who will use it. However, provided the benefits can still be gained, it is preferable to use anonymised data.

Anonymising data

Unless data needs to be personally identified to achieve its purpose, always use anonymous data.

Where you intend that data will be anonymous, rather than a guarantee, many people may be satisfied with a high-level assurance such as:

We use data in a form that will not identify you personally, and we do not use it to target you or other individuals. While it may be theoretically possible to re-identify you from the data we hold, we take several measures to make that highly unlikely.

For people with a greater level of concern or where the data is more sensitive, describe the measures you have in place to reduce the risk of individuals being personally identified, but stop short of providing a guarantee. Include:

- techniques you are using that make re-identification more difficult, such as encryption, pseudonymisation (for example, where names are converted into unique numbers), data being analysed at an aggregated, rather than individual, level, and adding 'noise'
- controls on who will be able to access the data and for what purposes
- assurances about sharing the data – with whom and for what purpose
- assurances about linking the data with other datasets and steps to minimise the risk of re-identification
- assurances that the people accessing the data are prohibited from attempting to identify individuals
- a date for the destruction of data after use.

Provide these details through an online link that allows people to drill down if they want more information and avoid your statement appearing too long and complex. People who already have a high level of trust in your organisation and the proposed data use are unlikely to need this further detail.

6. Can I see and correct data about me?

People want to be able to find out what information is held about them, by whom and for what purpose. An ongoing audit trail, showing how information has been shared and used over time, should be available on request.

People also want to be able to correct wrong information about them. Incorrect information in data repositories can be extremely damaging to the individuals or families concerned.

The following guidance is aimed at data uses where sensitive data is involved or where the potential consequences for individuals are serious. In other situations, a lower standard of access to and ability to correct data may be acceptable, provided all requirements under the Privacy Act 1993 are met.

Clients' ability to see their data

Explain how people can find out what data is held about them, by whom, and for what purpose and how it is used and shared.

People will have higher trust levels in your organisation, if the organisation makes a commitment to providing

people with the data it holds about them.
Explain any circumstances in which data held about an individual will not be provided. Rather than list the exceptions in the Privacy Act 1993, explain the circumstances in which your organisation will not provide data.

Clients' ability to ask that their data be transferred

Be clear about whether you are willing and able to transfer data to another organisation at an individual's request.

Correcting data

Provide a phone number that will directly connect an individual with someone qualified to deal with sensitive requests.

Put suitable safeguards in place to prove that the person requesting the information is the person to whom the data relates.

Act promptly on requests to correct data.

Establish a process, with a timeline, for responding to requests for corrections and share this proactively with your customers. This process needs to include how data that has been shared with another organisation will also be corrected.

Explain how you will be accountable for any failures to correct wrong information, including the consequences if your staff disregard requests to correct information.

Offer to meet with any person who has requested a correction that you will not or have not acted on. This provides an opportunity for you to discuss your reasons and for the person seeking a correction to explain their situation.

7. Will I be asked for consent?

In some cases, consent is not legally required. However, people want the ability to give permission for specific data to be used by specific organisations for specific purposes. They also expect:

- to be notified before any new data use or sharing occurs
- time limits on permission
- to be able to withdraw consent in the future.

It is common for consent to be asked for as part of long, legalistic statements of terms and conditions. These are frequently skipped over by people wanting to access the service or product on offer, raising the question of whether 'consent' in these circumstances is genuine or informed.

The European Union's new General Data Protection Regulation imposes quite demanding standards for consent. The following guidelines draw on these regulations.

Ensuring consent is informed

Ensure consent is informed by answering all eight key questions in the Guidelines.

Be clear about where people have a choice and where data provision is a condition of receiving the service or product. Use the following three categories.

Data you are requiring as a condition of supplying the service or product.	In most cases, this should be only the data that is strictly necessary for the service.
Data beyond what is strictly needed for service delivery, but is authorised under legislation.	Be explicit about any consequences of not providing this additional information.
Information beyond that needed for service delivery or authorised under legislation (for example, for marketing or research).	Consider seeking this information, and consent for its use, separately. In some cases, this might best be done after the service or product has been delivered. Be explicit about any incentives you are offering in exchange for gaining the right to use customer/client information.

Obtaining consent

In most cases, it is desirable to explicitly ask for consent to use data about individuals, even when the data is anonymised.

Ask people to give consent through a positive action (for example, by ticking a box or clicking an 'I agree' statement).

Make the request for consent short and easy to understand and display it separately, rather than as part of a lengthy terms and conditions statement.

Give people as much choice as possible about which organisations will use the data and for what purposes (for example, so a patient can choose to share their data with a hospital but not with a pharmacist). Make it easy for people to adjust their choices over time.

Make it as easy to withdraw consent as it is to give it.

Where people are in vulnerable situations (for example, a person using a rape counselling service or a women's refuge), it is especially important to limit the initial data collection to the minimum needed for service delivery. Issues of data use and consent should be addressed at a later stage such as when the client has finished with the service and can feel free to refuse the request.

Where the information being collected relates to a person under 16, seek consent from their parent or guardian.

8. Could my data be sold?

People are concerned about the potential for their personal data to be sold. Selling personal data without explicit permission can severely undermine trust.

Under the Privacy Act 1993, 'personal information' (that is, information about an identifiable individual) can be disclosed in only limited circumstances. However, even the sale of non-identified information could be of concern, so organisations need to clearly state when they sell data.

If there is no possibility that your organisation will sell personal data – information about individuals, whether personally identified or not – state this clearly.

Personally-identified data

If the data you collect from customers could be sold in an identified form, seek consent unless the sale is part of the sale of a business as a going concern.

If a business is being sold as a going concern, advise customers and provide an opportunity for them to opt out of the customer database.

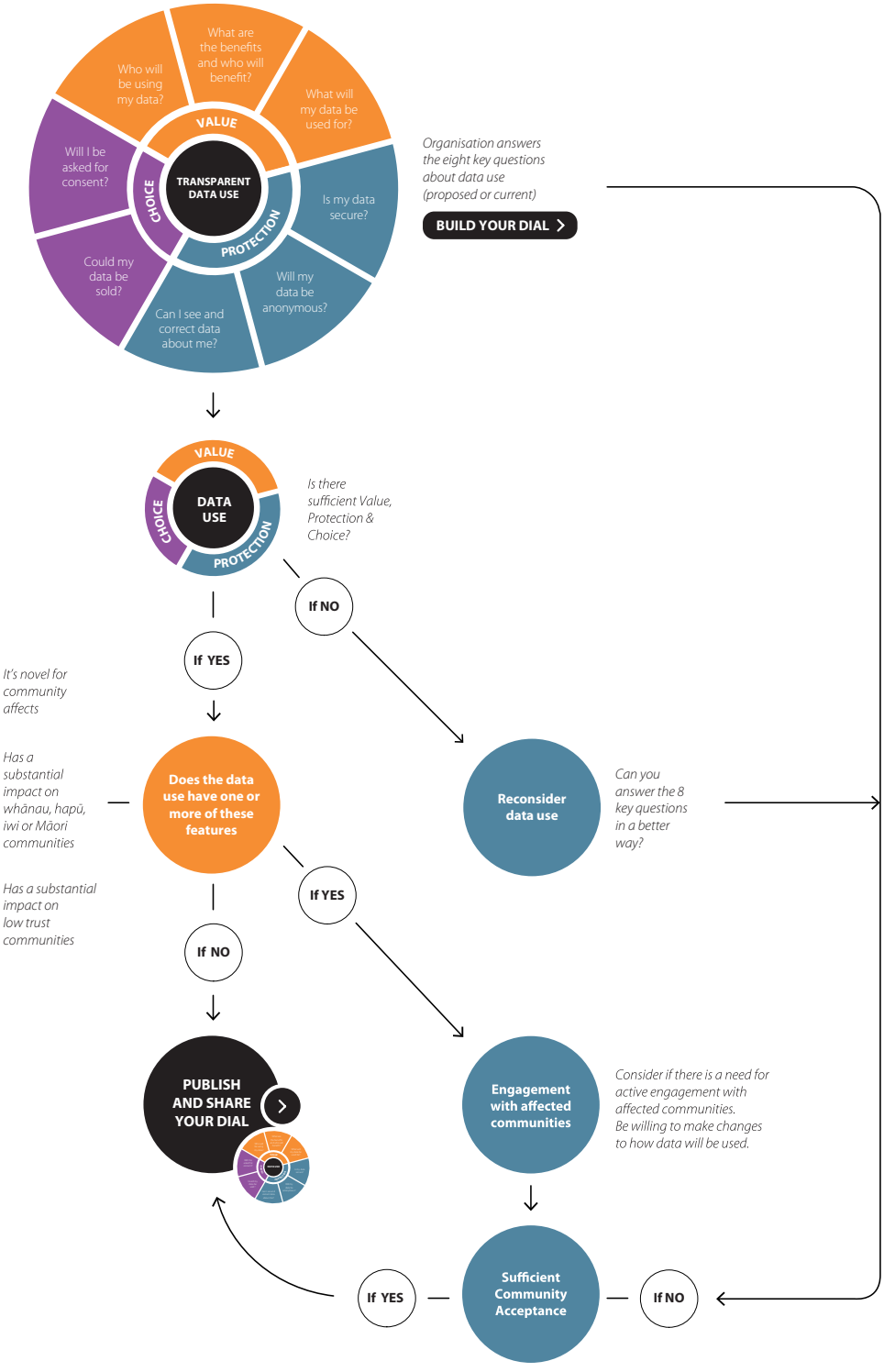
Non-identified data

Data sold in an anonymous form could be linked or matched with other data that could make it personally identifiable. If you intend selling anonymous data:

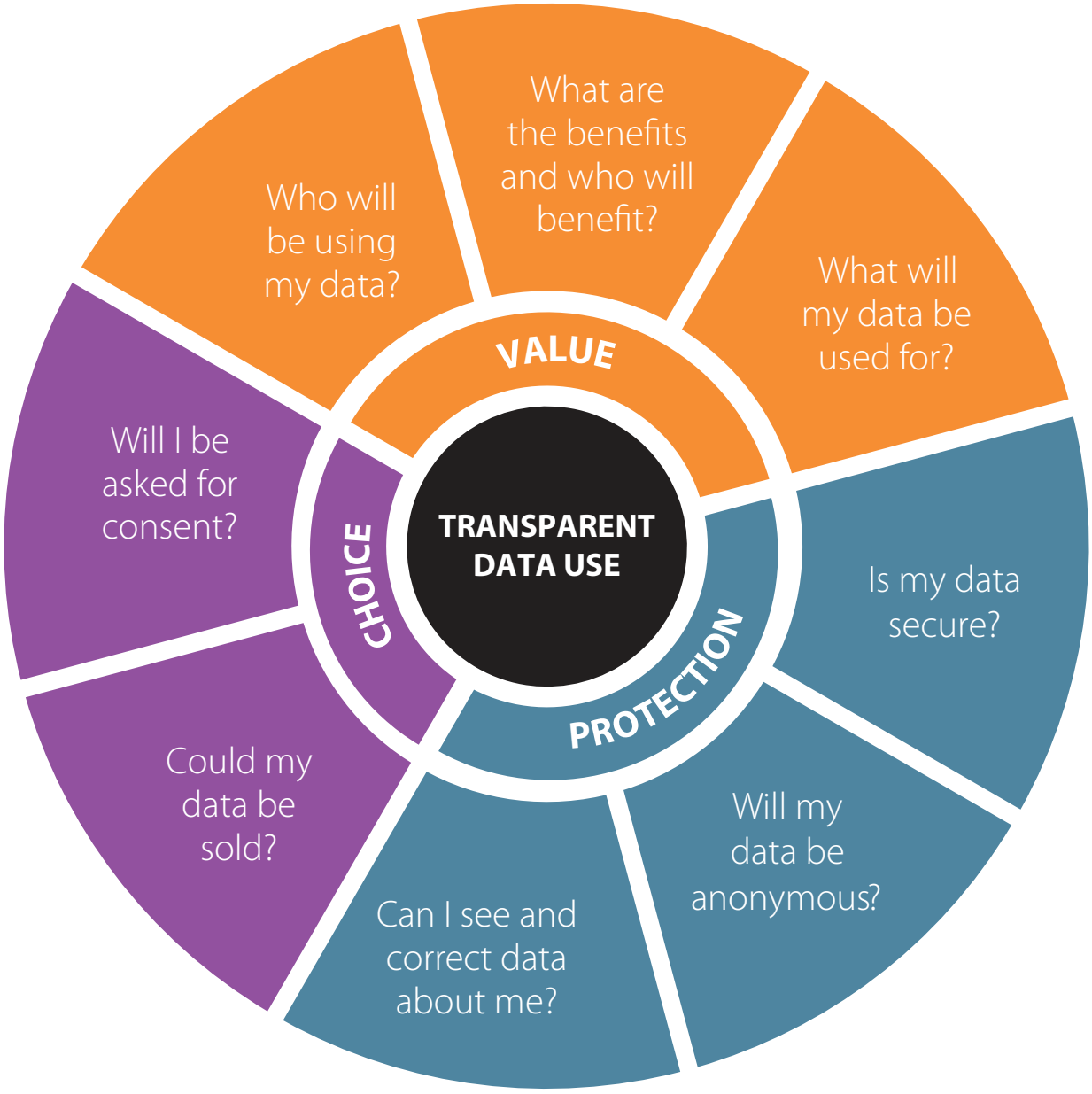
- tell customers who the data is being sold to and for what purposes (for example, marketing)
- seeking consent first is preferable.

For further information on the background of this guide please refer to our Background doc here: *https://trusteddata.co.nz/wp-content/uploads/2017/08/Background-Trusted-Data.pdf*

How organisations should use the Guidelines



The transparent data use dial



DATA FUTURES PARTNERSHIP