Food Data Trust

Legal, Structuring and Governance Report

March 2021

Contents

1. Introduction and Executive Summary of Recommendations

We have been instructed by the University of Lincoln to prepare a report identifying key legal and governance issues arising in connection with the potential establishment of the FSA Food Data Trust ("**FDT**") and to provide options for governance arrangements, contractual frameworks and, potentially, an appropriate corporate vehicle for setting up and operating FDT as a data trust.

While this legal report may be read on a stand-alone basis, it has been prepared in conjunction with the report prepared by the University of Lincoln and commissioned by the Food Standards Agency entitled "Food Data Trust: A framework for information sharing". That report examines the role of information sharing in ensuring safe food production supply networks and proposes a data trust framework to more efficiently enable secure data sharing for the benefit of all stakeholders in the food system.

In this report we have used the term 'data trust' broadly, to mean a trust framework for digital collaboration.

Establishment of a data trust can be a mechanism for achieving a defined set of aims including:

- enabling data to be shared and exchanged, moreover, selectively, for the benefit of those sharing or exchanging the data and possibly also for some broadly conceived public benefit purpose;
- respecting the interests of those with legal rights in the data;
- ensuring the data is used ethically and in accordance with the rules established by the data trust; and
- ensuring that whoever holds or uses data which is subject to the data trust rules does so safely and securely, and that data is dealt with appropriately (for example by deletion) if participation in the data trust or the data trust itself, comes to an end.

Specific data trusts may also have one or more of the following aims and characteristics:

- collective and/or selective management of stakeholder rights and interests, (including any sharing of benefits received by the data trust);
- standard set of rules etc. to govern all data sharing;
- custodian/steward makes decisions on behalf of data providers/data users;
- the generation of income and other benefits derived by or from the provision of data services in order to support the activities of the data trust and to make the data trust sustainable; and
- ability to evolve to have new purposes, governance and working methods.

Executive Summary of Recommendations

1. **Purpose:** following appropriate consultation with its stakeholders, FDT should finalise and clearly express its statement of purpose and related objectives. That purpose and those objectives will be the touchstone for FDT's activities and should be reflected (including, where appropriate, as binding obligations) in its governance framework, rules and contractual framework governing the provision and use of data.

2. **Legal Form:** FDT could initially be established as a contractual relationship between stakeholders or as an entity with separate legal personality. Section 3 sets out the pros and cons of each approach and provides an indication as to what factors point towards which approach. If an entity with a separate legal personality is thought appropriate, a company limited by guarantee would likely provide the most appropriate form.

3. **Rules:** FDT should begin work on the development of rules that set out how FDT will function and that will govern its basic operations. The rules will bind all of FDT's participants – along with FDT itself if it is a distinct legal person – and can be used to underpin certain overarching values or principles, such as the independence of FDT's decision-making. Stakeholders and prospective stakeholders should be consulted as part of the process of drawing up the rules.

4. **Independence:** in developing the governance framework and writing the rules and (if applicable) articles of association for FDT and the contractual framework under which data will be provided and used, it should be borne in mind that, preferably, no one set of stakeholders should be able to dominate or dictate FDT's direction or decision-making.

5. **Governance Framework:**

    a. Whether or not FDT has a separate legal personality, we recommend an initial two-tier governance structure which would comprise relevant stakeholders – at the membership level – and, potentially, nominated representatives of certain sets of stakeholders – at the level of a council or board.

    b. Depending upon the maturity of FDT's business, it might also be necessary to appoint a further layer of executive management that would report to the council or board.

    c. It may also be desirable to establish advisory committees to advise the council or board on matters such as data ethics and technology.

d. If FDT has a separate legal personality, then the governance framework could be incorporated into its articles of association or equivalent and consideration could also be given to the adoption of a corporate governance regime such as the Wates Corporate Governance Principles for Large Private Companies. If FDT has no legal personality, the governance framework would need to form part of the binding multilateral or bilateral agreements to which the various stakeholders are party.

e. It is of critical importance that the governance structure is acceptable to FDT's stakeholders – in particular, data providers and data users – and this structure should, therefore, be road-tested with potential stakeholders.

f. The governance structure should not be so complex that FDT is unable to make timely operational decisions. While representation and balance will be important for the gaining of stakeholder trust, so will the efficiency of FDT's day-to-day decision-making.

g. A council or board that engenders confidence among all stakeholders will be an asset to FDT. It may, therefore, be worth considering some form of representation for data users within the governance structure. Some form of annual stakeholder meeting could also be considered.

h. Certain material decisions could be reserved to broader stakeholder representation, requiring voting outside the board or council structure. In corporate terms, this would be a form of shareholder resolution as opposed to a board resolution.

6. Contractual Framework for Data Provision and Use:

(a) If FDT has no separate legal personality, we envisage a multi-party code or contract among all data providers and users. Conversely, if FDT has a separate legal personality, we envisage it entering into bilateral contracts with individual data providers and data users that are consistent with and may incorporate the rules described above.

(b) We recommend that FDT consult with stakeholders, including representatives of the prospective data user and data provider communities, on the form of the data provision and data use agreements and on the key issues that will need to be addressed from the perspective of those stakeholders. By way of example, to the extent that University researchers will engage with FDT, either as data

providers or data users, careful consideration will need to be given to obligations of the University to provide open licences to research results including data generated in the course of research activities.

(c) In order to establish appropriate terms and conditions to govern the provision and use of data, a working group should be set up to manage consultation with stakeholders and to consider the issues identified in Annex 2 including the potential consequences for the terms and conditions under which data is provided and used:

- the nature of FDT as data steward1 and a provider of data services;
- the nature of the data that FDT will hold or to which it will provide access;
- the nature and identity of the different categories of data providers;
- the nature and identity of the different categories of data users;
- risk allocation and liability flows among the data providers and data users and, if FDT has a separate legal personality, FDT;
- the financial and funding model for FDT.

(d) If there will be numerous different scenarios under which data will be provided, held and used, and/or depending upon the nature and sensitivity of the data in question, a suite of different template data provision and data use agreements may be required to govern the various different scenarios.

7. **Termination and Winding Up**: FDT should consider now how to mitigate the effects on its stakeholders of a winding up of FDT. In particular, FDT's rules, together with the terms of the data provision and data use agreements, should make clear what happens to the data upon a solvent or insolvent winding up of FDT. To deliver sustainability, FDT must make

[1] If the data trust is a distinct legal person, it may bear this responsibility (and liability) directly. If, however, it has no distinct legal personality, this responsibility will be borne by the stakeholders collectively in such manner as they agree between them. This usage of the term 'data steward' should be distinguished from the idea that a designated individual (whether internal to the data trust or external and providing services to the data trust) might be charged with overseeing this aspect of the data trust's operations.

provision in its financial model for funding to meet data curation obligations beyond the winding up of FDT. If FDT has no distinct legal personality, these obligations will fall upon the stakeholders themselves. Whether the data trust has a distinct legal personality or not, consideration will also need to be given to the withdrawal (whether voluntary or forced) of stakeholders from the data trust.

Risk Management

This report focuses on legal options, recommendations and practical steps to facilitate the establishment and sustainable operation of FDT. However, given that the report has been commissioned from us by the University of Lincoln, and that FDT may, initially at least, be partially dependent on resources provided by stakeholders in order to function, we should acknowledge that the establishment of FDT does create risks, as well as benefits and opportunities, for the University and other stakeholders with whom the FDT is closely associated. Examples of such risks include:

1. **Investment risk**: it appears likely that initial contributions will take the form of in-kind (e.g. human capital) rather than financial contributions. Over time, it is hoped that the sustainability of FDT will be supported by revenue streams that can be reinvested in its activities. Until that time, however, any in-kind contributions will be at risk.

2. **Reputational risk**: those stakeholders with whom the FDT is closely associated, should be aware that a failure of FDT may have a negative impact on reputation. The risk of any reputational damage for stakeholders arising from cyber or data breach of FDT will be mitigated by the fact that any technical resources supplied by stakeholders will likely only be made available (if at all) for a limited time and small-scale proof of concept.

3. **Contractual and financial risk**:

    - if FDT has no legal personality, FDT's stakeholders will have to enter into direct contractual relationships for the provision and supply of services and will therefore be directly liable in respect of such. Each stakeholder will also be responsible for its own tax position in respect of the operation of the FDT.

    - if FDT has its own legal personality, it will be able to enter into contracts in its own right (and also employ its own employees). This would, in principle, shield FDT's stakeholders from financial liability in respect of the acts or omissions of FDT. That said, at least in its early days, it may

be that third parties would look for some form of guarantees or security in respect of the financial or other obligations of FDT.

4. **Data and GDPR risk**: The personal data that will be produced, shared or processed by the stakeholders of the FDT will need to be mapped to ensure that suitable arrangements are put in place for the FDT and, importantly for stakeholders to identify their roles for any processing activities. This includes where a stakeholder may also act as a supplier to the FDT. The basic accountability framework for sharing personal data is the same whether the FDT has its own legal personality or not, however the specific implementation of the compliance framework will vary based on the factual situation. There is not a statutory requirement for accountability for non-personal data, though we recommend that the framework for data mapping, apportioning responsibility and liabilities is a model to be used for all data sets.

   (a) The accountability framework should include:

   - the data to be shared and for what purpose;
   - who the data will be shared with (internally and externally);
   - the lawful basis for sharing the data;
   - permitting the exercise of fulfilment of individuals' rights;
   - any risks assessments carried out for the sharing/processing of the data;
   - any limitations on the use of the data by the parties, and any requirements for further use;
   - terms for security and auditing of the operation of the framework by the stakeholders and suppliers and; data return or deletion;
   - terms for engagement with a regulators;
   - considerations for standards and data quality; and
   - considerations for apportionment of liability in the event of data loss, or infringement of statutory obligations.

   (b) If the FDT does not have its own legal personality, the stakeholders will need to determine the individual

responsibilities of the purpose and means of processing data. This will include stakeholders who will provide services to the FDT and situations of joint responsibility for the use of the data. This will require a data map to be created with the nature and scope of the data to be collected and shared within the FDT to determine each party's role, and whether that party is acting as a controller or processor, or both. In some cases parties may be acting joint controllers, as well as a supplier (e.g. hosting the data). Based on this information appropriate data sharing agreements need to be put in place (whether bi-lateral or multi-lateral) and, most importantly agreements need to be clear where one party is providing services.

(c) If the FDT has its own legal personality, the above data mapping and accountability framework will be similar. However, the practical application will be different, as the FDT will have its own legal compliance responsibilities and may act as a controller and/or processor in its own right, as distinctive from the activities of the stakeholders. This will require the FDT to consider its own compliance obligations, entering into contracts with suppliers (particularly for hosting and processing activities) and liability provisions based on the risks of the data and processing activities.

5. **Competition law risk**: The sharing of certain (sensitive) confidential information between competitors can amount to an infringement of the competition law rules. The exchange of any commercially sensitive information must be minimised so that it goes no further than necessary to achieve the legitimate purpose of FDT. The type and scope of the information being shared (for example age, content and frequency) will need to be considered and it may be necessary to aggregate and/or anonymise the data before it is accessible. Privacy enhancing technologies (PETs) will also be worth investigating in this context. The purpose of FDT and how the data is used will also need to be carefully considered. If the (unintended) effect of FDT is, for example, that certain suppliers end up being "blacklisted", they may claim that FDT is operating as an anti-competitive agreement (a type of "collective boycott"). Similarly, if FDT is used as a collective purchasing arrangement, these can in certain circumstances also amount to an anti-competitive agreement. FDT, in addition to the providers/users themselves, could be fined by the UK Competition and Markets Authority ("**CMA**") if it is found to be a "facilitator" of an anti-competitive data sharing arrangement.

In due course, a competition law protocol should be drafted setting out such things as FDT's purpose, objectives, membership criteria, the parameters of what can and cannot be shared or discussed, the scope of interaction

outside the arrangement, risks and mitigating steps, etc. A necessary precursor to this will be to establish how FDT will function in practice and on a day-to-day basis. The protocol could form part of a more overarching governance document or policy, or it could be a stand-alone document. If there is a desire for discussions to take place between market participants/competitors before the competition law protocol is in place, we would recommend putting a preliminary protocol in place to ensure that these initial discussions are also compliant.

It is important that the founding stakeholders actively consider such risks and seek to mitigate them in implementing the recommendations set out in this report, as well as monitoring existing and new risks on an on-going basis. It is recommended that risk registers be established, both at the level of individual stakeholders and at the level of the FDT and updated regularly to reflect the changing nature of FDT, its relationship with the stakeholders and the associated risks.

2. Purpose

For the reasons we set out below (see Rules and governance considerations), any data trust should begin with a clear statement of purpose. Not only will a compelling statement of purpose facilitate trust among stakeholders, but it will also provide the ultimate measure against which governance bodies and stakeholders can check to ensure that the data trust remains true to its purpose. To this end, we have extracted the following definitional elements from various communications provided to date:

a trust framework for food standards

…to make food safer, ease regulatory compliance and reduce friction in the sharing of information relating to food standards

The fulfilment of these goals will in turn facilitate:

greater resilience in the food system

In Purpose and rules, below, we discuss how elements of the purpose and these objectives can be enshrined within FDT and, if FDT has its own legal personality, accepted by FDT as legally binding obligations, which will be enforceable against it by certain of its stakeholders.

Recommendation: following appropriate consultation with its stakeholders, FDT should finalise and clearly express its statement of purpose and related objectives. That purpose and those objectives will be the touchstone for FDT's activities and should be reflected (including, where appropriate, as binding obligations) in its governance framework, rules and the contractual framework governing the provision and use of data.

3. Legal Form

Having decided upon FDT's purpose, the legal form that it will take, will need to be identified. The proposal states that the FDT will be a:

"[legal entity] acting as a Trust Framework to enable and facilitate data sharing amongst an organised community of willing partners who would form a federation that would have a collective voice. This could take the shape of a not-for-profit foundation or institution acting on behalf of this community."

As outlined, the aim is to design an ecosystem of trust. FDT will sit at the heart of this ecosystem. There are two broad possibilities as to the legal form this should take:

- a contractual model: this would involve a standardized form of data sharing agreement without the establishment of any form of additional legal structure or personality
- a corporate model: this would involve the establishment of a company or other legal person which would be responsible for various tasks relating to the provision of access to and use of data. The documents of incorporation would be supplemented by contractual arrangements.

In the contractual model, all of the rules for the operation of the data trust will need to be set down (and repeated) in a series of bilateral (or multilateral) agreements between data providers and data users. This, when combined with the fact that each party would need to take action on its own behalf to enforce the terms of that agreement against any counterparties, makes it likely that providers of data will only be willing to provide access to data on highly specific terms. Where the aims of the stakeholders will require significant flexibility and scalability then a simple contractual model is unlikely to be most appropriate model.

In the corporate model, there is a degree of flexibility and scalability that is lacking from the contractual model. This model requires a greater degree of trust on the part of stakeholders, however. In conceptual terms, data providers are being asked to give up a degree of control over the data they are providing – presumably in return for some incentive or reward. They will only do so if they feel they can trust the structure or organisation that has been set up to effect this.

We consider various forms of company below. Whichever form is chosen, the company in question would operate as the data platform owner and manager and enter into contractual arrangements with providers of data and proposed users.

The contractual terms would allow for:

- required investment in the company to fund infrastructure requirements such as platform development and maintenance – this could be by way of non-returnable capital contribution or loan from either the data provider or data users as circumstances merit;
- required returns on supply of data;
- required charges for use of the data;
- other contractual rights and obligations specific to the circumstances including access to and usage of data.

Returns and charges could be related to commercial exploitation or fixed. The contract terms would dictate all required obligations and liabilities between the contracting parties.

Here, we focus on three forms of company: a company limited by shares, a company limited by guarantee (a CLG) and a community interest company (a CIC). We do not consider here the possibility of employing a legal trust as we believe that such a choice would impact negatively upon the ability of the FDT to achieve its objectives. Nor do we consider here, the possibility of employing a Limited Liability Partnership (LLP) to this end. While LLPs are similar in some ways to companies limited by shares, they are transparent for tax purposes and any profits generated by an LLP will be treated as the profits of its members. We do not, in this note, provide any advice in respect of any tax, commercial or accounting aspects of adopting any of the legal structures for FDT

We can, of course, provide more detail if you wish to discuss any of the above options further.

The principal differences between the three forms of company mentioned above are summarised in the table set out in Annex 1.

It is unusual for a CLG to be used as a vehicle for a profit-making enterprise and a CLG's articles of association will often (but not always) prohibit or restrict the making of distributions to members. Rather than shareholders sharing in its profits (as would generally be the case with a company limited by shares), any profits made by a CLG will generally be applied to a not-for-profit cause – in this case, FDT's purpose.

The key questions here are:

- is FDT to be capable of paying a dividend to its shareholders (if any); and
- will FDT require access to external finance?

In some past research into data trusts with which we were involved, potential stakeholders stressed the importance of the data trust being independent and expressed concerns about any data trust making profits, other than to the extent such would be applied to the development of the data trust's business.

Our understanding from discussions with you is that in the case of FDT: (i) it is not envisaged that profit or surplus generated by FDT will be distributed to its members; and (ii) it is not envisaged that FDT will seek to raise debt or equity finance. Rather it is expected that FDT's activities will be financed through third party grant funding and from revenue generated from its own activities including the provision of data services.

These factors suggest that a CLG may well be the most appropriate vehicle for FDT, provided that if the focus of FDT changes over time and it broadens its horizons to encompass more purely commercial activities, then establishing a trading subsidiary company limited by shares could also be considered.

It should be borne in mind that a CLG (unlike a company limited by shares) does not have share capital that it is able to show on its balance sheet. This often makes it more difficult for a CLG to raise external debt finance. The alternative possibility available to companies limited by shares, of investment by way of equity finance, is precluded here because of the structure of the CLG. Because of these difficulties, and for the sake of completeness, we think it worth drawing attention to CICs as a further alternative corporate vehicle.

A CIC is a limited liability company which has been formed specifically for the purpose of carrying on a business for social purposes, or to benefit a community. Although it is a profit-making enterprise, its profits are largely applied to its community purpose rather than for private gain. This is achieved by way of a cap on any movements of value from the CIC to its shareholders or members (such as by way of dividends).

This model allows shareholders to share in some of the profits of the data trust, while ensuring that the CIC continues to pursue its community purpose. CICs are regulated by the Office of the Regulator of CICs (the CIC Regulator), and are required to file a community interest statement at Companies House, which is also scrutinised by the CIC Regulator. The CIC's share capital would appear on its balance sheet, thus increasing its ability to raise external finance. The CIC Regulator decides whether an organisation is eligible to become, or continue to be, a CIC and it is worth noting that some representatives of the CIC Regulator have in the past expressed a degree of scepticism as to whether or not a CIC is an appropriate vehicle for a data trust.

From our understanding of the facts and circumstances here, we believe that a CLG is the most appropriate legal form for FDT.

If it had been intended that FDT be capable of paying dividends to shareholders, then a company limited by shares or a CIC might have been more appropriate than a CLG (recognising that the CIC Regulator would first have to decide whether FDT is eligible to be a CIC and that the ability of a CIC to pay dividends to non-asset locked shareholders is limited to 35 per cent. of its distributable reserves).

Similarly, if there had been concerns over FDT's ability to raise finance, then a company limited by shares or a CIC may have been more appropriate than a CLG.

If, however, as we understand to be the case, surpluses generated by FDT's activities (including the provision of data services) are to be applied to its business and its financing arrangements are secure, then a CLG will likely assist in gaining traction with those stakeholders who believe that the independence of the data trust would be compromised by virtue of its ability to pay dividends to shareholders. Of course, such financial sustainability is predicated on the forecasts of income generation being relatively accurate.

The choice of vehicle should be made, bearing in mind that once a structure has been chosen, it will not be possible to convert that structure into an alternative structure. By way of example, it will not be possible to convert a CLG into a company limited by shares (or vice versa) and nor will it be possible for a CIC to discard its status as a CIC. However, as indicated above, there will remain the opportunity in the future to establish a trading subsidiary of FDT, which may be a company limited by shares, should facts and circumstances change and it be appropriate to do so. The use of trading subsidiaries is a path well-trodden by the University already in managing the research, education and commercial activities in which it is engaged.

We note the potential for FDT to operate on an international basis; however, we believe that the first step should be its establishment on a national basis. Once the concept has been proven, other states – and nationals of other states – will be more receptive to the idea of international cooperation in this respect.

Recommendation: If it is intended that FDT should have separate legal personality, it should be incorporated as a company limited by guarantee. Implicit within this is the expectation that any profits generated by it will be applied to a not-for-profit cause – that is, FDT's purpose.

4. Rules and Governance Considerations

Previous research with which we have been involved has shown that a sense of trustworthiness is essential to enable any data trust to operate. Good governance has the ability to engender a sense of trustworthiness and therefore has the power to 'make or break' any data trust.

In the context of a data trust, trust has to flow in a number of different directions. For example, a data provider will want to be able to trust any steward of its data to act appropriately and responsibly and not to misuse the data entrusted to it, while a data user will want to be able to trust in the integrity of the data on which it is relying. Moreover, where data is particularly sensitive, there may be a wider public concern that will need to be addressed before a data trust can gain any real traction. An effective governance model will need to address all of these concerns.

Before we consider governance in more depth, it is worth noting that even the best governance will do little to engender a sense of trustworthiness, if it is not transparent in nature and underpinned by some form of accountability and sanction. While this can be achieved partially from within a governance framework, interested parties will, in certain circumstances, inevitably need access to other external forms of redress and enforcement. Most obviously this might take the form of access to the courts or arbitration to determine disputes or enforce rights, but it might also – at some point in the future and as has been suggested in recent research on the viability of data trust models – include access to a regulator who could be responsible for enforcing a code of conduct.

5. Purpose And Rules

As stated above, a data trust should begin with a clear statement of its purpose. In this case, our working assumption is that FDT's purpose is:

…to constitute a trust framework for food standards

This high-level statement would be supplemented by more detailed goals, such as the objectives set out above (see **Purpose**); namely, to make food safer, to ease regulatory compliance and to reduce friction in the sharing of information relating to food standards.

One of the key structural decisions regarding the operation of FDT is whether its role will be to monitor and control individual transactions or whether it will, rather, be responsible for monitoring or certifying that its relevant stakeholders have established and agreed terms that will then govern the exchange of information between them.

The purpose could, if FDT has a separate legal personality, be included in FDT's articles of association; however, given that the FDT's shareholder or member base will likely not correspond to its stakeholder base, it may make more sense to treat its purpose in a similar manner to the rules that will underpin that purpose (see below).

We note that some degree of "road testing" has already been undertaken with respect to this purpose, but in any event suggest that continuous feedback is obtained from potential stakeholders. The greater the level of approval from potential stakeholders, the more likely they are to engage with the project.

Beneath (and underpinning) FDT's purpose, will sit its rules. These will set out in more detail, the way in which FDT will function, so as to allow it to achieve its purpose. While not necessarily a public document, the greater the degree of transparency as to FDT's operations, the greater the level of confidence that stakeholders and the wider public will be likely to feel in its functioning.

The rules will need to cover FDT's basic operations; that is:

- in broad terms, the nature of the data that will be collected;
- the identity or class of the persons or organisations with whom it will be shared; and
- the uses to which such persons or organisations will be entitled to put that data.

The rules could be used to underpin certain overarching values or principles, such as FDT's independence (see Independence, below) and to ensure compliance with the competition law rules (see Annex 4).

The rules should bind all of FDT's participants (including, if FDT has separate legal personality, FDT itself). In practice, this could be achieved either by having the participants sign up to the rules as a stand-alone document, or by incorporating the rules by reference into FDT's operational agreements, for example, a data provision agreement or data use agreement. As mentioned above in respect of the purpose, the rules might be incorporated into FDT's articles of association; however, to the extent FDT's shareholder or member base does not correspond to its stakeholder base, this measure may not provide much comfort to its stakeholders.

The rules would cover a variety of other issues, including:

- FDT's technical architecture and the role (if any) FDT will play in the storage and processing of that data;
- interoperability between FDT and each of its participants and potentially, as between participants (i.e. the shared technical standards that will apply to data provision, storage, use and processing);
- how FDT will make decisions and the extent to which stakeholders and participants will be consulted and have a role in decision-making;
- the independence and transparency of FDT;
- the obligations of each participant and FDT (such as the extent (if any) to which FDT is expected to engage in any form of monitoring or audit of data use, particularly in respect of any personal data);

- information security (in particular, given the fact that the relevant data will be held centrally);
- any applicable service levels; and
- any significant departures from FDT's standard form data provision agreements and data use agreements.

Please note that in all instances where we refer to FDT undertaking certain actions or making decisions, if FDT has no legal personality, we are really talking about FDT's participants taking these actions and making these decisions, in accordance with FDT's purpose and rules.

Alongside any consideration of rules, the consequences of any stakeholder failing to follow those rules will also need to be considered. Proportionate and transparent methods of censure - that are consistently applied - will not only encourage compliance but also strengthen the sense of trustworthiness that the data trust will require in order to operate. The consequences of breach will vary depending upon the seriousness of that breach. Minor breaches could be dealt with by way of warnings or fines; more serious ones by public censure and/or expulsion from the data trust, along with a potential claim for damages. Whether any breach was intentional or accidental might also be considered in determining the strength of response.

In the same way that feedback should be obtained from stakeholders in respect of FDT's prospective purpose, so would it be advisable to engage stakeholders in the drawing up of any code or rules. This would likely maximise the chances of broad stakeholder engagement in the project as a whole. For these purposes, stakeholders would include representatives from both data providers and data users.

Recommendation: FDT should begin work on the development of rules that set out how FDT will function and that will govern its basic operations. The rules will bind all of FDT's participants (and, if FDT has a separate legal personality, FDT itself) and can be used to underpin certain overarching values or principles, such as FDT's independence and compliance with the competition law rules. A competition law protocol should be drawn up in due course (either as a stand-alone document or as part of an overarching governance document) and, if there is a desire for discussions to take place between market participants/competitors before the protocol is in place, we recommend putting a preliminary protocol in place to ensure that these initial discussions are compliant. The consequences of any breach of the rules (whether intentional or accidental) should also be considered. Stakeholders and prospective stakeholders should be consulted as part of the process of drawing up the rules.

6. Independence

We touched on the importance of independence in the context of a data trust's legal form. It is doubly important in the context of governance. Independence means different things to different people, however. In our view, "independence" in this context, is a question of balance – rather than being wholly excluded from a data trust's direction or decision-making, no one set or class of stakeholders should be able to dominate, dictate or disrupt a data trust's direction or decision-making.

Recommendation: in developing the governance framework and writing the rules and (if appropriate) articles of association for FDT and the contractual framework under which data will be provided and used, it should be borne in mind that, preferably**,** no one set or class of stakeholders should be able to dominate, dictate or disrupt a data trust's direction or decision-making.

7. Governance Framework

We set out below a possible governance structure which will inevitably need to be considered alongside FDT's proposed purpose. Whether FDT has its own legal personality or not, perhaps the key aim of the governance structure is to find a balance between the differing interests of stakeholders and to find this balance in such a way as will facilitate trust and encourage engagement amongst stakeholders and potential stakeholders.

In the course of writing this report, we have looked in varying degrees at the various models adopted by each of the Data Sharing Coalition, iShare, the Amsterdam Data Exchange, the HAT Community Foundation, the European Grid Initiative and Open Banking. These models show that there are a number of different approaches that can be adopted to governance frameworks, but the basic issue is very simple: a need to find a balance between stakeholder representation and operational efficacy. In its simplest form, this points towards a two tier structure:

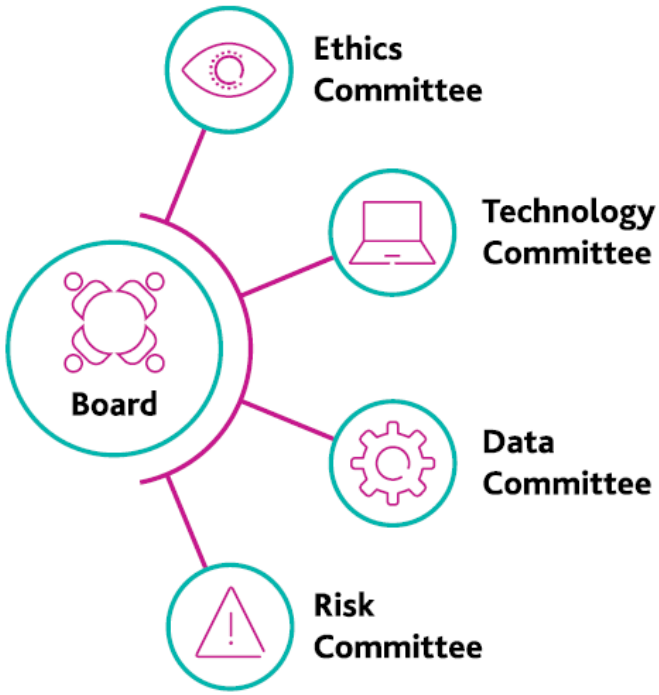
- stakeholder membership; often broad in nature; and
- a smaller decision-making body.

In corporate terms, this is the balance between the shareholders and the board.

This smaller decision-making body (a board of directors or representative) would be responsible for overall governance. It could be led by an independent chair with executive and non-executive directors, including civic leadership. It would be responsible for all statutory matters, strategic direction, managing conflicts of interest, hiring executives and, potentially, approving financials. It could be supported by the following advisory sub-committees:

- Risk: responsible for risk management oversight including security and data risks;

- Ethics: responsible for oversight of ethical risks;
- Data: responsible for data management oversight; and
- Technology: responsible for deployment and use of technology within the DFT infrastructure.



The constitution of the Board and each of its committees will need to be considered. All committees are capable of including independent external representation. Civic leaders could be appointed to represent any relevant purposes.

There is an obvious interplay between the data and technology committees, in that data quality and formats must permit interoperability.

If FDT has its own legal personality, it should also consider the following possible committees:

- an audit committee (responsible, among other things, for monitoring the integrity of a company's financial statements and reviewing that company's internal financial controls and risk management systems);
- a remuneration committee (to determine a company's remuneration policy for the company as a whole and including the setting of remuneration for the chair, executive directors and senior management); and
- a nomination committee (responsible primarily for board appointments and succession planning).

The above structure is both robust and practical. It is of critical importance, however, that the governance structure is acceptable to FDT's stakeholders – in particular,

data providers and data users – and this structure should, therefore, be road-tested with potential stakeholders. One counterpoint to this is that the governance structure should not be so complex that the data trust is unable to make timely operational decisions. While representation and balance will be important for the gaining of stakeholder trust, so will the efficiency of a data trust's decision-making.

To this end, the governance structure should reflect not only the nature but also the maturity of FDT and it is perfectly feasible to commence operations with a small number of stakeholders, each of whom would have rights of veto over certain decisions such as the amendment of FDT's purpose or the principal rules established at FDT's outset.

A board that engenders confidence among stakeholders will be an asset to a data trust. It may, therefore, be worth considering some form of representation for data users within the governance structure. There will be certain concerns – such as the quality of data and metadata – that will be common to all users.

The ethics committee could be independently chaired and include independent ethics experts to help engender confidence within the stakeholder community as a whole.

To the extent FDT's stakeholder base differs from its shareholders or members, its annual general meeting may be of limited value or interest to stakeholders. Given this – and the need to encourage stakeholder engagement – some form of annual stakeholder meeting could also be considered.

A governance structure based on the proposals above appears sensible, in that it seeks to take into account stakeholder views and concerns, while not being overly complex. As stated above, however, stakeholder buy-in will be critical and should be sought at the design stage.

In addition, if FDT has its own legal personality, it could consider applying a corporate governance regime such as the Wates Corporate Governance Principles for Large Private Companies (the Wates Principles). The Wates Principles recognise the diverse range of private companies within the UK and are designed to encourage the board of a company to apply each principle by considering them individually, having regard to that company's specific circumstances.

Recommendations:

1. It is of critical importance that the governance structure is acceptable to FDT's stakeholders – in particular, data providers and data users – and this structure should, therefore, be road-tested with potential stakeholders.

2. The governance structure should not be so complex that the data trust is unable to make timely operational decisions. While representation and

balance will be important for the gaining of stakeholder trust, so will the efficiency of a data trust's decision-making.

3. A board that engenders confidence among all stakeholders will be an asset to a data trust. It may, therefore, be worth considering some form of representation for data users within the governance structure. Some form of annual stakeholder meeting could also be considered.

4. If FDT has its own legal personality, it should consider adopting a corporate governance regime such as the Wates Corporate Governance Principles for Large Private Companies.

8. Contractual Framework for Data Provision And Use

Complementing the overarching rules established for the operation of FDT (see Rules and governance considerations) will be contracts between FDT (if it has legal personality) and its stakeholders and specifically with data providers and data users. If FDT has no legal personality, all such contracts will need to be among FDT's stakeholders. Clearly, these contracts will need to be consistent with the rules established for the operation of FDT and may incorporate those rules specifically by reference.

It is possible to regulate data provision and data use arrangements through: (i) in the case of an incorporated data trust, bilateral contracts between the data trust and each data provider and data user; (ii) bilateral data sharing contracts between each data provider and each data user who wishes to access the relevant data; (iii) a multi-party code or contract to which all data providers and users accede[2]. If FDT is not incorporated as a separate entity, then option (i) is not valid. To adopt option (ii) would be to devolve responsibility to individual data providers and data users who would most likely then contract on the basis of the data provider's standard data sharing agreement as would happen currently in the absence of FDT.

Accordingly, if FDT is not incorporated then option (iii) - the multi-party contractual code – may be the preferred approach. Hallmarks of such an arrangement include that: (i) most prospective data provision and data use arrangements are readily identifiable and can be addressed within the multi-party arrangement; (ii) data users and data providers are willing or compelled by regulation to accede to the multi-party arrangement; and (iii) a governance model has been developed to administer the multi-party code or contract and to manage proposed modifications to it.

In pursuance of FDT's purpose and the objectives outlined in section 2, it is likely that flexible data-sharing and data use arrangements will be important to cover a

[2] An example of such an arrangement being the Smart Energy Code, which defines the rights and obligations of those involved in the UK's smart metering infrastructure including in respect of use of data.

range of scenarios. Accordingly, if a multi-party code or contract is the model for FDT to adopt for the purposes of regulating data provision and use, then it will need to have sufficient flexibility to accommodate those different data sharing scenarios.

It is likely that prospective stakeholders may come in many shapes and sizes, potentially encompassing research institutions, large and smaller corporate entities, and governmental and inter-governmental organisations.

We recommend that FDT develops a range of data provision and data use terms that will be set out in the multi-party contract among the data providers and data users. It appears likely that a number of different contractual models will need to be developed to address different scenarios. There will be no "one size fits all" form of data provision agreement or data use agreement.

The data provision and data use terms that are developed will address different scenarios in an appropriate manner. By way of example, the data access terms may range from simple subscription terms that enable an individual researcher to access a discrete data-set at no cost for the purposes of his or her research activities to a more sophisticated form of agreement under which FDT may provide data services, including analytics, on a commercial basis to a customer.

Writing appropriate terms to govern the provision and use of data (and by "use" we mean both allowing direct access to data to a user but also the provision of services by FDT using data held by it[3]) is not a task to be completed by FDT in isolation. It is critical that FDT consults extensively with stakeholders and, specifically, with the prospective data user and data provider communities.

Only by addressing the needs of these stakeholders will FDT be able to create contractual frameworks that facilitate trust and incentivise both data providers and data users to engage with FDT and support its activities. Accordingly, we recommend establishing a working group drawn from FDT's stakeholders, including a range of representatives from different prospective data providers and data users, to consider the key issues to be addressed in the contractual frameworks that will govern engagement with those data providers and data users.

This work shall include considering the impact on such contractual frameworks of:

- the nature of FDT as data steward and a provider of data services;
- the nature of the data that FDT will hold;
- the nature and identity of the different categories of data providers;
- the nature and identity of the different categories of data users;

[3] For example, see the approach taken by eDRIS (part of the NHS) to make available NHS health data as a service.

- risk allocation and liability flows among FDT, the data providers and the data users; and
- the financial and funding model for FDT

We have included more detailed analysis and some conclusions on each of these areas in Annex 2.

Having given consideration to the various elements identified in this section 8 and in Annex 2, FDT will be in a position to develop the terms on which data providers and data users provide, access and use data. As noted above, if FDT is not a separate legal entity, this would be codified into a multi-party contract, which will be based also on the rules described in section 5 (Purpose and Rules). Among other things, we would expect the terms under which data is provided and used to cover data quality and format. In the case of data provision terms, the data provider would be expected to warrant that the data has been lawfully contributed (including in relation to intellectual property rights) and may be used for the ongoing purposes of FDT and its data users. The terms would also need to set out clearly each party's role in the context of data protection (e.g. whether a party is a data controller or processor for the purposes of GDPR) for contributed data and any other personal data shared. They would also need to set out clearly any restrictions on use for anti-competitive purposes, specifying that any collaboration between users outside and beyond the legitimate purpose of the FDT would be at the users' own risk. We would also expect these agreements to cover issues that may arise in relation to confidentiality and intellectual property rights under the FDT, including in relation to inputs (i.e. data provided) and outputs (i.e. through use of data).

The data provision and data use terms will be dictated by FDT's stated purpose and the requirements of the prospective participants in FDT, whether data steward, data provider or data user.

If the data in question is of low sensitivity, easily accessible, not subject to regulatory, commercial or other constraints and both data providers and data users are supportive of open access on a no or low cost basis, then it may be that simple contractual terms might be adopted for that data, enabling ease of access to data on a decentralised basis through the acceptance, electronically, of specified data end user terms. This access model may use a simple and relatively permissive licence approach to documenting data access, for example the two forms of data licence published by The Linux Foundation were suggested in a previous pilot project in which we were involved.[4]

If, on the other hand, the contrary is true and sensitivity is high and regulatory, commercial or other constraints are significant, then it is likely that more bespoke and complex contractual terms will be required that addresses identified risks and

[4] The Linux Foundation, '[Community Data Licence Agreement]'.

issues and that is more restrictive in nature. This contractual model may sit within a more centralised data trust construct that adopts a rigorous approach to on-boarding the prospective data user.

Based on our understanding of the FDT project, it appears that a balance will need to be struck to construct a legal framework for data provision and access that addresses provider concerns sufficiently without creating a degree of complexity that may deter potential participants, whether prospective providers or users.

Non-exhaustive examples of key issues that may be addressed in data provision and access framework contracts include:

- Criteria for becoming a data user or provider including any technical requirements and the on-boarding process
- Process for forming the contract and incorporation of FDT rules (if applicable)
- Scope of permitted data use
- Specific restrictions on data use purposes
- Financial terms (if any)
- Grant of licence
- Sub-licensing of data use
- Confidentiality
- Freedom of information (if applicable)
- Personal data protection particulars (including, if applicable, transparency, purpose limitation, security, data breach reporting obligations, international transfers, onward transfers, use of processors and processor obligations, data subjects rights, data retention and schedule of particulars
- Data security (if applicable)
- Technical standards and requirements
- Characteristics, standards and quality of data
- Derived data – control and use
- Attribution to data provider
- Rights in respect of derived data
- Governance and dispute resolution (including linkage, if appropriate, with FDT governance model)
- Warranties and liability (including protection for FDT)
- Process for changing the data provision and access terms
- Duration, termination and return of data (if applicable)
- Audit rights
- Governing law

As noted above, it will be important to engage with all stakeholders in developing the contractual framework under which data will be provided and made available for use to ensure the forms of agreement reflect the needs of prospective data providers and data users and do not act as a barrier to engagement with such stakeholders.

Given that one of the criteria that will determine how much a stakeholder is willing to trust FDT is the trustworthiness of both FDT and its other stakeholders, this will need to be built into the criteria for potential stakeholders to become data users and/or data providers, and also into the obligations to which they are required to sign up to as stakeholders. Other factors that will give rise to trust in this context, are transparency of decision-making, consistency of application of FDT's rules and a willingness on the part of FDT to enforce its rules and contractual rights, if necessary. As mentioned in paragraph 3 (contractual and financial risk) of Risk Management (above), if FDT has no separate legal personality, the enforcement of those rules and rights will fall to the stakeholders rather than to FDT.

An exemplar schematic of how the contractual framework might look is set out in Annex 3.

If FDT is incorporated then we would expect that there would be no need to have a multi-party code or contract governing data provision and use. Rather those matters would be addressed in bilateral contracts between FDT and each data user and data provider. However, the same considerations and issues described in this section 8 would apply and be taken into account when developing the data provision and data use templates.

Recommendations:

1. If FDT is not incorporated then a multi-party code or contract among all data providers and users would be developed include a range of data provision and use terms that are flexible and address a number of different scenarios under which data will be provided, held and used, as well as the nature and sensitivity of the data in question. If FDT is incorporated, then, instead, we envisage that FDT shall enter into bilateral contracts with individual data providers and data users that are consistent with and may incorporate the rules described above.

2. We recommend that FDT consult with stakeholders, including representatives of the prospective data user and data provider communities, on the form of the data provision and data use agreements and on the key issues that will need to be addressed from the perspective of those stakeholders.

3. In order to establish appropriate terms and conditions to govern the provision and use of data, a working group should be set up to manage consultation with stakeholders and to consider the issues identified in Annex 2 including the potential consequences for the terms and conditions under which data is provided and used of:

    - the nature of FDT as data steward and a provider of data services;

- the nature of the data that FDT will hold;
- the nature and identity of the different categories of data providers;
- the nature and identity of the different categories of data users;
- risk allocation and liability flows among FDT, the data providers and data users; and
- the financial and funding model for FDT.

9. Termination and Winding Up

Alongside FDT's legal and governance structure, we think it useful to consider the position upon a hypothetical winding up of FDT. Above, we discussed the fact that a sense of trustworthiness is essential to enable any data trust to operate. In order to be considered trustworthy, FDT will, inevitably, need to have considered what will happen when it ceases to operate – whether this occurs voluntarily or involuntarily.

The rights of a data provider to withdraw its data from FDT will need to be balanced against the rights of a data user, which may be in the process of using that data for the purposes of an ongoing project. With this in mind, we suggest that a distinction be made between:

- projects that have been completed;
- projects that are in progress; and
- future projects.

Relevant terms should be included in the data provision and data use agreements.

Similarly, FDT's rules, together with the terms of the data provision and data use agreements, should make clear what happens to the data upon a solvent or insolvent winding up of FDT.

A data provider will wish to prevent any involuntary transfer of or granting of access to, its data to third parties, while data users will have a legitimate interest in being able to continue to access data with a view to completing their ongoing projects. There is no silver bullet for insolvency but sound planning can, however, mitigate its worst effects and provide some reassurance to FDT's stakeholders in respect of the meeting of their respective expectations.

Also, as mentioned above, whether the data trust has a distinct legal personality or not, consideration will need to be given to the withdrawal (whether voluntary or forced) of stakeholders from the data trust.

While we do not go into detail on this here, we will, of course, be happy to discuss this further.

Recommendation: FDT should consider now how to mitigate the effects on its stakeholders of a winding up of FDT. In particular, FDT's rules, together with the terms of the data provision and data use agreements, should make clear what happens to the data upon a solvent or insolvent winding up of FDT. This should include addressing, and making provision for, arrangements to ensure, to the extent necessary, the on-going curation of data beyond the winding up of FDT. The FDT's rules will also need to address what happens upon the withdrawal (whether voluntary or forced) of a stakeholder from the data trust.

10. Conclusions and Next Steps

Clearly, some of the recommendations made and issues raised in this report will require further thought and discussion to determine the best approach to take.

It is recommended that clear works-streams and associated deliverables be identified, agreed and documented to take forward each of the recommendations. In some areas this will require allocation of responsibility to existing members of the project team and engagement with stakeholders including the prospective data user and data provider communities. Ultimately, the approach taken to legal and governance issues should be driven by clearly identified business and operational need and should be underpinned by a robust and sustainable financial model. It may be further work will be needed to engage with FDT's prospective stakeholders and to develop the financial and funding model, including certainty that initial funding will be available, before progressing some of the recommendations contained in this report.

Annex 1

Corporate Structure Options

Summary of Key Differences Between Company Types			
	Company limited by shares	Community interest company (CIC)	Company limited by guarantee (CLG)
Separate legal personality	Each of these types of company has a separate legal personality, distinct from its members or shareholders. Each is therefore able to own assets, enter contracts, employ employees and be sued in its own name.		
Ownership	Owned by shareholders.	A CIC may take the form of a company limited by shares or by guarantee and its ownership will therefore depend on its structure.	Owned by members (otherwise known as guarantors).
Financial contribution from shareholders or members	A shareholder has to pay for shares up-front.	This will depend on whether the CIC is a company limited by shares or a CLG.	A member does not have to make any financial contribution to the company unless and until the company becomes insolvent.
Right to profits	A share gives a shareholder the right to share in the profits of the company by way of receiving dividend payments.	This will depend on whether the CIC is a company limited by shares or a CLG.	The members of a CLG are not entitled to dividends, but see the position on distributions below.

Summary of Key Differences Between Company Types			
	Company limited by shares	Community interest company (CIC)	Company limited by guarantee (CLG)
Ability to pay dividends	Can pay dividends to shareholders (subject to certain formalities) up to limit of its distributable reserves. Generally (but not always), the amounts shareholders receive will depend on the ownership percentage represented by their shareholdings.	Can pay dividends (subject to certain formalities) up to: • limit of its distributable reserves to any shareholder(s) or member(s) who are also asset locked; and • 35 per cent. of its distributable reserves to other shareholders or members.	Cannot pay dividends but can distribute surplus profits to members unless restricted from doing so under its articles of association. Any distributions will be divided equally between members. The articles of most CLGs prohibit the making of distributions.
Liability of shareholders or members	A shareholder enjoys limited liability. If the business becomes insolvent, the shareholder is only required to pay for any unpaid sums on its shares. The company itself is liable for all debts beyond this sum.	See company limited by shares or company limited by guarantee (as appropriate).	A member guarantees a fixed sum of money to the company. This is the extent of a member's personal liability to the business and it must be paid if the company becomes insolvent.

Annex 2

Contractual Framework – Factors and Considerations

The nature of FDT as the data steward and provider of data services

If the FDT is to be established as a company, the identity of its initial member or members will need to be determined. If the FDT is established as a wholly-owned subsidiary company of a public body for the purposes of freedom of information legislation[5], applicable freedom of information laws may require FDT to provide data or information it 'holds' either pro-actively or on request to a person, irrespective of whether that person is a participant in the data trust (for example a signed up data user). If data or other 'held' information (which could cover the agreements between the parties, the minutes of any of the committees (e.g. ethics considerations, licensing agreements – any information held in recorded format) is disclosed under such laws, the data trust will not have any control over its subsequent use. While there are some exceptions to the disclosure of data under transparency regimes, data providers will be aware of this additional method of disclosure and we expect that it will need to be addressed in some manner within the contractual frameworks under which data is provided and used.

Of course, this issue should not be overplayed as – for example – the University itself is well-used to holding significant volumes of sensitive research and other data. The University manages that data effectively within the context of such freedom of information legislation and relies on relevant exemptions within that legislation to ensure that data is not disclosed inappropriately.

The nature of the data to be held by FDT

In developing the contractual frameworks that will govern the provision and use of data, it is important to understand the nature of the data that will be held by FDT. In particular, it will be important to understand whether or not, by its very nature, or due to external factors, such as the contractual terms under which it has been provided or through the operation of law, that data is subject to restrictions on access and/or use that will need to be reflected in the governance and contractual framework within which FDT is to operate.

For example, there exists a likelihood that certain datasets provided to FDT will contain personal data either as part of the dataset, or linked with meta-data that will have privacy law implications, particularly for data protection law compliance under the GDPR and Data Protection Act 2018. This may raise potential issues around processing purposes which are different to the original collection purpose, processing by different categories of users and possible cross-border transfers of the data. Individual privacy assessments will need to be carried out for different

[5] Freedom of Information Act 2000

scenarios and appropriate data protection provisions written and included in both the data provision and data use template agreements.

For data that is personal data, there are a number of aspects of data protection legislation which FDT will need to ensure are met in order for the data to be made available to, and used by, data users. Of particular importance for the data user is the legal basis for processing and the principle of 'purpose limitation'. In most cases it would appear that the data user will be 'further processing' the data (i.e. using it for a purpose different to that which it was originally collected). Under the GDPR, this means that various conditions must be met for this use to be lawful depending on the data source, categories of data, and most importantly the compatibility of the proposed use with the original use. There may be mitigating steps (such as pseudonymisation) to ensure fair and lawful use of the data. One of the lawful bases will need to be identified for the data use. These are factors which will have to be assessed by FDT before giving access to a data user and determining the terms under which such access shall be given.

The nature of the data may also mean its use is controlled by other applicable laws including the law of confidence. Where competitively useful information is provided to FDT, the Competition Act 1998 may require access to data to be subject to certain limitations or confidentiality requirements.

There may be sector-specific industry codes or regulatory requirements that are relevant to the data provided to FDT.

Data may be protected by intellectual property rights, most obviously copyright or database rights, which may prevent the use of data without the permission of the owner of those rights. Any authority given to a prospective data user by FDT to use any such data must be consistent with those rights and with the terms of any corresponding licence granted to FDT by the creator or provider of that data. For example, even if data is made available under a relatively permissive open data licensing regime, such as a Creative Commons licence[6], the licence terms may require, at least, that the data provider be attributed in any subsequent re-use of the data. In particular, any licence to, and granted by FDT should ensure that the definition of data is adequate to cover the data being provided and its use. There may also be provisions as to which party will own any intellectual property rights created during the course of the data use.

Even in the absence of legal or contractual restrictions on the use to which data may be put or made available for use, data will need to be strictly controlled by FDT if it is possible that it may be used by "bad actors" for illegal or unethical purposes, such as for the purposes of financial fraud. This is partly a question of good governance, but, FDT may also consider it good practice to vet potential data users, through an

[6] Creative Commons

appropriate registration process, and to ensure that contractual terms under which data is made available explicitly prohibit the use of the data for these unintended purposes. We note that FDT has already given significant thought to the development of a data provider and data user on-boarding process and we suggest that completion of terms and conditions governing data provision and use with data providers and data users be built into that on-boarding process.

On a case by case basis, FDT will wish to consider whether it is necessary or appropriate for contractual and technical restrictions to be applied to the access and use of different data-sets held by FDT. As part of that consideration, FDT will need to reflect on whether or not its purpose can be fulfilled if those restrictions are applied. In assessing this, FDT will want to consider the effect that any restrictions (or indeed a lack of restrictions) may have on prospective participants and their willingness to participate in the activities of FDT.[7] In this respect, a balance needs to be achieved between, on the one hand, meeting the purpose of FDT and ensuring anticipated societal and other benefits can be achieved and, on the other hand, ensuring that the contractual and technical framework under which access is granted adequately protects the interests of the participants (including data providers and data users) and enshrines the ethical and compliant use of data as a core principle.

In practice, achieving this balance may be difficult. Some of the benefits to be realised from using data may not be known at the time FDT and its purpose are established or at the time data is supplied. Therefore, whilst we must, of course, recognise in the established contractual frameworks the importance of not undermining the concept of trust and credibility that sits at the heart of such arrangements, of which ensuring appropriate and lawful use of data, including personal data, is a key tenet[8], we must also not lose sight of the inherent risk that establishing onerous access and data use requirements may undermine the ability of FDT to fulfil its purpose and deliver the benefits anticipated on its establishment.

This need for FDT's data governance and contractual frameworks to be flexible was noted in the joint report by the British Academy and Royal Society 'Data management and use: Governance in the 21st century', October 2017. That report highlighted the need to anticipate unexpected users and uses and observed that, as new ways to analyse data are developed, unexpected patterns and insights which go beyond the original purpose could arise. In addition, as the volume of data held within FDT expands, the potential for that data to generate unexpected patterns and

---

[7] In the report 'Data Ownership: Rights and Controls: Reaching a Common Understanding' summarising discussion at a British Academy, Royal Society and techUK seminar on 3 October 2018 it was advocated that there be a shift in focus to how data is used rather than how it is owned or controlled noting that "We have tended to focus on controlling the collection of data, but there should be a shift in focus toward the use of data and the impact of that use on individuals."

[8] In the UK, the Data Protection Act 2018 and the General Data Protection Regulation (EU/2016/679).

insights will also grow. This should be borne in mind in developing contractual frameworks that will govern the provision and use of data.

The nature of the data providers

In considering the contractual basis on which data may be made available for use, a responsible data steward will also consider the nature and identity of the providers of data.

A data provider may be subject to regulatory codes or guidance which are applicable to the sector in which they operate or the country in which they are based (in addition to laws applicable to data protection, privacy and intellectual property). Certain countries are also beginning to apply data localisation laws. Applicable regulations may dictate that data should not be disclosed publicly or made available for particular purposes without the adoption of appropriate safeguards that, among other things, protect the rights and interests of data subjects. This may have an impact on the data that can be made available and the contractual or other terms under which it is made available.

Some of the prospective data providers and data users may be regulated entities. Any applicable regulation will supplement relevant generally applicable legal obligations to which they are subject, such as GDPR and competition law. As a result of such regulation, these prospective data providers and data users may require the contracts under which they are prepared to provide data to contain terms which address their regulatory concerns. Examples may include provisions governing the security standards that FDT applies to the handling and storage of data, restrictions on the purposes to which data may be put, a right to audit FDT systems that hold their data and a right to have data returned in specified circumstances.

FDT will need to understand the concerns and sensitivities of the data provider community and to create a practical, technical and contractual framework that safeguards their interests and facilitates trust. Specifically, it will need to develop with the data provider community a contractual framework under which data will be provided and used that does not expose the data provider to undue liability or regulatory action and that aligns the data users' scope of use with the requirements of the data provider including mitigating the risk of mis-use of provided data and infringement of third party intellectual property rights.

The nature of the data users

The identity of prospective data users will also impact on the process and terms under which access to data is made available.

In certain areas, it may be that the same dataset may be used for both good and bad purposes by authorised FDT data users. The question arises, what steps can FDT

take to ensure that the contractual terms under which access to data is made available provide for that data to be used in an ethical way and in a manner which is consistent with FDT's purpose and the premise and terms under which the data providers made that data available?

FDT should consider the risk of data being used for unethical or unintended purposes. If a risk exists, it should consider how technically, contractually and as a question of process, it may ensure that data is not accessible to users who may use it in inappropriate ways. This may involve establishing a rigorous registration and on-boarding process, which enables FDT to identify prospective data users and carry out a degree of due diligence over those prospective data users, if appropriate. Access to data may need to be subject to technical restrictions that prevent "bad actors" accessing data. The contractual terms under which data is made available should, of course, set out the scope of use and prohibit the use of data for unlawful purposes or purposes that are not consistent with FDT's own purpose and objectives.

It is clear, given the multi-faceted objectives of FDT, that users may come in "different shapes and sizes". We recommend that FDT develops a suite of template data user and access terms that are appropriate for a range of different data types and a range of different data users and that, if FDT is not a separate corporate entity, will be incorporated into a multi-party contract or code among data users and data providers. If FDT is established as a separate corporate entity, then the relevant data use and access terms will be included in bilateral template contracts between FDT and the relevant data providers and data users. For example, the data use terms that may apply to the use of low-risk data by an academic researcher may be significantly more straightforward than those which govern access granted to commercial organisations to use more sensitive supply chain data. Consideration of the nature of the prospective data users and the most appropriate user terms should take place during the on-boarding process.

Beyond the identity of a data user, the territory in which a data user is based may also have implications for FDT. If a prospective data user is based in a country which is subject to sanctions or export control restrictions, or which has data localisation laws, then, depending on the nature of the data, it may not be appropriate for FDT to allow access to data to a prospective data user in that territory. Restrictions may also apply to getting the data into that jurisdiction and getting it back out, if necessary. There may also be intellectual property rights considerations depending on in which jurisdiction the data is used and in relation to in which jurisdiction any outputs arising out of the use of the data that may give rise to intellectual property rights are created.

Equally, from a data protection perspective, if data held by FDT contains personal data, then restrictions will need to be satisfied if the data user is located outside of the UK/EEA. Depending on where data users are located, FDT will be able to select the one best suited to protect the data it provides, from the range of transfer

mechanisms available. For some transfers, no additional provisions would need to be addressed in the contract framework (i.e. transfer of personal data to a country or international organisation that has an 'adequacy decision' from the European Commission), while for others, additional contractual obligations may have to be imposed on a data user before the data is provided[9].

In addition, competition law considerations may have consequences for FDT and the contractual terms under which access to data is granted. One determining factor for whether a competition law issue does arise will be the identity of the data providers and the data users.

We expect that data users may expect certain contractual and legal safeguards in terms of their use of data accessed from FDT. For example, a user may request:

- FDT to give some form of warranty or contractual comfort that the data accessed and used is at least materially accurate. Given the varied and many sources from which data may be obtained in this instance, that may be problematic for FDT;
- a licence granting the data user the right to use the data accessed from the data trust, and clarity as to the scope of its use rights and any ability to share with others. FDT will need to ensure that the terms are consistent with any licence granted to FDT by the data provider;
- comfort and assurance that, to the extent that the data user is dependent on data-sets for its operations and activities, that it will have continuity of access to those data-sets and that the circumstances under which such access can be removed are clearly set out;
- in use-cases involving the use of data for research, an understanding of how control of derived data and its use as between FDT, the data provider and the data user will operate; and
- assurance that personal data accessed has been collected and provided fairly and lawfully (including in relation to third party intellectual property rights) and that the data user is entitled to use it for the stated purposes.

Risk allocation and liability among FDT and its stakeholders

The apportionment of potential liabilities as between the various stakeholders will need to be carefully considered; particularly if personal data is to be included within FDT. By way of example, GDPR provides for joint and several liability in respect of compensation to individuals (data subjects), as well as the possibility of fines or other penalties for infringements from regulators.

There is scope, within the data provision agreements, to require data providers to ensure that any data they provide may be lawfully placed within FDT, and to meet FDT's requirements in respect of transparency and quality of data, etc. Data

[9] Articles 44 to 49 GDPR.

providers could also warrant to FDT that their data does not infringe third party intellectual property rights. That said, as FDT will have a role in deciding who will be able to use the data and for what purpose, and may allow data from more than one data provider to be combined and used by a data user, it is doubtful that FDT will, if it has a separate legal personality, be wholly able to escape responsibility for decision-making, or liability to a regulator or data subjects.

FDT, as a steward of personal data, will have responsibilities under GDPR. If FDT has its own legal personality, these responsibilities will be its responsibilities[10]. If, however, FDT has no legal personality, these responsibilities will fall upon various of the stakeholders. For example, a data subject might make a subject access request to FDT in respect of the personal data it holds, or seek to exercise other rights over that data, such as erasure. FDT will have to process such requests, which might also have an impact on a provider or user of that personal data.

In this case, given FDT may likely apply its profits / any surplus solely for the purpose of advancing the objectives of FDT, it would be useful to agree with stakeholders that absent very particular circumstances such as, for example, fraud, liability will sit, to the extent legally possible, with the stakeholders rather than with FDT itself. This will inevitably be a balancing act, however. On the one hand, FDT will want to be able to assure a data provider that its data will be secure and used appropriately, but on the other, will only be willing to accept limited liability in this respect. To assist prospective data providers, FDT should consider at least accepting obligations to take action against data users and third parties, in case of a security breach or inappropriate use of the data provider's data. Cyber insurance could also be considered.

As stated above, it is important to bear in mind that if FDT has no legal personality, the actions and liabilities that we refer to as being those of FDT will, in fact, be the actions and liabilities of various of the stakeholders.

These considerations will need to be taken into account in both the data use agreements and the data provision agreements. While indemnities from data providers and data users (that is, an obligation on the part of the data providers and data users to pay for any loss or damage that has been or might be incurred by the FDT in certain circumstances, for example in the event of infringement of third party intellectual property rights) will help to improve a FDT's risk profile, FDT will not simply be able to shift all potential liabilities onto a provider or a user. We have recently seen examples of regulators seeking to fine organisations in a data chain for

[10] It is customary for a corporate vehicle to provide an indemnity under its articles of association in favour of its directors for liabilities that may attach to them in the performance of their duties.

their own failings and, as a matter of public policy, it is questionable whether a contractual indemnity will be effective in respect of a regulatory fine.

Risks assumed by the University in connection with the establishment and operation of FDT are dealt with in the **Introduction and Executive Summary** above.

The financial and funding model for FDT

FDT will, of course, need to be "affordable and sustainable"[11]. It requires a funding model that enables it to be established, operate effectively and, ultimately, be wound up in an orderly manner. If financial incentives are important for enabling the participation of data providers then the financial model, including as regards the costs (if any) of accessing data, will need to be structured accordingly.

Consideration will need to be given to the circumstances in which fees will be levied for access to data and data services (and what those fees will be) or whether in certain cases, say for the purposes of academic research, data and data services will be made available on a free of charge basis or as a quid pro quo between participants who may be both providers and users of data. It is possible that a financial model is adopted under which certain organisations, say, academic research institutions do not pay a fee, whilst other users, say, commercial organisations do. The terms under which access to data is made available will need to reflect the financial subscription model adopted.

The question of how fees will be levied for access to data and the provision of data services is a matter intrinsically linked to the wider question of how FDT in general will be funded. This includes how the technical solution for data sharing to be used by FDT will be financed. One matter cannot be considered without the other. If the establishment of FDT and its on-going operation is funded by a third party, say pursuant to a grant, then the terms under which such funding is provided will need to be reflected, as appropriate, in the terms and conditions under which access to data is made available.

We understand that most of the data held by FDT will originate from third party data providers, rather than from FDT itself. We must bear in mind that the participation of data providers may be conditional upon them receiving some form of financial return or benefit tied to use of their data by data users. In such a scenario the terms of data access will need to take account of any financial incentives offered to data providers. Conversely, any financial subscription model for access to data cannot act as a barrier to user participation; otherwise the purpose and objectives of FDT will be frustrated.

[11] Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 46-48

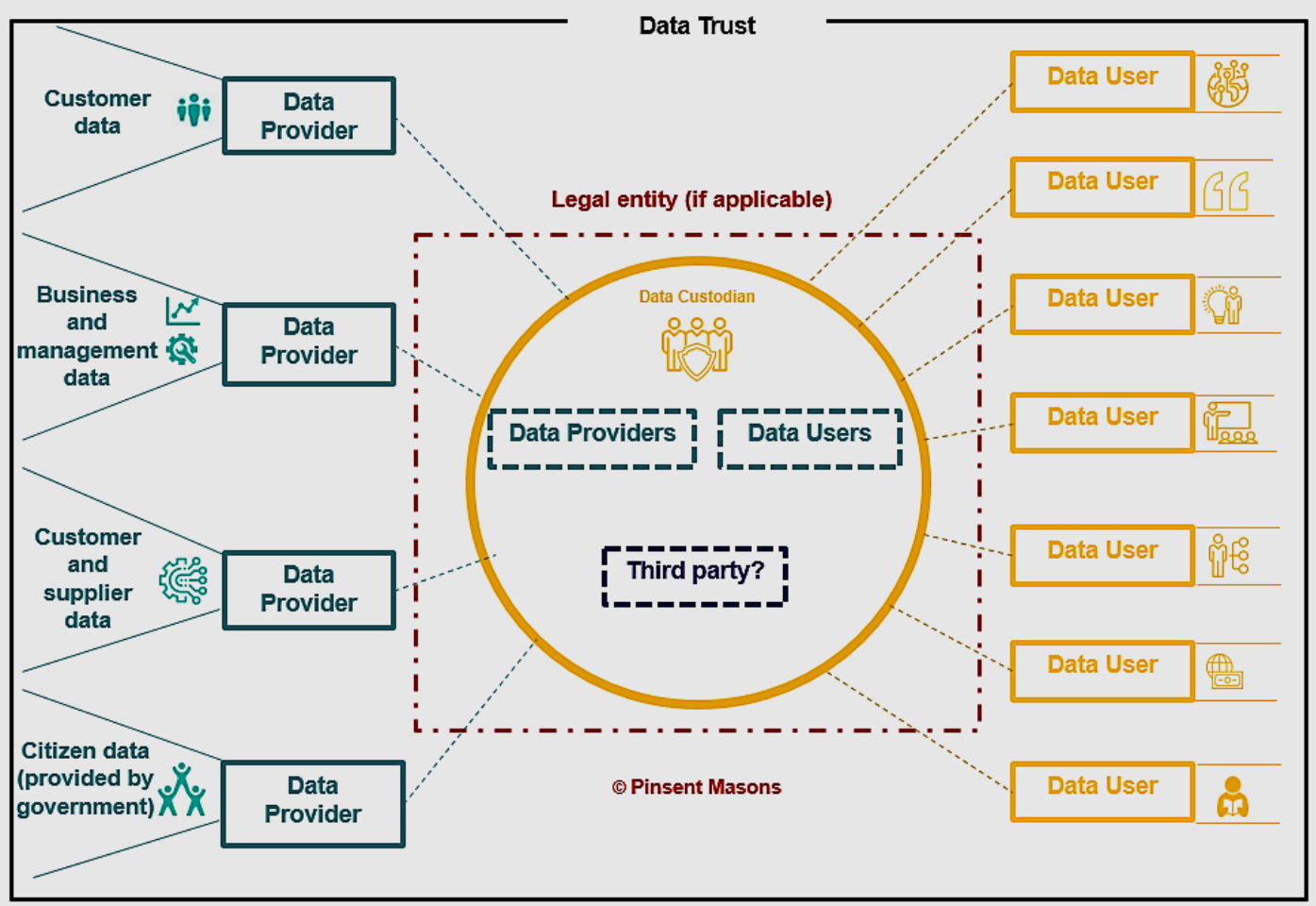
In determining how fees will be charged by FDT, a number of other matters need to be considered, over and above consistency with any agreed financial model. These include:

- will fees be fixed or will fees vary depending upon the type of data, the type of data use (such as a different fee depending upon whether the use is for research or commercial purposes), type of data user (such as student, SME, large corporate), or type of access (such as whether access is granted perpetually or for a limited period of time only);
- will certain fees be one off fees or recurring fees;
- how will the revenues generated be used and will data providers receive any financial return? There may be tax implications that will need to be considered depending on the model adopted;
- how will fees be paid operationally and will FDT have operational processes in place to support this or will it rely on the University of Lincoln systems and processes initially?; and
- will payment be required as a prerequisite to access data? If so, how will this be addressed in the end to end operational process for making data available to data users?

Ultimately, where fees are payable for access to data or the provision of data services, then this will need to be addressed in the contractual documentation that is put in place to govern access to that data or those data services.

Annex 3

Contractual Framework Exemplar Schematic



Annex 4

Competition Law

1. Competition law considerations

Competition law in the UK is principally concerned with two main prohibitions:12

- Chapter I of the Competition Act 1998 (and Article 101 of the Treaty on the Functioning of the European Union) prohibit agreements between undertakings and concerted practices, which have as their object or effect the prevention, restriction or distortion of competition (the "Chapter I Prohibition"); and
- Chapter 2 of the Competition Act 1998 (and Article 102 of the Treaty on the Functioning of the European Union) prohibit an abuse of a dominant position (the "Chapter 2 Prohibition").

The Chapter I Prohibition

Inherent to the Chapter I Prohibition is the principle that a company must independently decide its own commercial strategy. Primarily, this means that there must be no coordination between competitors. Such 'coordination' is not limited to direct agreements between competitors (for example price-fixing or agreements to exclude competitors from a market[13]), but can also include exchanges of commercially sensitive information, either directly or through a third party used as a hub to exchange the information (which foreseeably will be the main competition law concern with a data trust).

Competition law does not prohibit the exchange of 'any and all' information between competitors. There are lots of types of information which can be openly shared; competition law is concerned about 'commercially sensitive' information which is

---

[12] In the UK there is also a 'market investigation' regime. A market investigation is not an investigation into a breach of competition law; rather it is an investigation into the competitive economics of a market to ensure that competition is working in an effective manner. If it is concluded that competition is not working effectively, the UK competition authority (the 'CMA') can require companies to accept certain 'remedies' to improve competition. In previous market investigations these remedies have included opening access to data such as the introduction of Open Banking to the retail banking industry. They have also conversely included reducing access to data where transparency between competitors was already too significant (for example in relation to the UK cement sector).

[13] In October 2017, the European Commission carried out dawn raids as part of an investigation into alleged agreements by Polish banks not to provide data to Fintech rivals (who had the users' consent to access that data).

used to set competitive strategy (for example pricing, volumes, costs, bidding intentions, trade secrets, future market strategy information etc.). However, competition authorities recognise that in certain circumstances information sharing can bring about significant benefits to competition and to customers, in particular where the results are made publicly available (for example through benchmarking to increase standards, or shared research and development to create new products or services which would otherwise not exist).

The sharing of certain particularly sensitive information types, such as future pricing and volume information, is almost always prohibited. Beyond this, it will be important to minimise the exchange of commercially sensitive information so that it goes no further than necessary to achieve the legitimate purpose of the FDT. The type and scope of the information being shared (for example age, content and frequency) will need to be carefully considered and it may be necessary to aggregate and/or anonymise the data before it is shared. It may be the case that certain data can be viewed only by the FDT corporate entity/managers and suitable ring-fencing arrangements will need to be put in place.

Another potential concern would be the purpose of the FDT and how the data is used. If the (unintended) effect of the FDT is, for example, that certain suppliers end up being "blacklisted", they may claim that the FDT is operating as an anti-competitive agreement (a type of "collective boycott") contrary to the Chapter I Prohibition. Similarly, if the FDT is used as a collective purchasing arrangement, these can in certain circumstances also amount to an anti-competitive agreement under the Chapter I Prohibition.

In summary, to manage the Chapter 1 competition law risks, the FDT will therefore need to ensure that the legitimate purpose and use of the data is clearly defined and must have sufficient governance in place to ensure that any exchange of 'commercially sensitive' information between competitors is properly controlled and that all participants understand the limits of what should be shared

The Chapter 2 Prohibition

The Chapter 2 Prohibition prohibits abuses of a dominant position. Accumulation of data is not, by itself, problematic from a competition law perspective. For the FDT to breach this prohibition the FDT would firstly need to be in a dominant position (for example if the FDT becomes dominant in the provision of certain data or access to the FDT has become essential for competitors in order to compete effectively); and secondly the FDT would need to be in some way abusing this position. Abuses could be, for example, charging excessive access fees, imposing unnecessary terms and

conditions[14], discriminatory access or refusing access to certain companies (for example through the use of exclusive licences).

The House of Commons Select Committee[15] has previously expressed concern about a small number of large technology companies having already created data monopolies. An overriding principle of a data trust is to increase access to data. Any restrictions imposed on whom can access data needs to reflect this principle. The Committee advocated "… the need for strong ethical, data protection and competition frameworks in the UK, and for continued vigilance from the regulators". They called for the UK government and the Competition and Markets Authority to review the issue of data monopolies in the UK and regulatory frameworks currently in place. This echoes concerns expressed in 2016 by the Organisation for Economic Co-operation and Development (OECD) when it recommended that big data be incorporated into competition law enforcement and give rise to competition law enforcement if anti-competitive conduct regarding access to and use of data are observed. In 2019, the UK Competition and Markets Authority ("CMA") announced a new Digital Markets Strategy which includes a specific Data, Technology and Analytics Unit to consider the implications of "big data" in a digital world, including "substantial network effects, economies of scale and scope, the role of data and the computing power to use it, scope for personalisation, and market concentration". The CMA is particularly concerned about the use of self-learning pricing algorithms, which have access to large quantities of information, could result in (unintended) anti-competitive effects.

Examples of where competition law authorities have forced the sharing of data due to concerns regarding a lack of competition include in 2012, where in order to avoid an abuse of dominance decision, Thomson Reuters offered commitments to the European Commission that they would allow financial institutions (for a monthly fee) to use its data collection software to access real-time data feeds from sources other than Thomson Reuters. In the UK, the market investigation regime (which is different from investigations into a breach of competition law (see Footnote 12)) has otherwise been used to increase access to data as a way of remedying competition concerns. For example, since 2016 the largest energy suppliers must now disclose

[14] For example, on 7 February 2019, the German competition authority prohibited Facebook from combining user data from a different sources without explicit consent. It was insufficient that consumers accepted Facebook's terms and conditions which allowed for this; Facebook was considered dominant in the market for social networking and therefore was applying an exploitative term which consumers had no other option but to accept.

[15] House of Lords Select Committee Report, Artificial Intelligence Committee, 'AI in the UK: ready, willing and able?' Published 16 April 2017 - HL Paper 10.

their customer lists and other customer information to other operators to allow them to target new customers.

2. UK subsidies regime

The provision of subsidies by public authorities to “economic actors” is subject to the subsidy control rules established by the EU-UK Trade and Cooperation Agreement (TCA). This regime requires authorities to ensure that such subsidies are compliant with a set of "Principles" as set out in the TCA, including the requirement that a subsidy achieves a public policy objective and the requirement that any negative effect on trade between the UK and EU be outweighed by the benefits in terms of achieving the policy objective. Although at present there is no independent authority which ensures that the grant of subsidies complies with the Principles, the TCA requires that such an authority be established. The grant of a subsidy in breach of the subsidy control rules can be challenged in the courts by way of judicial review. In addition, the EU can seek to impose "remedial measures" against the UK where the grant of a subsidy causes (or there is a serious risk that it will cause) a significant negative effect on trade or investment between the UK and the EU.

Contact Details

Andrew McMillan
Andrew.McMillan@pinsentmasons.com
Pinsent Masons LLP

DOI: 10.5281/zenodo.4575625