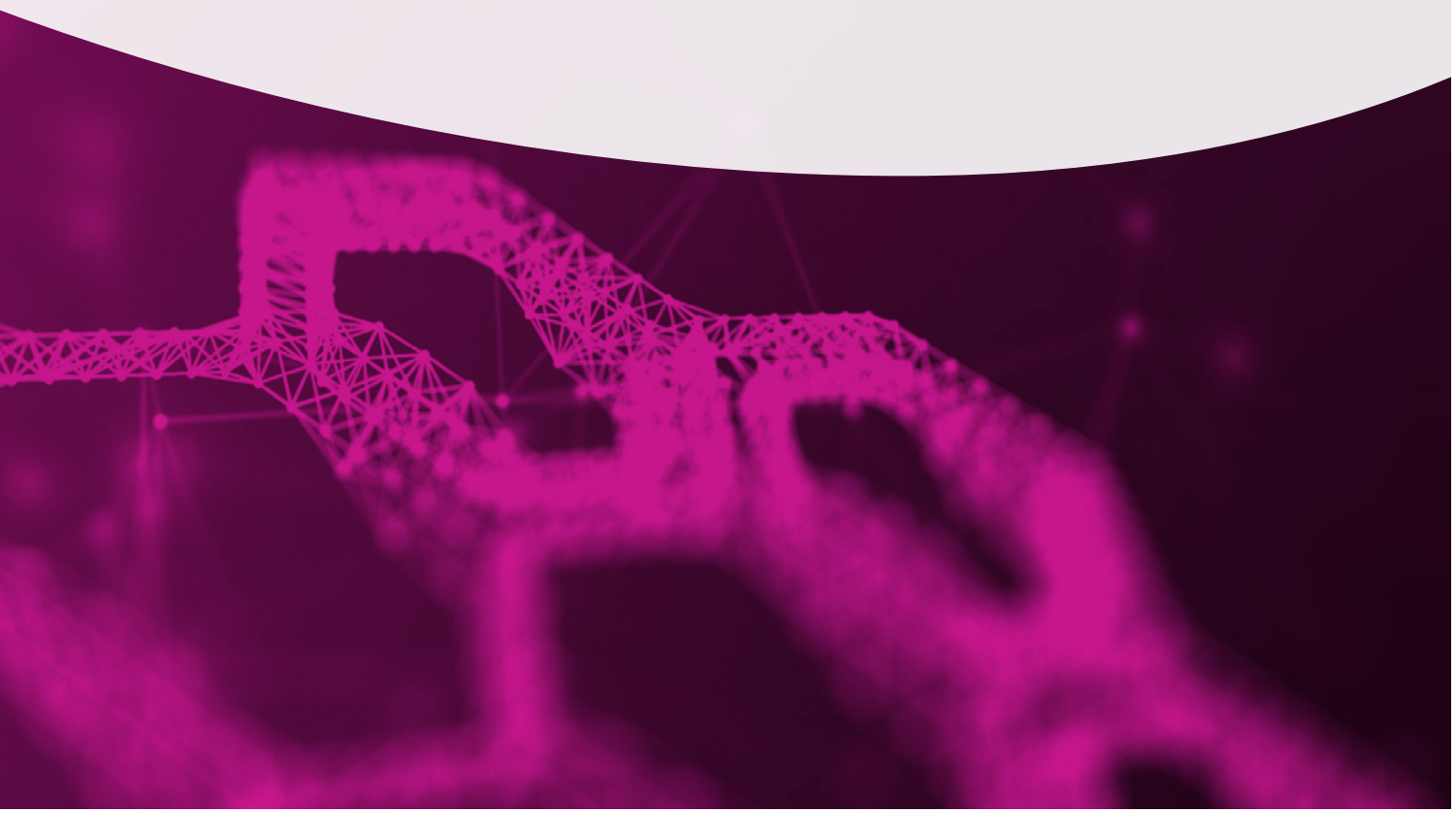
Queen Mary University of London

bpe SOLICITORS

Pinsent Masons

Data trusts: legal and governance considerations

April 2019



Authors

BPE Solicitors — **Sections 2, 3 and 5**

Pinsent Masons — **Sections 4, 6, 7 and Annex A**

Professor Chris Reed,
Queen Mary University of London — **Sections 1, 8 and Annex B**

Acknowledgement

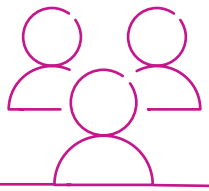
This project was commissioned and run in collaboration with the Open Data Institute as part of a project funded by the UK Government's Office for Artificial Intelligence and Innovate UK. It builds on research from the ODI's Innovation programme funded by Innovate UK.

The views in this report are those of the authors.

Jurisdictional note

This report aims to explain the most important legal issues which a data trust will face no matter which jurisdiction it is established in. We have generally used UK or English law to illustrate our findings, though for data protection laws we have mainly referred to EU legislation. Readers should note that that there are many more legal and regulatory considerations that might be relevant here than has been possible to cover, and that even the important legal issues we discuss might be treated rather differently in other jurisdictions.

This report is a starting point, and far from a definitive statement of the law. While we imagine certain aspects of our analysis will be capable of applying more widely, we are conscious that various legal and cultural differences will, in each case, need to be factored in.



Foreword

In 2018/19, the Open Data Institute collaborated with the Office for AI and Innovate UK on a project to assess whether the use of data trust structures might be effective in widening access to data in a manner which engenders trust. This followed the 2017 Independent review of AI for the UK government[1], which recommended the further exploration of data trusts as a concept.

BPE Solicitors, Pinsent Masons and Professor Chris Reed of Queen Mary University of London are appointed by the Open Data Institute to advise on the legal, contractual and regulatory aspects of data trusts as part of this project.

To date, the use of data trusts has remained theoretical. By applying the concept of a data trust to three real world challenges we have been able to explore that concept in different ways and, where appropriate, propose recommendations that will help others to understand data trusts and their potential applications better.

- The first pilot considered whether new services for citizens could be developed through the use of data in areas like energy consumption, parking spaces and charging bays for electric vehicles. This concept and potential use case for a data trust is further explored in the GLA/Greenwich legal report.[2]
- The second pilot explored reducing illegal wildlife trade by making wildlife data from across the world more accessible so that new services can be built. This concept and potential use case for a data trust is further explored in the Wildlife report.[3]
- The third pilot looked at tackling food waste by using data to track and measure waste in supply chains to support better decision making that helps to reduce waste. This concept and potential use case for a data trust is further explored in the Food waste report.[4]

The Open Data Institute has published a synthesis report which summarises the wider findings and proposes both a lifecycle for data trusts and recommendations for next steps.[5]

A report was also prepared by BPE Solicitors as an extension of one of the pilots considering the wider legal landscape for data trusts.[6]

We are delighted to present our findings, on the legal, contractual and regulatory aspects of data trusts.

> Our vision is to make data work for everyone. Companies and governments need to retain trust in how data is collected, maintained and shared if we are all to realise its full benefits. That's why the Open Data Institute has been researching the different ways these organisations can increase access to data while retaining this trust.
>
> **Open Data Institute**

[1] See Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 45-47, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

[2] The GLA/Greenwich legal report (http://theodi.org/article/gla-data-trusts-legal-report/).

[3] The Wildlife report (http://theodi.org/article/data-trusts-wildlife/)

[4] The Food waste report (http://theodi.org/article/data-trusts-food-waste/)

[5] The Synthesis report (http://theodi.org/article/odi-data-trusts-report/)

[6] Legal landscape review (http://theodi.org/article/data-trusts-legal-landscape-review/).

Pinsent Masons

Data trusts captured the imagination of our lawyers as a way to build trust and realise value in data. To deliver this report we have brought together lawyers from across our firm who all have extensive experience of advising clients on data-driven projects, whether from a structuring or contractual perspective, or in terms of regulatory compliance. We are thrilled to have been given this fantastic opportunity led by the ODI to collaborate with other experts. We believe that together we can make a difference by using our knowledge and expertise as leading technology and data lawyers to provide structures and approaches that: enable change and effective decision-making; promote progress; and help make data work better for everyone.

> Recognising that data, as an asset and enabler for progressive change, and the effective use of that data, is crucial to our clients' futures Pinsent Masons established a Data Trusts Working Group in early 2018. I am delighted to see that the incredible efforts of our lawyers in founding this Working Group are not only benefiting our clients but also helping to unlock the value of data to society as a whole.
>
> Simon Colvin, Partner and Head of TMT, Pinsent Masons

Chris Martin
Partner, TMT
T: +44 131 225 0040
M: +44 7917 598 672
E: chris.martin@pinsentmasons.com

Andrew McMillan
Partner, Corporate
T: +44 20 7490 6504
M: +44 7801 142 357
E: andrew.mcmillan@pinsentmasons.com

Jenny Hotchin
Group Innovation Manager
Previously Associate, TMT
T: +44 20 7490 9285
M: +44 7769 916 777
E: jenny.hotchin@pinsentmasons.com

Joanne McIntosh
Legal Director, TMT
T: +44 131 225 0041
M: +44 7767 383 192
E: joanne.mcIntosh@pinsentmasons.com

Michele Voznick
Legal Director, TMT
Privacy, data protection & information law
T: +44 20 74906332
M: +44 7920414353
E: michele.voznick@pinsentmasons.com

Sarah Cameron
Legal Director, TMT
T: +44 20 7490 6335
M: +44 7920 270 992
E: sarah.cameron@pinsentmasons.com

Lauro Fava
Associate, TMT
Privacy, data protection & information law
T: +44 20 7418 7121
M: +44 7717 208 944
E: lauro.fava@pinsentmasons.com

Mark Marfé
Senior Associate, Intellectual Property
T: +44 20 7490 6320
M: +44 7884 114 974
E: mark.marfe@pinsentmasons.com

Ayla Skene
Consultant, Competition, EU & Trade
T: +44 1 567 8489
M: +44 7770 620 275
E: ayla.skene@pinsentmasons.com

Chris Thomas
Legal Director, Employment & Reward
Commercial trusts & charities specialist
T: +44 121 623 8699
M: +44 7500 121 963
E: chris.thomas@pinsentmasons.com

Richard Snape
Associate, Competition, EU & Trade
T: +44 121 626 5756
M: +447795 497 689
E: richard.snape@pinsentmasons.com

Caryann Cook
Senior Client and Legal Project Manager
T: +44 20 7054 2608
M: +44 7771 943 941
E: caryann.cook@pinsentmasons.com

BPE is an active law firm member of the Foundation for Science and Technology and frequently engages with the Royal Society, the Royal Academy of Engineering and other learned societies in STEM. The firm's Science & Technology team is in a unique position to engage with stakeholders, covering a panoply of "STEM" organisations and this engagement with a wide range of stakeholders enabled us to provide an overview of opinions in the business, government and charity sectors.

The specialist experience and expertise of the Science & Technology team at BPE Solicitors paved the way for us to be one of only two law firms in the country to be awarded the tender to collaborate with the ODI on these innovative data trust pilot projects.

Rob Bryan
Partner and Head of Science & Technology
T: +44 1242 248228
M: +44 (0)7740 619656
E: rob.bryan@bpe.co.uk

Rupert Parker
Trainee
T: +44 1242 248222
E: rupert.parker@bpe.co.uk

As a result of these projects, the concept of data trusts, how they can be used and the benefits of using them have been explored. We firmly believe that data trusts, whilst not without challenges, have a huge role to play in how data could be shared in the future. This has potential to bring huge insights to a range of stakeholders who have the opportunity to benefit in a transformational way.

> BPE are delighted to have been selected to collaborate on these innovative data trust pilots. We have been advising clients in STEM for many years and have been able to apply our experience and knowledge of both technology and third party ownership of data to these data trust pilots demonstrating how data trusts can be used practically and effectively.
>
> Rob Bryan, Partner, BPE Solicitors

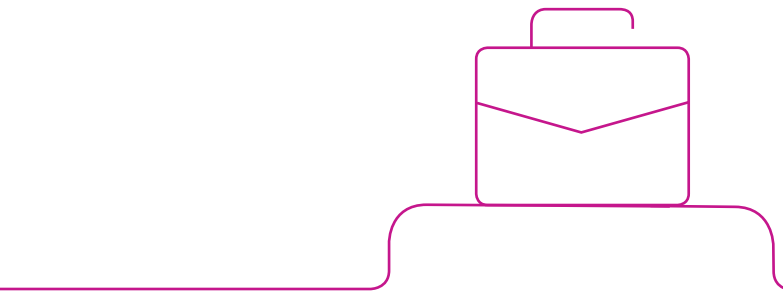
Emily Barwell
Solicitor
T: +44 1242 248487
E: emily.barwell@bpe.co.uk

Chris Reed is Professor of Electronic Commerce Law at the Centre for Commercial Law Studies, Queen Mary University of London. Chris has worked exclusively in the computing and technology law field since 1987, and teaches University of London LLM students from all over the world. He has published widely on many aspects of computer law; his latest books are Rethinking the Jurisprudence of Cyberspace (with Andrew Murray, Edward Elgar 2018) and Making Laws for Cyberspace (OUP 2012), Research with which he was involved led to the EU directives on electronic signatures and on electronic commerce. From 1997 to 2000 Chris was Joint Chairman of the Society for Computers and Law, of which he is an inaugural Honorary Fellow. Chris has acted as Specialist Adviser to the House of Lords Select Committee on Science and Technology, as an Expert for the European Commission, represented the UK Government at the Hague Conference on Private International Law and has been an invited speaker at OECD and G8 international conferences.

Chris Reed
Professor of Electronic Commerce Law
Centre for Commercial Law Studies
Queen Mary University of London
T: +44 207 8828100
E: chris.reed@qmul.ac.uk

Pinsent Masons

Contents



Queen Mary University of London

Executive summary

Legal structures

Trust law is not an appropriate legal structure for data trusts. But the fundamental underlying concept, that those who are stewards of data should be responsible for proper oversight of its sharing and use, is achievable through different legal structures. Both an appropriate corporate structure and a contractual structure can be used to impose the required obligations on data stewards, though the more complex a data trust is (particularly if it will have a changing membership and evolving purpose) the more likely it is to need a corporate structure. These legal structures are more flexible and amenable to future development than the legal trust. In the future there might be a useful role for a public regulator which oversees some aspects of data trusts, but at present there is no regulator which could easily assume that role.

Providing data to the data trust

There are four main problem areas which data providers face, and which need to be accounted for if the data trust is to work:

- Data protection and privacy law. Unless data sharing via a data trust was disclosed as a purpose and consented to when personal data were collected, sharing requires a fresh legal justification. Consent from data subjects would provide such a justification, but is challenging to obtain. Legitimate interest and performance of a public task are alternative justifications which might be available, but the scope of these is uncertain. Anonymisation and pseudonymisation do not necessarily solve this problem. If sharing personal data can be legally justified, the trust will of course need to implement processes to protect privacy and data protection rights, and to comply with data protection laws.
- Commercial confidentiality also needs to be protected by the data trust, because both data providers and third parties who have confidentiality rights in the data might have a claim against the data trust or against data users if confidentiality is breached.
- Intellectual property rights can, to some extent, exist in data, and where they do then the data trust will need to secure appropriate licences from rights owners and to ensure that the terms of those licences are complied with.
- Data providers will also need to ensure that their contractual obligations to third parties do not preclude them from sharing data via the data trust.

Rules for data users

The data trust's rules for data users will need to be legally binding, and must ensure that the rights and interests of the data trust, data providers and data subjects are respected. All this is largely achievable via contract. However, there are particular categories of data which receive extra legal protection; for example, the use of some types of particularly sensitive data may be restricted by, among others, data protection laws and national security laws. Regulated sectors such as healthcare and financial services may have special rules which need to be complied with, and the use of data from, or by, the public sector requires special attention. It is also important that these contractual rules fit the financial model of the data trust and impose appropriate technical obligations on participants in the data trust.

Enforcement of the data trust's rules

Rules are potentially meaningless if there is no way to ensure they are obeyed. Any breach of the rules is likely to be a breach of contract, for which legal sanctions are available through court action. But court action is expensive and likely to be too slow for the needs of a data trust, which include maintaining confidence that its rules provide appropriate protections for all the stakeholders in data. Thus the report suggests that alternative dispute resolution mechanisms need to be incorporated into the data trust's rules and a variety of such mechanisms is available, each with advantages and disadvantages which need to be assessed against the data trust's needs. Some obligations are imposed by law, such as data protection, and these obligations can be enforced by regulators. A useful supplement to enforcement of rules subsequent to a breach is some form of audit, either internal, external or both, to identify breaches or potential breaches and to recommend changes which avoid recurrence.

Governance

A data trust must attempt to balance the wide range of rights and interests across both participants and wider stakeholders, and to generate trust among them about the proper conduct of the activities of the data trust. Achieving all this requires a governance mechanism which focuses on the overriding aims and objectives of the data trust. This needs to provide appropriate representation of stakeholders in selecting the data trust's management; a mechanism for agreeing changes to the purpose and operation of the data trust; and oversight and assurance that the data trust rules and operating methods are complied with and are effective. The overriding aim of the governance structure is to achieve trust.

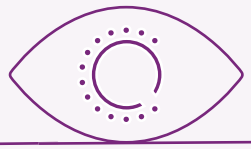
Ending the data trust

A data trust's purposes may have run their course, or data providers and data users may wish to stop using the data trust. In either event, the data trust will need to be brought to an end. This requires prior planning, so that stakeholders understand how this will be achieved before they engage with the data trust, commit data to it, or receive data subject to its rules. From a data sharing perspective, the fundamental question is: what is to happen to data which has been

shared? That question needs to be answered explicitly, along with all the other questions which arise when an organisation is wound up.

Law reform

The report does not specifically recommend law reform to facilitate the use of data trusts, though it does suggest that attempting to reform trust law so that it could appropriately govern data trusts would be a long and difficult project, if it is even achievable. Most of the legal issues which data trusts face can be dealt with adequately through existing legal mechanisms, particularly contracts and corporate law. However, if personal data is involved then the uncertainty about how far, under data protection laws, a non-consent justification might be available to allow data sharing, represents a real obstacle to some data trusts. That uncertainty could be reduced through guidance from data protection regulators about how they interpret these matters in relation to data trusts, which would thus engender confidence that data sharing which followed that guidance would be unlikely to breach data protection laws.



Queen Mary University of London

SECTION 1
What is a data trust in legal terms?

As explained in the 2017 Independent review of AI for the UK government[7], the primary purpose of a data trust is to solve one of the fundamental problems faced when utilising machine learning. Machine learning is based on data-driven research, and the quality and usefulness of its findings is increased if the data sets it uses are comprehensive and rich in detail. However, much potentially useful data is at present held in silos, some by public organisations and some by private entities. Machine learning which uses these datasets, whether individually or as a combined dataset, is likely to generate insights which could not be achieved if each organisation were restricted to using only its own data.

There are other possible benefits from data trusts. Sharing data for research and development could produce real societal and economic benefits when used in domains other than machine learning. Sadly (from a data researcher's perspective), there are many obstacles to data sharing. Some of these obstacles arise because of the legal interests of those persons to whom the data relates, and of the "owners"[8] of data which might otherwise be shared.

1.1 Legal obstacles to data sharing

Datasets which include information about individuals or organisations engage two main legal interests.

- If the dataset contains personal data, i.e. data which relates to an identified or identifiable living human individual, then that individual has fundamental rights which include privacy, non-discrimination and data protection. One important function of a data trust is therefore to ensure that data sharing does not infringe those rights. In most cases, sharing data does not infringe rights if there are appropriate rights protections in place, and these protections are achieved through the rules for data sharing which are established via the data trust's governance mechanisms (see Section 6).

  However, EU data protection laws (see Section 3.1) place substantial constraints on whether data can be shared at all. They provide that data collected for one purpose may not normally be used subsequently for a different purpose without a lawful ground for processing. In some cases this might require the consent of each data subject represented in the dataset unless there is some alternative justification under the law for processing for the new purpose. If the sharing of personal data can be legally justified, the governance system will need to pay special attention to its mechanisms which are designed to respect the rights and interests of data subjects under the law. Identifying how this should be done is particularly problematic where the data was collected for one purpose and it is uncertain whether data subjects would have agreed to provide it for the new purpose.

- The second constraint is applicable to both individuals and organisations, and arises where the data set contains information which is confidential (see Section 3.2). The law protects the confidentiality of information where its disclosure imposes on the recipient a duty to preserve it as confidential. Much personal information is likely by its nature to be subject to obligations of confidence when it is disclosed (for example medical or financial data). Non-public data about corporations, such as sales figures or customer locations, is also highly likely to be confidential. Sharing would disclose that confidential information to other researchers and thus be in breach of the law unless there were consent or some other legal justification for the sharing.

A known technique to reduce the risk of infringing these interests is to anonymise the data. This has two drawbacks, though. First, anonymisation makes it more difficult to link different datasets, and linkage of this kind is important for big data research and development. Second, all anonymisation techniques are vulnerable to de-anonymisation technologies,[9] and some data protection regulators have taken the view that data which can potentially be de-anonymised should still be treated as personal data.[10]

Those who have intellectual property rights in datasets also have legal interests which create obstacles to data sharing:

- the creator of a dataset will sometimes, though not always, own intellectual property rights in part or all of the data, most likely either copyright or database right. Or indeed, these rights may be owned by a third party and the creator will have an obligation to respect those rights (see Section 3.3). These rights enable their owner to control access and copying by others. Even if the current possessor of the dataset did not create it, the possessor might still own or be able to enforce the intellectual property rights by virtue of an assignment of licence of those rights from the creator; and

- until the dataset becomes publicly disclosed, it will be confidential to its owner and this allows the owner to use the law of confidence to control access and copying (see Section 3.2).

These legal interests give commercial value to the dataset and enable their possessor to control commercial exploitation by others. The owner of a valuable asset will often wish to place conditions on its use so as to secure a return on investment and prevent the asset's value to its owner being diminished; and if it is disclosed widely by being placed under the rules of a data trust, the owner may have no practical way of securing any further direct return from its use. This is not to say that owners of rights in data will never be willing to share the data without restrictions – the rights owner may have altruistic motives, as is seen for some rights owners in the case of the wildlife pilot project, or may perceive the likely return from exploiting the rights to be less valuable than the collective benefit from unrestricted data sharing – but a data trust will at least need to consider whether it needs to incentivise potential data providers by offering the possibility of use restrictions.

One essential characteristic of any data trust is that its legal structure, governance and operating practices make sharing of data possible while still respecting these varying legal interests.

Data trusts can increase efficiency here because data users will only need to enter into a single data use agreement with the data trust, rather than negotiating individual agreements with each data provider. This single point of agreement may also assist start-ups and SMEs who lack the experience and expertise to negotiate appropriate data sharing agreements because they can rely, to some extent at least, on the data trust's expertise in this area.

Thus one essential characteristic of any data trust is that its legal structure, governance and operating practices make sharing of data possible while still respecting these varying legal interests.

1.2 Ethics and public benefit

Data trusts might aim to achieve more than mere data sharing, which could otherwise be achieved (to some extent at least) by legally binding agreements between providers and recipients. These data trusts would have the additional purpose of achieving a societal or public benefit which is wider than just the benefit gained by those who make use of data, and which will be part of the justification for sharing data in the first place.

If those data trusts did no more than respecting the legal interests discussed above, they might not be considering the public benefit adequately. A number of ethical issues would therefore need to be provided for, most saliently:

- assuring the credibility, trustworthiness and reliability of the data analysis which makes use of data in the data trust. These are highly dependent on the quality of the data used for analysis. To provide assurance, there is a need for those who generate that data to be accountable both to other data users and to wider society for its accuracy, completeness and provenance. There may also be concerns about the credibility, trustworthiness and reliability of the methods chosen by data users to process the data, and the data trust might wish to concern itself with these too. The internal norms and rules of data trusts will need to provide assurance mechanisms which aim to achieve a high level of accountability, in addition to protecting individual rights and interests.
- complying with other ethical obligations which aim at protecting the public interest. Some of these will be at a sectoral level, and for some sectors there may even be internal or external regulation about which the data trust needs to provide guidance or assistance to data providers and users to help them achieve compliance. For example, medical ethics are relevant to any decision to share patient data, and are subject to the legally binding regulation of the medical professions as well as to those professions' own internal ethical codes, breach of which can lead to sanctions for medical professionals. All kinds of data-based research raise broader ethical issues, and each data trust will need to decide how far to take these into account when developing governance and operating procedures. Should, for example, a data trust impose obligations on those using its data to obtain ethical oversight for their work? If so, how should it do so? Some idea of the difficulties can be seen in the outcry over Facebook's experiment to identify how far the content of its users' news feeds affected their emotions.[11] This research relied on ethical review by Cornell University, which undertook the research in partnership with Facebook, but that review examined only the plans of Cornell's own researchers and assumed that no ethical issues arose in respect of Facebook's activities.

Appropriate responses to these, and other, ethical issues will need to be built into the governance and operational processes of the data trust (see Section 6).

[7] See Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 45-47, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

[8] As this report explains in Sections 2.2.1 and 3.3, data cannot be owned in the same way that physical property is owned. We use "ownership" here to denote the legal rights which a person who possesses data has which can be used to prevent others from using that data.

[9] Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", (2010) UCLA LR 1701.

[10] EU Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP216, 10 April 2014).

[11] Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, 2014. Experimental evidence of massive-scale emotional contagion through social networks. http://www.pnas.org/content/111/24/8788.full. For reactions to this experiment see eg "Facebook reveals news feed experiment to control emotions", The Guardian 30 June 2014; http://www.independent.co.uk/life-style/gadgets-and-tech/facebook-defends-secretly-manipulating-users-emotions-says-experiments-improved-our-service-9572145.html.

Queen Mary University of London

1.3 A data trust does not need to be a legal trust

Many discussions of data trusts assume that they will also be a legal trust. But, for the reasons explained in Section 2, we think this is highly unlikely. Legal trusts are possibly the least suitable legal structure for this purpose.

The conception of a legal trust is that a person or group of persons, the *trustees*, become the legal owners of *property*, but have an equitable obligation to hold, use and deal with that property solely for the benefit of a different group of persons, the *beneficiaries*. At first sight, this seems to fit with the idea that a data trust's role is to preserve the interests of those who have rights in data. Why should that data not be owned by trustees, but used only for the interest of those who are defined in the trust documents as the beneficiaries of the data trust?

The simple answer is that data is not capable of constituting property in the legal trust sense, and thus cannot form the basis of a legal trust in any of the legal systems which have a concept of trust law.[12] But even if data were recognised as property for trust law purposes, there are two more important reasons why trust law is unsuitable here:

- first, a legal trust must be run for the benefit of the beneficiaries, not the wider public. The exception to this is a charitable trust, which we have not examined because the restrictions of charity law mean that a charitable trust would only be suitable for a minority of data trusts.[13] For an ordinary legal trust, trustees are required only to consider the collective interests of the beneficiaries when dealing with trust property. This means that they cannot allow data to be used for some socially beneficial purposes if that use does not also benefit the legal trust's beneficiaries, i.e. those described in the trust deed.
- second, the trustees are obliged not to use the property of the legal trust in a way which generates benefits for themselves[14] unless the trust deed specifies otherwise.[15] This means that providers and users of data will find it difficult to be trustees if they are envisaging benefits for themselves as a result of data sharing. This is likely to deter many organisations, particularly data providers, from participating. The requirement that (subject to the trust deed) any financial benefit received as trustee may not be retained but becomes trust property,[16] is an obvious reason why this form of data trust is unlikely to be viable for commercial actors.

Thus even if a data trust could be constituted as a legal trust, that legal structure would prevent it from doing many of the things a data trust is intended to achieve.

This tells us that we should not, initially, focus on one particular legal structure for data trusts. Instead we need to identify what a data trust is aiming to achieve. Once that is known, there are alternative legal structures which can be adopted, with suitable adaptations, which will allow the data trust to achieve its aims. These structures are examined from a legal perspective in Section 2, and some of the legal issues which arise from a range of possible commercial and organisational choices are analysed in the legal landscape review.[17]

1.4 What a data trust might be

From a legal perspective, a data trust is a mechanism for achieving a defined set of aims. At the highest level, those aims are:

- to enable data to be shared;
- for the benefit of those sharing 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 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 the data trust comes to an end.

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

- collective management of individual 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; and
- ability to evolve to have new purposes, governance and working methods.

One important point to note is that data sharing between members of a small group of commercial organisations can easily be managed through already known contractual legal structures, and the mechanism of a multi-party data sharing agreement is simpler and cheaper than that of a data trust. However, if the group of those sharing data is large, and particularly if their interests are not closely aligned, then use of a data trust might be appropriate. This is also so if the membership of the group is likely to be changing constantly, because admitting new members to a data sharing agreement requires the agreement of all the existing members.

The legal analysis in this report investigates the law as it would apply to a mechanism with these high level aims.

Of course, each individual data trust will have much more detailed aims, and these will affect the answers to questions such as "What legal structure should the data trust adopt?" and "How should it be governed?" These detailed aims will also affect the application of the law because law's meaning depends on the particular factual circumstances, and a different context may lead to a different legal answer. Thus this report outlines the general framework of the law as it applies to data trusts, but cannot (without further detailed analysis) give the specific answers which individual data trusts need.

In an ideal world the analysis in this report would enable the construction of a "repeatable framework" and "standardised, repeatable terms"[18] for structuring and operating a data trust, so that prospective data trusts could simply adopt a clear template and follow a set of guidelines. As will become apparent on reading further, however, this is not achievable. Each data trust will be driven by its overriding aims and objectives, and also by the needs, desires, rights and interests of its stakeholders. That combination will be different for every data trust, so that if the legal structure, rules and governance of the data trust do not fit appropriately then the data trust will not attract data providers and data users and will face opposition from data subjects and others with rights and interests in the data. That said, it has been possible to identify in this report the main legal options available to data trusts, and the reasons why each might be adopted or rejected. This information should be of real use to prospective data trusts when devising their own, individual, frameworks.

Each data trust will be driven by its overriding aims and objectives, and also by the needs, desires, rights and interests of its stakeholders.

[12] Although trusts are a purely common law concept, equivalent legal structures are available elsewhere – see Lillian Edwards, "The problem with privacy: A modest proposal", (2004) 18 International Review of Law, Computer, and Technology 309, 326. However, expert commentators agree that in the current state of the law it is highly unlikely that a court will classify information or data as a species of conventionally understood property – for a useful overview and analysis see Jeffrey Ritter & Anna Mayer, "Regulating Data as Property: A New Construct for Moving Forward", (2018) 6 Duke Law & Technology Review 220, 247-252.
[13] See the Legal landscape review (http://theodi.org/article/data-trusts-legal-landscape-review/) for an analysis of some of these issues.
[14] Aberdeen Town Council v Aberdeen University (1877) 2 App Cas 544.
[15] The difficulty here is defining the permitted benefits in advance, and in ensuring that the trustee's overriding fiduciary duties are not compromised.
[16] Bray v Ford [1896] AC 44.
[17] Legal landscape review (http://theodi.org/article/data-trusts-legal-landscape-review/).
[18] See Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 45-47, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

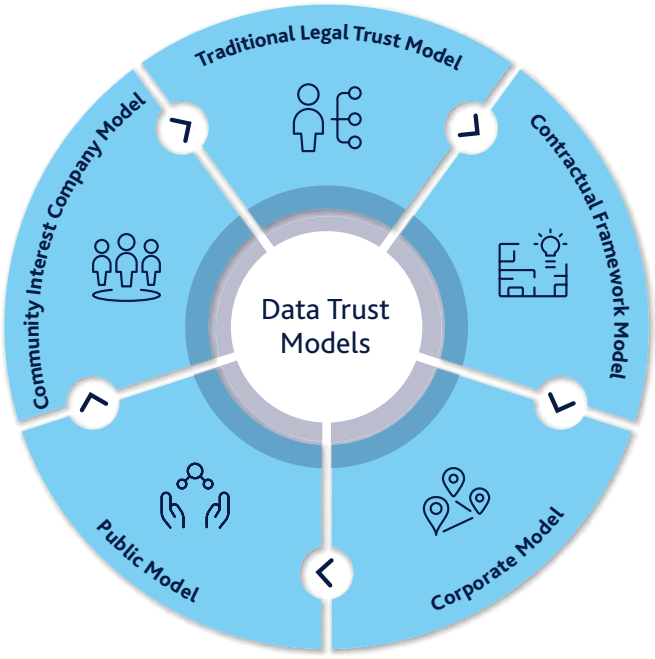
SECTION 2
Potential legal structures

The preferred legal structure for a data trust is, of course, key to determining its ability to enable the purpose of a data trust to be fulfilled. Further, the choice will affect the governance structure of the data trust, compliance with the data trust's rules, and what happens to the data on termination, in addition to the other points referred to in later sections of the report.

The potential options available to structure such a data trust are identified below, together with the advantages and disadvantages of each and a consideration of which, under the various circumstances, would seem to be the most appropriate.

2.1 Options

Five potential legal structures for the data trust model are identified below.



2.1.1 Traditional legal trust model

The traditional legal trusts model adopts the structure that is used when a legal trust is commonly applied to assets being cared for by trustees for the benefit of the trust's beneficiaries, and may apply to the sharing of data. In a traditional legal trust, a settlor gives assets to the trustees, who technically own the assets, in this case being data, but who are obliged to use them for the benefit of the beneficiaries, under the auspices of the document that created the legal trust.[19] The appeal of this as a model is obvious as it seems similar to the original concept[20] of a data trust, a model where data is provided to the legal trust and managed by the trustees for the benefit of its beneficiaries.

2.1.2 Contractual framework model

The theory behind this model is to have something akin to a standard form of data sharing agreement[21] that would, without having a separate organisational structure in place, form a contractual agreement by which data providers provide data which the data trust can allow to be used by third parties within the aims of the data trust.[22] Also party to the contract would be anyone involved in the actual processing of the data. This model would require third parties accessing the data to enter into an agreement with the data provider for its use, thereby assuring the data provider that the third party will use the data in the prescribed way, and a method of redress for breach of contract if they do not. Additionally, a contract signed by two parties (for example a data provider and the data trust) can purport to give rights to a named third party, or named category of third parties, capable of being enforced under the contract.[23] It should be noted though that, although such a provision grants the right of a third party to enforce under the contract, if the third party is not a signatory or has not otherwise agreed to the terms, then the contract cannot purport to give that third party the burden or legal obligations under the contract.

The structure of a data sharing agreement under the contractual framework model would be in a similar form to other signed written agreements. Typical provisions under such a standard form

[19] Whishaw v Stephens [1970] AC 508, HL
[20] See Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 46-48, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk.
[21] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf
[22] Chris Reed and Irene Ng, Data Trusts as an AI Governance Mechanism (23 November 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3334527
[23] The Contracts (Rights of Third Parties) Act 1999
[24] Competition Act 1998
[25] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[26] S.171 Companies Act 2006
[27] S.3(1) Companies Act 2006
[28] S.11 Companies Act 2006
[29] https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies

agreement relate to each party's obligations in keeping confidential information protected, provisions relating to the return or destruction of confidential information and restrictions in terms of disclosure, to name a few. Additionally, there will be provisions that limit the purpose for which the data is used, for example for a specified purpose stated from the outset, the purpose for which the data trust was created or limited in a way that would prohibit damage to the provider's interests. It is important that restrictions on who can access the data do not mean that there are issues under competition law for offences like abuse of a market position.[24]

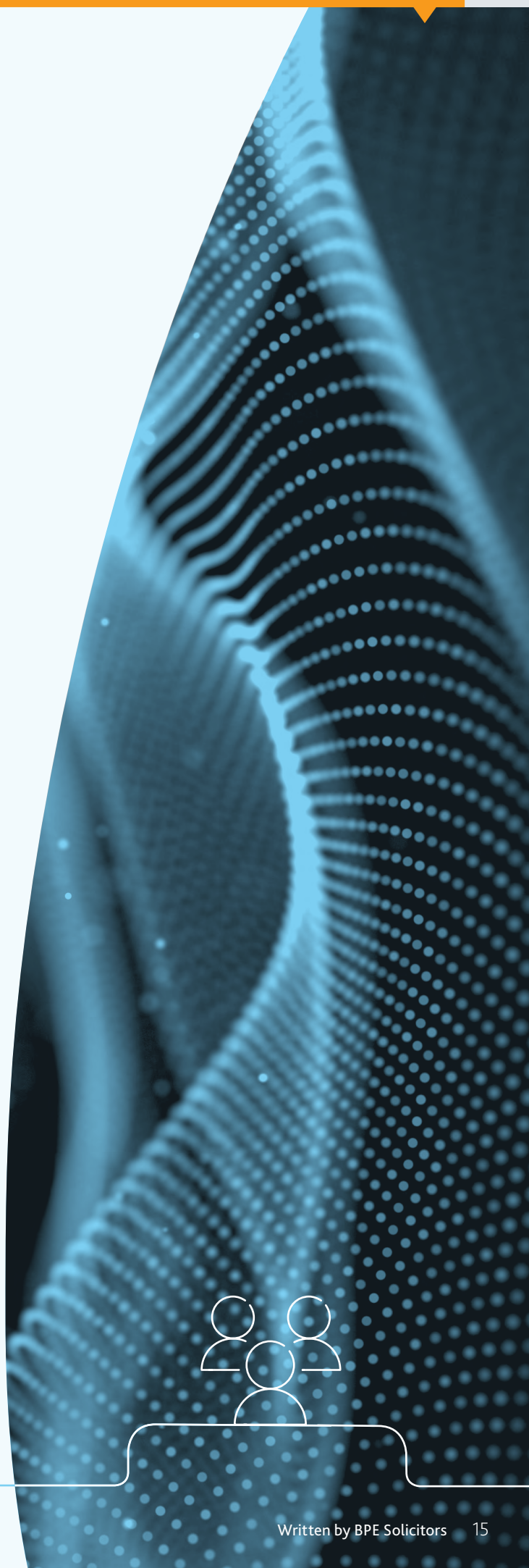
There would also potentially need to be a supplementary agreement, including standard clauses to ensure security of personal data, in the event that it is transferred to a party outside of the European Union.[25]

2.1.3 Corporate model

A corporate model envisages either a separate company or partnership being set up that would manage provided data and afford access to it. Alternately, a group structure involving an unincorporated association could be used. If a corporate form is followed which has its own legal personality, data providers would provide (most likely, license) their data to the corporate organisation to use. Representatives of the data providers, or independent externally appointed and mutually agreed individuals, might act as the directors making decisions on the day-to-day running of the data trust.[26] "Shareholders" of the company could potentially be the data providers.

A further possible structure within the corporate model that also has its own separate legal personality is a Limited Liability Partnership ("LLP"). The LLP model is suggested over a normal partnership model due to there not being unlimited liability for the partners of the LLP. This means that in the event of involuntary insolvency of the data trust or an adverse claim being made against it, then the liability of the partners under the model would be limited. Each member will be an equal partner with a right to any distributions under the partnership and an equal say in the decisions made by the partnership.

A company limited by guarantee ("CLG") is similar to a company limited by shares. However, there is no share capital[27], and therefore distributions (if there are any) are made to members of the CLG equally regardless of contribution to the data trust. Often though rather than a distribution being made, funds are retained and put towards the organisation's stated social purpose. For this reason the model tends to be used for NGOs, clubs or schools/churches to name a few. Members have very limited liability[28] and the structure allows for any number of objectives to be followed although these tend to be community-minded or at the very least non-commercial, as any profit that can be distributed to members would have to be to each member equally as there are no shares that a member could hold more than one of. A CIC (detailed below) can be a form of CLG that is assured it pursues its social purpose by the Office of the Regulator of Community Interest Companies.[29]



In the case of an unincorporated association, this is an informal structure of an organisation that has no separate legal personality[30] and as a result has no inbuilt organisational structure or ability to hold assets in the name of the organisation, therefore making it generally an unsuitable form for a data trust.

It is important to note that a data trust is unlikely to take the form of a charity organisational model as, in order to obtain charitable organisational status, the data trust would have to ensure the data were used exclusively for the public benefit.[31] This would mean that data providers would in no way be able to benefit from the running of the data trust, and that would likely preclude individual data providers, and outright inhibit commercial organisations from providing their data, as to do so with no benefit to the company would put the commercial organisation's directors in breach of their duty to promote the success of the company.[32] A commercial organisation could support a charity, and many do so in order to meet corporate social responsibility goals and for the reputational benefits, but if the aim of the data trust is to receive a return on the data held then a charitable form would be wholly inappropriate.

Similarly, co-operatives and community benefit societies are unlikely to be appropriate and therefore not covered further in this analysis. This is because, whilst they are separate organisational structures to which data could be licensed, co-operatives operate for the benefit of their members, thereby potentially precluding pursuing an additional social purpose, and community benefit societies operate for the benefit of wider society, thus potentially running in contradiction to the wishes of its members. Additionally, in the case of a co-operative, each member gets an equal share and say in how the co-operative is managed. This could raise difficulties for some data providers who are providing lots of valuable data, causing them to potentially resent those who have an equal say to them, but who have only provided small amounts of less valuable data. Organisations that have a share structure would therefore mitigate such an imbalance.

2.1.4 Public model

This model does not currently exist but hypothesises a public regulator that would set the standard, set out rules applicable to the regulation of all data trusts and enforce any breaches of these regulations. This could either be set up as an independent organisation whose aim is to be a regulated data trust, or else the role could potentially be subsumed into the Information Commissioners Office ("ICO") current role of enforcing data protection legislation.[33] The data trust would already be subject to ICO authority as a processor of data but potentially specific compliance points unique to data trusts could be included under their scope. This would mean that whilst the data trust itself would take some other form, likely organisational or corporate, the data trust rules, standards and regulation would be dictated by a third-party public body.

2.1.5 Community interest companies model

A community interest company ("CIC") is a form of company that focuses on non-charitable social enterprise but does not have to operate exclusively for the company's social purpose[34] and can even share distributable profits

[30] Hanchett-Stamford v Attorney General [2008] EWHC 330 (Ch)
[31] S.4 Charities Act 2011
[32] S.172 Companies Act 2006
[33] https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/
[34] Companies (Audit, Investigations and Community Enterprise) Act 2004

as dividends to its shareholders (albeit subject to a maximum aggregate cap of 35 per cent of distributable profits).[35] In essence, a CIC will have the same governance structure as a company with a few directors making decisions on the running of the company, but it has a social purpose which is stated on founding the company. The CIC will need to demonstrate to its regulator, the Office of the Regulator of Community Interest Companies,[36] that it is operating towards this purpose.

2.2 Advantages and drawbacks

2.2.1 Traditional legal trust model

Advantages

The traditional model has the advantage that it is an established legal structure for the stewardship of assets such as money or property, for the benefit of beneficiaries. Furthermore, the wider public might also have had experience with legal trusts in a personal context, and thus they might have assurance that a data trust will follow a rigorous set of pre-existing legal provisions for managing their data. Additionally, the trustees would be bound to follow the rules of the legal trust and if they breach their fiduciary duties under the legal trust they could be personally liable for any loss. This could be seen as beneficial to the data providers, but a detriment to anyone acting as a trustee. Whether this would be preferable would depend on the purpose of the data trust and the particular stakeholders.

Drawbacks

The key disadvantage to the traditional model is that the law, as it stands currently, does not consider data to be an asset capable of being held under a legal trust, i.e. as property.[37] Additionally, a traditional equitable trust of physical assets, as it stands, can only be managed for the benefit of the beneficiaries under the legal trust.[38] This not only means that the public benefit of the trust data is at best a secondary aim, but it equally means that trustees themselves cannot benefit from administering the legal trust unless the legal trust deed expressly permits this, although they can be indemnified out of trust assets for all costs, charges and expenses that are properly incurred.[39] This therefore means that the trustees would have to be independent of the beneficiaries (in this case the data providers as well as data users), otherwise the providers would not be able to receive a benefit from this model.

2.2.2 Contractual framework model

Advantages

The contractual framework model has the benefit that it is reasonably flexible and can be adapted with relative ease to different data trust requirements, as appropriate. The cost of setting up is also low, although fees that are paid to processors for analysis of the data might be a factor, and changing the rules can be as easy as amending the contractual arrangement (albeit with the consent of all signatories to the current contractual framework).

Disadvantages

There are several drawbacks to this model. First, that the form of contract would have to be carefully scoped to provide a fair benefit to each of the signatories and ensure that the responsibility for breaches of the data trust contractual arrangement lies with the appropriate party at fault. Additionally, it would be those who are party to the contract who are bound by it and not third parties who have not signed the agreement. This would mean that any third party wishing to access data would have to enter into an agreement with each data provider to pool the data together for their particular need, as the contractual framework would mean that there is no centralised entity through which data is shared. It is possible for there to be a set of "club rules" to which each party to the data trust will assent when joining the data trust.[40] This set-up could be a set of mutually agreed to rules under which data sharing is governed, however it does not address governance structures or provide a separate organisational structure that can manage or facilitate the sharing, relying instead on each individual data provider and prospective data user to manage any sharing arrangement.

2.2.3 Corporate model

Advantages

The corporate model has myriad options on the type of company structure to use. With the exception of the unincorporated association (which is itself not a corporation but is still an organisational structure), corporations would be able to hold assets (such as a database of data) in the name of the corporation and representatives of the stakeholders could make up the board who would manage the day-to-day operations of the corporate body. Additionally there are established forms of governance to dictate the running of the company in the case of a limited company.[41]

Disadvantages

Under the traditional corporate model using the format of a limited company, its directors have a duty to promote the success of the company.[42] This means that directors would be potentially prohibited from acting in a way that benefits the public as a whole unless there was an ancillary benefit to the company, as otherwise doing so means that potential commercial concessions could be made that would mean a director is breaching its duties. No director would want to take on the risk of doing so as it could leave them exposed to a potential derivative claim from shareholders[43] for breach of their director's duties. This is potentially circumvented by having a stated social purpose in the company articles or under other provisions of the Companies Act[44] but the difficulties around this are something that a data trust should be wary of if it opts for the company limited by shares corporate model.

[35] Community Interest Company (Amendment) Regulations 2014.
[36] https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies
[37] Oxford v Moss [1978] 68 Cr App 183
[38] Knight v Knight (1840) 3 Beaver 148
[39] Re Beddoe [1893] 1 Ch 547
[40] Clarke v Dunraven [1897] AC 59
[41] Companies Act 2006
[42] S.172 Companies Act 2006
[43] Chapter 11 Companies Act 2006
[44] S.172(2) Companies Act 2006

It should also be noted that individuals have a marked distrust of traditional corporations[45] as they would see these as purely profit making institutions who do not take into account the public's interests. They would therefore be unlikely to trust a corporation to manage their data, let alone provide it in the first place. An LLP model has a similar issue with being primarily profit seeking, with the added difficulty of each partner having an equal say in the running of the LLP meaning those who provide large contributions to the data trust will have as much of a vote on matters as those who contribute less.

A CLG model, as discussed above, is a model that is already typically used for non-commercial organisations such as trade associations and societies. In terms of the structure, a CLG has many of the same benefits and disadvantages that a CIC has (discussed below). In fact where the CIC takes the form of a CLG rather than being limited by shares, the disadvantages are nearly identical. The main disadvantage of a CLG as opposed to a CIC is that there is that there does not have to be an in-built social purpose beyond what is included in the CLG's articles of association. Additionally there is no regulator ensuring that the social purpose of the CLG is being followed. Neither of these is necessarily a disadvantage for a data trust, but if it wants to hold itself up to a high ethical standard to engender public trust then this might be a drawback of a CLG over a CIC, which is not itself a CLG, model. Also, by not having a share capital, there is the potential for an imbalance in decision making as all data providers, regardless of their contribution, have an equal share in the CLG.

With the unincorporated association, the fact that the organisation cannot hold assets in its own name means that a central database of data would have to be held and controlled by a single party, leading to a potential imbalance in control between contributors. The other alternative is to have each data provider hold their own data and enable data users to access this data directly, which is similar to the current system of accessing data. Additionally it seems unlikely that other commercial actors would licence their data when it would be under the purview of another commercial entity, who could potentially take advantage of that data, rather than someone independent. Further, the unincorporated association has the issue that there is no structure of governance to dictate the relationship between members of the organisation beyond any organisational rules.[46]

2.2.4 Public model

Advantages

There are several key benefits to this model. There would be a consistent standard of rules applicable to all data trusts that would automatically apply and that they would have to be governed by. Additionally, by having a public regulator, who would enforce compliance on behalf of the data trust to the overall public benefit of data trusts, would likely waylay some of the fears the public would have in giving their data to the data trust.

Disadvantages

The big disadvantage to the public model is that no such regulator exists within the current government structure. In order for one to be created (in itself a slow process), the government would have to see the benefit in having one. There would also be a potential cost involved in having a regulator and an extra cost involved in enforcing compliance and managing data trusts, which would either come from the government's already strained budget, or represent a fee or tax on data trusts to cover the cost. Finally, whilst a regulator gives a form of trust rules by which data trusts should comply, there would still need to be an organisational structure to the data trust to manage the sharing and access to data. A public regulator would therefore have to be supplemental to any organisational structure of the data trust.

2.2.5 Community interest companies model

Advantages

The key feature of a community interest company ("CIC") is that, due to its hybrid nature, it has the governance and organisational structure of a company, with a few people (the board) being able to make day-to-day decisions on behalf of the CIC without input from the data providers (potentially its shareholders). A CIC can either be limited by shares or guarantee, meaning that there can either be members with an equal right to distribution (limited by guarantee) or a right to a distribution on the basis of contribution to the CIC (limited by shares). Commercial organisations, who perhaps contribute more data than individual data providers, could have either a voice on the board or a greater proportion of shares to reflect their more significant contribution. Also, crucially, unlike with a normal corporate structure, the principal goal of the CIC is for a particular goal to benefit the public (for example the open sharing of data), yet data providers are able to benefit from the running of the CIC. This is either through shared data produced in the course of running the data trust itself, or through an (albeit capped) ability to draw dividends which reflects a return to shareholders.

This would mean that commercial or individual data providers could potentially benefit from providing data as they could receive a share of the proceeds that any third party pays for access. This would therefore mean that a director that provides its company's data to the data trust is not necessarily in breach of their director's duties, as the commercial organisation could receive a tangible monetary benefit in addition to the benefits they might gain from collective analysis of the shared data. Additionally the CIC model allows for those data providers, who so wish, to have a seat on the board and therefore be more involved in the everyday operation of the data trust.

The fact that the purpose of a CIC is also regulated by an existing government entity might also reassure data providers that their data is not purely going to be exploited for the CIC's commercial benefit, but that the primary goal is to the wider society (although there will also be controls within any data licensed to the data trust that would prevent a breach of the GDPR by making use of the data beyond the purpose for which an individual consented). Such a CIC structure is also capable of being in place now and each CIC will have to prove each year to the regulator that it is acting in the public interest.[47]

Disadvantages

Currently it has never been tested whether the CIC regulator would consider the data trust format capable of being a CIC. In order to do so, a prospective CIC would have to show that a reasonable person might consider its activities to be in the public benefit.[48]

A further point to consider is the feature of a CIC called an "asset lock"; this prevents assets being used for the benefit of the members of the CIC, its directors or employees, unless such use of assets is incidental to the CIC's given social purpose. This would prevent an irrevocable licence of data from a data provider being returned to that provider say for example in the event of the insolvency of the data trust. The workaround for this is to have any data licensed to the data trust being terminable on immediate notice thereby allowing the asset to "snap-back" into the ownership of the data provider. Whilst this is a legally correct way of avoiding the asset-lock mechanism, the fact that it is a workaround and adhering to the letter rather than perhaps the spirit of the law, it might be viewed unfavourably by the public as a whole.

2.3 Legal obstacles and difficulties

As can be seen above each potential model comes with its legal issues.

One model suggested to "bypass" the legal requirements is a technological model. This is one method that has not been covered in the preceding parts above as it is a solution that eschews regulation, law and rules in favour of technological controls that would effectively achieve the same function of providing access to data in such way as is consented to by the data providers, but to the benefit or all commercial actors involved and to the wider benefit to the public. This model has been suggested as a potential structure. However, as it is not a legal structure, it has not been covered in further detail in this legal report relating to data trusts. Additionally, a technological model would still be subject to the provisions of the GDPR (see below) and other legal regulations and therefore there would likely still need to be a suitable governance structure and way to ensure compliance so that the data trust can maintain public faith. Additionally the technology is not suitably developed enough to allow this to be a model that can be implemented now.

If a technical workaround is therefore not possible at this time, the choice therefore falls to one of the other models suggested above. The traditional legal trust model would need alterations to the law either by having data classed as property and therefore capable of being an asset that can be held in trust, or by altering trust law to provide for data as an exception to the requirement that legal trust assets must be "physical".[49] Arguably these changes are too fundamental to be realistic solutions particularly as such changes would need to be initiated through legislation, which is a slow and uncertain process.

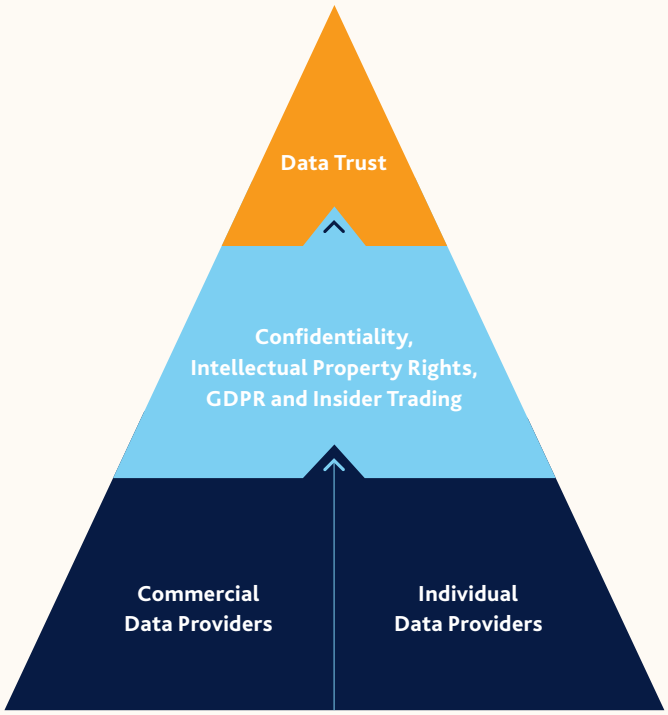
The public model also potentially falls at the same hurdle in that it requires an input from the government to set in place the structure of a regulatory body who would put in place the data trust rules, and who would be responsible for enforcement actions for beach of the rules. The contractual model, without having a central entity under which decisions can be made and the data pooled, seems little more than an expansion on current data sharing agreements and is a format that would be particularly unwieldy for large contributions of data from multiple data providers.

This leaves an organisational model of which a charity format would prohibit any benefit being returned to the data providers and the traditional limited company model can potentially have restrictions around benefits being provided for the wider public. The hybrid model of a CIC potentially reconciles the two and provides the organisational structure under which data can collectively be licensed to, and that allows a pre-established decision-making structure to be in place. Evidently though as this is not a pre-established form of benefit that the CIC regulator would have encountered before, potential CICs would have to persuade the regulator that the suggested form of data trust organisation fulfils the public interest criteria to be classed as a CIC. If this is not fulfilled and the benefit is seen to be strictly for the data providers and data users only, the format is closer to being a form of special purpose vehicle company specifically set up for the pooling of data for a specified purpose and the benefit of the data providers only.

[45] https://yougov.co.uk/topics/politics/articles-reports/2015/09/25/british-people-dont-trust-major-companies-and-orga
[46] Hamlet v General Municipal Boilermakers and Allied Trades Union [1987] 1 All ER 631
[47] https://www.gov.uk/government/publications/form-cic34-community-interest-company-report
[48] Section 36A Companies (Audit, Investigations and Community Enterprise) Act 2004
[49] Oxford v Moss [1978] 68 Cr App 183

SECTION 3
Providing data to the data trust

In order for a data trust to be useful, it must be populated with data to analyse and utilise accordingly. Whilst data providers can license the use of their data freely, the data trust will have to note various restrictions imposed by legislation and the common law when it is in receipt of this provided data.



3.1 Privacy and data protection

3.1.1 GDPR introduction

Data and privacy is particularly topical at the moment and on people's minds in the wake of news such as the Cambridge Analytica scandal.[50] Although implemented before this particular scandal hit, but after the actual offending data mining had taken place, the *General Data Protection Regulation ((EU) 2016/679*) (the "**GDPR**") details stricter requirements for organisations processing individual's personal data. This would be relevant for anyone licensing personal data to the data trust for their use (and is also applicable across all other elements of the data trust). The provisions of the GDPR were implemented into the law of England and Wales under the *Data Protection Act 2018*, but crucially its provisions will apply to all EU member states, so for that reason we refer throughout this report to the GDPR. It should additionally be noted that the Data Protection Act 2018 amended certain national laws to comply with the GDPR as this was directly applicable into the law of England and Wales upon it being put in place. It specifically made updates to derogations and the supervisory authority and covers personal data processing beyond what is covered under the GDPR.

GDPR prohibits the processing of personal data unless there is a lawful basis for that processing, as set out in Article 6. These are:

i) **consent** (individual has given clear consent for processing of their personal data);

ii) **contract** (processing necessary to fulfil the contract with an individual or because they have asked the organisation to take certain steps before entering into a contract);

iii) **legal obligation** (processing necessary to comply with non-contractual legal obligation);

iv) **vital interests** (processing necessary to protect someone's life);

v) **public task** (processing necessary to perform task in the public interest); and

vi) **legitimate interests** (processing is necessary for your legitimate interests or those of a third party, unless privacy interest overrides this).[51]

[50] https://www.theguardian.com/uk-news/cambridge-analytica
[51] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
[52] Article 4(11) GDPR
[53] Article 7 GDPR
[54] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/
[55] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
[56] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/
[57] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/
[58] EU Article 29 working party, opinion 05/2014 on anonymization techniques (0829/14/EN WP216)
[59] Article 4(1) GDPR
[60] GDPR Recital 26
[61] Scarlet Extended SA v Societe Belge des Auteurs, Compositeurs et Editeurs SCRL (SABAM) (Case C-70/10) [2011] ECR I-11959
[62] Breyer v Bundesrepublik Deutschland (Case C-582/14) [2017] 1 WLR
[63] GDPR Article 4(1)
[64] GDPR Article 13(1)
[65] Article 13(2) GDPR

Whilst under certain circumstances all of the potential bases for processing could apply, the most likely to be relevant to a universal structure of a data trust is the "consent" basis. Not only is this because consent can apply to all potential scenarios, it also means that the data provider is engaged and likely to have more confidence in the data trust than if his information were used without his consent. To be valid consent it must be "freely given, specific, informed and unambiguous".[52] Consent should also be able to be withdrawn at any time. This means that, if this legal basis for processing is used, data providers' data should be able to be removed from the data trust.[53]

There might also be some forms of data trust where the legal basis of "legitimate interest" could be relied upon by data users to process the data. However, this would be very much dependent on the data trust itself and this basis of processing does not engage potential data providers in any way. It might, though, be possible to construct a legitimate interest justification for the initial provision of data by the data provider (see Section 8.3.1 for detailed discussion).

Whilst the "public task" might seem like a useful basis to ensure lawful processing of personal data, the interpretation and treatment of this is construed narrowly. It relates to public authorities either carrying out its duties as a public body or doing something that is within the public interest which, in the context of the GDPR legislation, means something that has been "laid down by law". An example of this would be a private water company processing personal data in order to carry out its normal function of running its service as a utility provider (a power granted to it under legislation).[54] This would therefore prohibit private bodies relying on this basis and even public bodies if the processing fell outside its usual role or wasn't encapsulated under law. Additionally whilst the public might be assured that this basis is limited to public bodies processing their data, circumventing their consent might create resentment in the long term. Regardless of what form of basis for data processing is used, there will need to be a legal basis in order to be compliant with the provisions under the GDPR.

Further more stringent requirements are needed when special category data is processed (for example information about a person's: **i)** race; **ii)** ethnic origin; **iii)** politics; **iv)** religion; **v)** trade union membership; **vi)** genetics; **vii)** biometrics; **viii)** health; **ix)** sex life; or **x)** sexual orientation).[55] Processing can be permitted for these higher risk categories of data with explicit consent to the particular use of data under *Article 9(2)*.

It should also be noted that under *Article 8* of the GDPR and Section 9 of the Data Protection Act 2018, the personal data of children below the age of 13[56] can only be processed on the basis of consent where they are being provided with an online service "if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child". If the data trust falls outside of being such an online service then children who are deemed to be competent, as assessed on a case-by-case basis, can give their consent to the processing of their data, otherwise parental consent is required.[57]

Due to the stringent requirements that the GDPR imposes (see below) it might be tempting to circumvent the classification of data as "personal" by using anonymisation techniques, however this is not fool proof or without issue. If the data can be subjected to de-anonymisation techniques then the data will still be considered personal data capable of being regulated under the GDPR.[58] A data subject is the identified or identifiable person to whom the personal data relates, with a person being identifiable if he or she "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more fact so specific to the physical, physiological, genetic, mental, economic, cultural or social identity".[59]

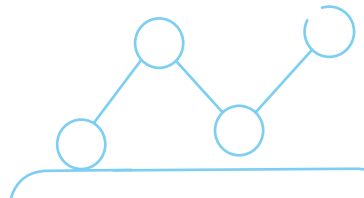
3.1.2 Anonymisation and pseudonymisation

If using anonymisation techniques within a data trust, whatever its legal form, consideration should be taken of all reasonable means (taking into account cost and technology) that someone is likely to use to identify a person including by "singling out" (i.e. identifying a person other than by name or address). This therefore means that pseudonymised data can still be considered personal data.[60] For example, web-user IP addresses are considered personal data as users can be precisely identified[61] or additionally where the website operator has "the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person"[62] which the GDPR specifically identifies.[63]

3.1.3 GDPR requirements

If the GDPR regulations apply the processing organisation must comply with: **i)** lawfulness; fairness and transparency; **ii)** purpose limitation; **iii)** data minimisation; **iv)** accuracy; **v)** storage limitation; **vi)** integrity and confidentiality; and **vii)** accountability.
Upon collection of the data subject's data, the data controller is duty bound to provide the data subject with numerous pieces of information that help engender the trust of the data provider. These include the identity of the controller, contact details of the data protection officer of the controller, the purpose for which the personal data is collected and the recipients or categories of recipients of the personal data to name the key ones.[64]

The data controller must also provide them with additional information in order to ensure the transparent processing of data including the period for which the data will be stored, the existence of the right to withdraw consent to use of the data at any time or request restrictions to be placed on use of that data, the right to complain to a supervisory authority and the other provisions that essentially detail how the data is to be processed.[65]



If the data is obtained from a third party, the receiving controller must provide the data subject with the same information within a reasonable period after obtaining the personal data up to a maximum period of one month[66] with the controller taking into account the circumstances the data was received and whether providing that information would be disproportionate.[67] If the data is being disclosed to a third party, then this information should be provided to the data subject at the latest when the data is first disclosed.

It is therefore apparent and within the general ethos of a data trust as we understand it, that consent could be the best option to meet the relevant data protection requirements. A data trust would have to be open and honest about the use of the data in order to provide fully informed consent and there would have to be information as to who will be able to access the data so that any common law confidentiality is not breached (this is further discussed in Section 3.2.1).

Whilst consent is likely the most appropriate legal basis for the processing of personal data in a data trust, the key issue is how such consent can capture all the potential usages of data that the data trust might wish. Of course each time an interested third party wants access to the data trust's data, which includes the personal data of the provider or data subject, the data trust could send an opt-in consent request to the data provider for the usage. The difficulties here however are both the increase in the amount of administration that this would involve and the risk of "consent-fatigue" on the part of the data providers. Additionally, if no consent is received the data cannot be processed, which could lead to the data trust holding large amounts of data that cannot be used.

The crucial point will be to draft a consent document that is clear enough that individual data providers are aware of what their data is being used for but wide enough that it captures all the potentially conceived purposes for the data being shared. This would result in only one initial consent being necessary and it would cover all the future uses of trust data that the data trust might wish. The data trust could, for example, limit the data being shared to companies that train machine learning software for driverless cars or only with charities that seek to support endangered wildlife, any limitation or expanding of scope will be determined by the needs of the individual data trust. Once the consent document is scoped and signed (or otherwise agreed to), any use that falls outside the agreed to usage of the data provider's data would need a further consent to be obtained. Depending on what the extended purpose is for however, the data trust could use aggregated data, if appropriate, thereby meaning the data is no longer counted as personal under the GDPR as individual data providers are unidentifiable.

3.2 Commercial confidentiality

If a commercial actor is to licence its organisational data to the data trust there will be an expectation that either they will get an ancillary benefit from the donation or that it will be used solely for the benefit of the public. In any case they would want assurances that their data will not be used by competitors to gain a competitive advantage.

There is also the potential issue with companies or individuals accessing data who, whilst not in competition with the data providing organisation, might still negatively take advantage of the data. A financial investment firm, for instance, could use the data available to make investment decisions that could affect the data providing organisation, against the data provider's wishes for the data trust and without their ability to control the flow of data. Journalists equally might access the data to demonstrate the poor success of the goals of the data trust which could negatively impact the data providing organisation in the press.

3.2.1 Confidentiality

It can be possible to legally (although possibly not practically) protect negative use of the data that is contrary to the purposes of the data trust. It is a broad principle of law that a person who has received information in confidence cannot take unfair advantage of it (to qualify, information must be confidential in nature, i.e. have the "necessary quality of confidence" and disclosed in circumstances importing an obligation of confidence). Such rights that are granted by confidential information law can be enforced against any information recipient even where the third party had no knowledge of the confidential nature of the information but became aware of it at a later stage.[68]

Therefore, as long as there are restrictions on the accessing of data, such as an agreement that an accessor of data will keep it confidential and won't use the information for any purpose beyond that which the data trust granted, then it should still retain the protection of being confidential information under common law (or, additionally, contractually confidential if appropriate). Whilst, legally speaking, third parties cannot take advantage of this commercial information in practical terms, this would be hard to enforce as it would be difficult to determine in what way a third party has benefitted from that information without full-disclosure from them. Of course, if the data was commercialised and the use of it became more widely known, then it could potentially come to the attention of the data provider or the data trust that the data was used without their consent.

It is important to note that whilst information that is posted on the internet would likely cause that information to lose its confidential status[69] (with the exception of partial or limited disclosure on websites that would take a concerted effort to find the information), confidentiality can be maintained with the safeguards in place to prevent the widespread dissemination of data trust information.

A company for example would not disclose anything capable of being a trade secret as it would likely lose the protection of being a trade secret as it would no longer have the "necessary quality of confidence" if third parties could access this information.[70]

Information can be disseminated to a large group without losing its quality of confidence provided that each one receives that data on terms of confidentiality (for example for a specific and limited purpose).[71] This would mean that commercial entities would likely require strict controls as to who can access data and that they do so in a way that maintains the confidential nature of the data for example by their accepting to the particular terms of the use of the data in that limited case.

If such public disclosure is limited then a third party trying to take advantage of the data for its own commercial ends would be prohibited from doing so.[72] A commercial entity would also wish to limit access as confidential information could be disclosed where it reveals details of crime or torts committed by the provider of the information.[73] So, whilst a data user could have access to data trust information that is confidential, should that data user come across data that leaves the organisation legally exposed (say that shows it committed a crime or tort), that information could potentially be more widely disclosed.

Otherwise, a third party receiving confidential information would first have to ask the consent of the information provider before the information can be used.[74] A commercial organisation should also ensure that it has not breached its own requirement to maintain confidentiality, by sharing information with the data trust. A commercial organisation is also subject to the GDPR and therefore must comply with the obligations referred to in the section above before transferring any personal data.

3.2.2 Company law requirements

It is also important to clarify the motivation of commercial organisations sharing their data unless there is a direct and quantifiable benefit to the company. Unless there is a joint decision by the shareholders to allow the sharing of data, the directors are bound by s.172 of the Companies Act 2006 which imposes the duty to promote the success of the company. Arguably there is a positive image associated with contributing to a data trust if it is to be used for laudable goals to the benefit of the public. However if there is a resulting commercial detriment a director would be in breach of their director's duties, as long as it can be shown that the directors did not act with reasonable, care and skill in making their decision.[75] The difficulty a director would face however is that a decision that is made with the public good in mind, would be difficult to justify as taking reasonable care to promote the success of the company. It would be arguable therefore that commercial organisations will wish to limit or restrict entirely the opening up of a data trust to any third parties beyond those they will receive a direct commercial benefit from, making a data trust more akin to a data-sharing special purpose vehicle company.

3.2.3 Insider trading

A firm would also have to be aware of not falling foul of the Market Abuse Regulation which relates to inside information, as firms that issue financial instruments (for example shares) are affected by this. If information is shared with a data trust and this information has not been made public, and if it would have a significant effect on the financial instrument's share price, anyone that profits by taking advantage of that information would be liable to prosecution under the Market Abuse Regulation for insider trading.[76] When issuers disclose information to a third party in the normal course of its duties it must make a simultaneous disclosure to the public.[77] There are conditions by which there can be a delay of disclosure of this information provided that: **i)** immediate disclosure is likely to prejudice the issuer's legitimate interests; **ii)** delay of disclosure is not likely to mislead the public; and **iii)** the issuer is able to ensure the confidentiality of the information.[78]

[66] GDPR Article 14(3)
[67] Article 14(5)(b) GDPR
[68] Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31
[69] Barclays Bank Plc v Guardian News and Media Ltd [2009] EWHC 591 (QB)
[70] Saltman Engineering Co Ltd v Campbell Engineering Co Ltd [1948] 65 RPC 203
[71] CF Partners (UK) LLP v Barclays Bank Plc [2014] EWHC 3049 (Ch)
[72] Seager Ltd v Copydex Ltd [1967] RPC 349
[73] Lion Laboratories Ltd v Evans [1984] 2 All ER 417
[74] Seager v Copydex Ltd [1967] 2 All ER 415
[75] Re D'Jan of London Limited [1993] BCC 646
[76] EU Market Abuse Regulation, Regulation (EU) No 596/2014 Article 7
[77] Article 17(8) Market Abuse Regulation
[78] Article 17(4) Market Abuse Regulation

3.2.4 Summary

It therefore seems again as long as all participants consent to the use of the data by the data trust then there would be no issues as long as that consent is not withdrawn. Practically speaking, however, commercial organisations will likely wish to keep tight control over disclosure of confidential or otherwise valuable information to maintain confidence, competitive advantage and prevent adverse actors utilising their data to their detriment. Additionally, any public sector body or individual will also wish there to be controls placed on their data to prevent its widespread dissemination.

3.3 Third party intellectual property rights

3.3.1 Consent and licensing

Evidently, if any third parties have intellectual property rights in the data that the data provider/data providing organisation is providing, then consent of the relevant party will be needed to ensure that there is no infringement of these rights. This would either come in the form of assignment of the legal rights in the property (such as a copyrighted image or patented process) or in a license to use the data for a specified duration and/or purpose. At this time, there is no overarching EU legislation that deals with intellectual property and thus this is dealt with under national laws within jurisdictions with each form of intellectual property having its own provisions that determine how it may be protected and exploited.[79] Enforcement can also be more difficult due to the fluid nature of intellectual property as an asset, meaning that identifying breaches can be more difficult where the intellectual property right is not registered.

Copyright is a statutory property right[80] and is capable of being transmitted by assignment or by operation of law,[81] however moral rights, performers rights and artist resale rights are not. Any copyright assignment of title would have to be signed on behalf of the assignor although this could potentially cover assignment via email.[82] Assignment can be a "floating reverter" where the assignment is limited for a particular time period or reverts on the trigger of a future event.[83]

3.3.2 Database rights

By compiling the data into one place, the data trust itself will generate intellectual property rights in the collection of information from disparate data providers. Databases are considered to be intellectual property under the Copyright, Designs and Patents Act 1988 as "a collection of independent works, data or other materials which a) are arranged in a systematic methodical way, and b) are individually accessible by electronic or other means".[84] This means that the database as a collection is protected by copyright in the same way as any other instance of copyright. It should be noted that similarly as data is not considered an asset[85], a database is not considered tangible property capable of being the subject matter of torts relevant to an interference with possession.[86]

Databases are also protected under Databases Regulations 1997/3032[87] which prohibit the extraction or re-utilisation of "all or a substantial part of the contents of the database".[88] Database rights under the Regulations are limited to 15 years, however if the database is changed in a substantial way this can give rise to a new 15 year period of protection.[89] This database right only arises where there has been a substantial investment in creating the database; any investment in creating the data itself is ignored for these purposes.[90]

Individual sources of data from a commercial actor that constitutes a database in its own right will be subject to database rights until such time as it is mixed with other sources of data to create a whole new database with its own rights, assuming that the mixing requires sufficient investment.[91]

3.3.3 Summary

The type of intellectual property law involved, and therefore the type of licensing or assignment appropriate, is context specific depending on the type of data used. Where such intellectual property rights apply it will be possible to transfer or license such rights. However, to do so, it will require the consent of the owner of the third party intellectual property rights.

3.4 Contractual obligations to third parties

Whilst individuals, unless they are employees or subject to commercial agreements, will be unlikely to have contractual obligations to third parties that would prevent them from providing their data, commercial or non-profit organisations might do so.

3.4.1 Commercial partners

The company will owe a contractual duty to its suppliers and stakeholders not to disclose their information or anything relating to the details of their relationship due to the information likely being disclosed in such a way that constitutes circumstances that import an obligation of confidence[92] (unless there is an agreement to the contrary). Therefore their consent would be required in order for the organisation to provide their data to the data trust.

Commercial agreements between suppliers and data providers will likely have express restrictions on the data provider sharing data as the information will likely be confidential. In the case of commercial agreements, any explicit prohibition against sharing data will need an explicit amendment to change the provision. Similarly with personal data, if sharing is possible without the consent of the third party and they became aware of the sharing at a later date, this would likely disrupt the commercial relationship and cause them to lose confidence in the organisation. For a commercial data provider to agree to the sharing of data there would either have to be restricted usage or for there to be a defined benefit for the supplier as well.

3.4.2 Individuals

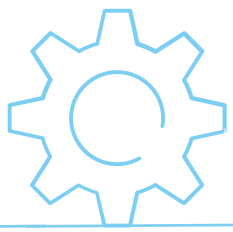
If the organisation wished to share information concerning their employee information, then this data would be subject to GDPR provisions, as referred to above, and their express consent to the use of their data would be required. Similarly customer data, if personal in nature, will be subject to the GDPR, so may require consent to be shared although this can be agreed to using the "tick box" method of consenting.[93]

Although not governed by a contractual relationship, a director would owe an equitable duty to the company and, by extension, its shareholders, to keep their information confidential (with shareholder information, if relating to individuals, being subject to the GDPR). A similar exercise would have to be carried out in ensuring there is a legal basis before any identifying shareholder information can be shared.

3.4.3 Summary

An organisation would have to ensure that any information shared does not breach a licensed use of any intellectual property right. To do so would impose liability on the transferring organisation. Additionally, data providers will have to assess their data before it is contributed to the data trust to ensure both that it retains any commercial confidentialities and that it complies with the provisions of the GDPR. If any of these are ignored, it could lead to claims from commercial partners or fines from the ICO, and would deter data providers from contributing their data to the data trust due to the potential risks involved. Data providers will also wish to ensure that when providing their data to the data trust, they are complying with relevant regulatory codes, guidance and restrictions on the use of data from public bodies. This is discussed in Section 4 and in the legal landscape review.[94]

[79] However, proposals are being considered for the European Directive on copyright in the Digital Single Market (2016/0280 (COD)) which will change this position once in force.
[80] s.1 Copyright, Designs and Patents Act 1988
[81] s.90(1) Copyright, Designs and Patents Act 1988
[82] s.90(3) Copyright, Designs and Patents Act 1988
[83] Crosstown Music Company 1 LLC v Rive Droite Music Ltd and others [2010] EWCA Civ 1222
[84] s.3A(1) Copyright, Designs and Patents Act 1988
[85] Oxford v Moss [1978] 10 WLUK 126
[86] Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281
[87] Which implemented into the law of England and Wales EU Directive 96/9/EC
[88] Article 16(1) Copyright and Rights in Databases Regulation 1997/3032
[89] Regulation 17 Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)
[90] British Horseracing Board Ltd and others v William Hill Organisation Ltd (Case C-203-02) [2004] ECR I-10415
[91] Forensic Telecommunications Services Ltd v West Yorkshire Police & Another [2011] EWHC 2892 (Ch), 9 November 2011
[92] Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31
[93] Recital 32 GDPR
[94] Legal landscape review (http://theodi.org/article/data-trusts-legal-landscape-review/).



Pinsent Masons

SECTION 4
Receiving data from the data trust

Section 4 is concerned with access to and use of data that is held in the data trust as administered by the data steward. This issue cannot, however, be considered in isolation.

As is made clear in Section 6, a data trust and the manner in which it functions will be defined by its stated purpose. This purpose will be a touchstone for determining, not only the data trust's legal structure and governance framework, but also the arrangements for the provision of data to the data trust and the terms under which prospective data users may gain access to that data. It is a given that the terms under which data users may access and use data must be consistent with the purpose for which the data trust has been established. In addition, on the basis that trust is earned rather than bestowed, the basis and terms under which data is made available must protect the interests of data providers, data users and any data subjects, as well as not exposing the data steward to undue risk.

By understanding the factors that will impact on the proposed data sharing arrangement and their significance, we can begin to explore whether or not a repeatable framework for data sharing can be established, which embodies the principles of sharing data in a "fair, safe and equitable way".[95] The form of that framework needs to be carefully considered. If the framework or the rules and underlying processes established to facilitate access to data are difficult to navigate (whether that be legally or operationally), do not represent an attractive prospect for data providers or data users, do not appropriately allocate risk, liability and accountability or are not transparent, then this will act as a barrier to the success of the data trust and the achievement of its overriding purpose. However, this barrier can be avoided if each participant in the data trust has a vested interest in making the data trust a success.

Examples of factors that will impact the terms of access and use of data include:

- the terms under which data has been provided, including any restrictions on use agreed by the data steward with a data provider and any other applicable obligations of confidentiality whether arising under common law or in contract;
- individual rights of data subjects;
- any rights of third parties including any intellectual property rights in the data;
- regulatory or other legal considerations, which may affect the scope of rights of access and use of the data, or the prospective user base including data protection, privacy law, State aid law and competition law;
- any particular sensitivities arising as a result of the identity of the data provider or the nature of the data;
- any conditions imposed on the data steward or a data provider by a third party funder of either the data trust or the work that has led to the creation of the relevant data;
- sensitivities arising from the potential for data to be used by "bad actors" for illegal or unethical purposes; and
- the financial / funding model for the data trust and the impact that may have on the terms under which data is made available.

In addition, each data trust will likely have factors unique to that data trust which will impact the terms for access and use of data. Factors may also vary in significance for different data trusts. Therefore, in considering whether it is possible to establish a repeatable framework for data trusts, we must recognise that a "one-size-fits-all" approach will likely not be appropriate.[96] That is certainly true when considering the factors mentioned above and, at the very least, the terms under which data is made available through the data trust must align with the terms under which such data was provided, on the basis that the rules for 'data out' need to correlate with those for 'data in'.

In designing an appropriate data sharing framework, we should also remember that where the data is personal data, data protection and privacy considerations will follow the data through the data trust; from the data provider to the data steward, and will impact the use of the data by a data user. These obligations may be present under the GDPR or under other data protection and privacy laws being developed in many other countries. The data trust will need requisite binding safeguards in place to ensure that it receives personal data lawfully, fairly and securely and that such personal data can subsequently be used by a data user.

4.1 Establishing the terms under which data may be made available

Property rights have long played a central role in the functioning of economic markets. However, data as an asset class is not owned and controlled like tangible property, or even other classes of intangible property, such as intellectual property rights. In fact, under English law, at least, the courts have not tended to regard data as something that can *per se* be owned at all.[97] As is noted in Section 3, intellectual property rights, whilst clearly relevant to the control and use of data, do not necessarily protect data as clearly and explicitly as, say, copyright in a novel or in computer software.

Therefore, we turn to contract and consider how access to and use of data can be regulated contractually; more specifically, we must determine the contractual terms under which the data steward is prepared and able to make data available to prospective users. In making that determination, it is a given that we shall consider at all times whether or not those terms remain consistent with the purpose for which the data trust has been established.

In considering the contractual terms that will govern access to and use of data, we can recognise the benefits in establishing a repeatable framework of data access, but must also acknowledge that, by necessity, the approach taken may vary depending on the facts and circumstances that apply in each case.

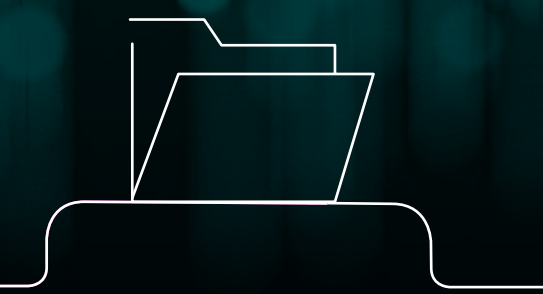
For example, in circumstances in which the data held is not particularly sensitive in nature and is not subject to significant regulatory or commercial constraints, a de-centralised model might be adopted. Data access and use under such a model may be governed by a relatively straightforward set of data access terms, which enable open access to data with minimal interaction between the data steward and the prospective data user who may access the data by subscribing electronically to the relevant terms.

By way of contrast, in circumstances in which the data is of a sensitive nature, say, sensitive commercial or personal data, or is subject to significant legal or other constraints, such as restrictive terms imposed on the data steward by data providers, then a more centralised model might be adopted. Under that model it may be that access to data is only available after the prospective user has been vetted and approved by the data steward. In this scenario, the contractual terms under which data may be accessed and used will likely be more prescriptive and restrictive in nature.

This can be illustrated by requirements imposed by the GDPR if personal data is being used by a data user, depending on whether it is acting as a 'controller'[98] or a 'processor'.[99] When a data steward shares, transmits or transfers personal data to a data user, it must determine whether the data user is processing the data as a 'controller' or as a 'processor'.

Where a data user is a 'processor', the GDPR mandates that certain contractual terms are in place covering a variety of obligations, including that the data will only be used on behalf of the controller based on prior written instructions. A data user / processor cannot use the data for its own purposes. The processor must also delete or return the data on demand.[100] Such a relationship would be unsatisfactory to most data users, who would want more control and to use the data for their own purposes. But, such an arrangement could allow for a data trust to engage a data user to undertake certain activities for the benefit of the data trust itself, or other users; for example, if the data trust were to engage the services of a cloud provider to assist with technical access to the data.

> The data trust will need requisite binding safeguards in place to ensure that it receives personal data lawfully, fairly and securely and that such personal data can subsequently be used by a data user.



[95] See Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 46-48, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

[96] The concept of a "one-size-fits-all" approach to data governance was considered in 'Data management and use: Governance in the 21st century a joint report by the British Academy and Royal Society', October 2017

[97] Oxford v Moss (1979) 68 Cr App Rep 183

[98] Article 4(7) GDPR 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[99] Article 4(8) GDPR 'processor' means a legal or natural, public authority, agency or other body which processes personal data on behalf of the controller.

[100] Article 28 GDPR.

It is more likely that the relationship of a data steward with a data user will be controller to controller; as the data user will have more control over the data, and use it for its own purposes (which are aligned to the data trust).

The data trust and the participants in it will need to decide whether the data steward, data users and the data providers will be independent controllers, each with their own individual responsibilities to data subjects or; act as joint controllers, where they jointly decide the purposes of the data processing. This determination will ultimately depend on how decisions are made about the data use, and who makes them. It is possible that within a given data trust, a combination of controller to controller relationships exist. Whatever the relationship between the data steward and the data users, the contractual arrangements will need to reflect the practical arrangements and detail which each participant is responsible for as well as the various obligations under the GDPR.

The examples given above envisage bilateral contractual relationships between the data steward and each of the data providers and the data users. There may also be circumstances in which data provision, data access and use and the role of the data steward in administering that use may be governed by a multi-party contract or code, which sets out the rights and obligations of all of the main participants in the data trust. An example of such an arrangement, although not a data trust per se, is the Smart Energy Code, which governs, amongst other things, the terms under which parties to that Code may obtain data generated by smart meters installed in UK households.[101]

In order to establish a contractual basis for making data available, it appears clear that one must consider all, or some at least, of the determinative factors referred to at the start of this Section.

4.1.1 The nature of the data

A logical starting point is to understand the nature of the data that will be held in the data trust. 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 the data has been provided or through the operation of law, that data is subject to restrictions on access or use that will need to be reflected in the design of the data trust and contractual terms under which data is made available to data users.

Certain data, due to its nature, may be subject to controls which need to be considered in setting up a framework for access and use of that data.

Certain data, due to its nature, may be subject to controls which need to be considered in setting up a framework for access and use of that data. These controls can take a variety of forms. For example, where the data is personal data, then in the UK its collection, use and disclosure will be subject to the GDPR and Data Protection Act 2018.

There are a number of aspects of data protection legislation which the data steward 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 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. Several lawful bases may be available for further processing, depending on the data source, categories of data, and most importantly the compatibility of the proposed use with the original use. These are factors which will have to be assessed by the data steward before giving access to a data user. A data trust should not limit itself to one legal basis 'by default' as this could unnecessarily curb data use and possible data users. The data trust should utilise all available 'tools' in the data protection and privacy 'tool box' to optimise use of the data by data users.

The nature of the data may also mean its use is controlled by other applicable laws (whether those laws are in existence now or are introduced during the operation of the data trust). Examples in the UK include the law of confidence which protects information of a confidential nature[102], the Health Service (Control of Patient Information) Regulations 2002 and the Human Fertilisation and Embryology (Disclosure of Information for Research Purposes) Regulations 2010 which protects types of patient data. Where competitively useful information is exchanged, the Competition Act 1998 may require access to data to be subject to certain limitations or confidentiality requirements. We explore the competition law considerations regarding use of data briefly in Section 4.4 and in more detail in Annex A.

It should be borne in mind that, even in circumstances in which a data trust is established in the UK, data provided to the data trust or the use of that data may be subject to laws and regulations which are applicable outside of the UK, particularly where the data held by the data trust originates from another jurisdiction, or if the data steward sends or permits use of the data by a data user in another jurisdiction.

Data that is sensitive in nature may also be controlled by policies or codes which limit or restrict its use. For example, in the UK, government information or information originating from government agencies may be subject to the UK Government's Security Classifications Policy.[103] There may be sector-specific industry codes or regulatory requirements. For example, smart meter consumption data, as well as being regarded as personal data and subject to the GDPR and UK data protection law, is also subject to industry specific restrictions on collection and use including under the Smart Energy Code[104], which, apart from use by energy companies for the fulfilment of certain specified regulatory and industry specific purposes (for example billing customers and balancing the grid) gives consumers control over the purposes to which their consumption data is used.

In addition to any duty of confidence that may arise under the common law, the use of data which is commercially sensitive may also be controlled by contract.[105] It is common business practice for such data to be subject to restrictions on use contained in a non-disclosure agreement or confidentiality obligations contained in a commercial contract. For example, if data was collected as part of a research project funded by a third party, the funder's terms and conditions may restrict how that data can be used, who it can be shared with and where it can be sent. A data steward will be mindful of the damage that may be caused if data it receives is subject to such restrictions and subsequent use by a data user constitutes a breach of those restrictions.

Section 3 of the report identifies certain intellectual property 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 to use any such data must be consistent with those rights and with the terms of any corresponding licence granted 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[106], the licence terms may require, at least, that the data provider be attributed in any subsequent re-use of the data.

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 if it is possible that it may be used by "bad actors" for illegal or unethical purposes. This is partly a question of good governance and Section 6 deals with that aspect by advocating the establishment of an ethics committee where appropriate.[107] However, in these circumstances, the data steward may also consider it good practice to vet potential data users, through an 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.

At the outset then, a data steward must consider whether or not it is necessary or appropriate for contractual and technical restrictions to be applied to access the data held within the data trust. As part of that consideration, a data steward will reflect on whether or not the purpose of the data trust can be fulfilled if those restrictions are applied. In assessing this, the data steward will consider the effect that any restrictions (or indeed a lack of restrictions) may have on prospective participants and their willingness to participate in the data trust.[108] In this respect, a balance needs to be achieved between, on the one hand, meeting the purpose of the data trust 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 use of data as a core principle.

In practice, achieving this balance may be difficult. As we explain in Section 6, some of the benefits to be realised from using data may not be known at the time the data trust and its purpose are established or at the time data is supplied. Therefore, whilst we must, of course, recognise 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[109], we must also not lose sight of the inherent risk that establishing onerous access and data use requirements may undermine the ability of the data trust to fulfil its purpose and deliver the benefits anticipated on its establishment.

[101] https://smartenergycodecompany.co.uk/
[102] The law of confidence and its potential impact on the ability of a data trust to use data is explored in Section 2.
[103] https://www.gov.uk/government/collections/government-security
[104] https://smartenergycodecompany.co.uk/
[105] Section 3 explores this issue in more detail.
[106] https://creativecommons.org/about/program-areas/open-data/
[107] See Section 6 for further detail on governance structures and ethics committee
[108] 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."
[109] In the UK, the Data Protection Act 2018 and the General Data Protection Regulation (EU/2016/679).

This need for data governance 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 a data trust expands, the potential for that data to generate unexpected patterns and insights will also grow. Therefore we advocate open access to data, whenever possible, and for the rules established for the data trust to be flexible enough to allow extensions to how data can be used within transparent parameters.

Whilst recognising the importance of establishing a data governance framework which is open and capable of adapting to meet emerging requirements and potential benefits, there will be circumstances when restrictions need to be applied to who may access data and how they can use data.

4.1.2 The nature of the data steward

Another factor in determining who will have access to data is the identity of the data steward. If a data steward is a corporate entity (say, a subsidiary company) established by a public sector body, transparency laws may require it to provide data 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). This will be the case under the UK Freedom of Information Act 2000 or the Environmental Information Regulations 2004. If data 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 would need to be aware of this additional method of disclosure. This may need to be considered in the set up of a data trust; for example, whether the data steward will hold the data 'on behalf of the data provider' to avoid it being caught by transparency laws. Disclosure under transparency laws is often deemed as a disclosure to the world at large, irrespective of the motive of a requester, and the risk that "bad actors" may try to gain access to data through this channel should not be overlooked.

4.1.3 The nature of the data provider

Issues arising in connection with the provision of data are addressed in detail in Section 3. However, in considering the basis on which data may be made available for use, a responsible data steward will also consider the nature and identity of the data providers.

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 and privacy). Applicable regulation may dictate that data should not be disclosed publicly or made available for particular purposes without the adoption of appropriate safeguards that, amongst 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 terms under which it is made available.

Taking the UK financial services sector as an example, in 2018 the Chairman of the Financial Conduct Authority emphasised the importance of consumers having absolute clarity over how their data is used and the need to develop rules, or a data charter, explaining such use to customers rather than imposing rules on customers via terms and conditions.[110] Therefore, for financial services organisations to provide consumer data to a data trust it would be crucial that they (and their consumers) understand what data is being used and for what restricted purpose. The technical and operational solution to be adopted for the data trust would need to be such that information was capable of being tracked and reported. The terms and conditions under which that data is made available would need to align with any restricted purpose and limit data usage accordingly.

As another example, in the healthcare sector, use of patient data in the UK is regulated by legislation and a number of codes of practice. For patient data to be made available for use in a data trust, compliance with that legislation and those codes would be required. A recent report has highlighted the potential benefits to be gained for patients, the NHS and society if patient data is made available for analysis through the use of data-driven technologies.[111] The report called for robust processes for evaluation, regulation and oversight where patient data is to be used. The report also noted the importance of achieving a balance between protecting data privacy and ensuring that any framework is not unnecessarily risk averse thus impacting on the ability to realise potential benefits. A good example of an approach which enables such data access, whilst safeguarding the interests of data subjects, is the Data Safe Haven operated by NHS Scotland.[112] The Data Safe Haven provides a platform for the use of NHS electronic data in research feasibility, delivery and pharmacovigilance. The interests of data subjects are safeguarded by, amongst other things, a Safe Haven Charter[113] which sets out the standards and principles with which participants must abide.

4.1.4 The nature of the data user

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. Take, by way of example, data relating to the density of an endangered species in certain geographical areas. That data may be used by conservationists for the purposes of taking positive steps to increase the population of that endangered species in those areas. Equally, in the hands of a "bad actor" that data could be used for the purposes of poaching or other detrimental ends.[114]

The question thus arises, what steps can a data steward take to ensure that data is used in an ethical way and in a manner which is consistent with the purpose of the data trust and the premise under which the data providers made that data available?

At the least, a prudent data steward will consider the risk of data being used for unethical purposes. If a risk exists, it should consider how technically, 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 registration process, which enables a data steward 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.

Beyond the identity of a data user, the territory in which a data user is based may also have implications for the data steward. If a prospective data user is based in a country which is subject to sanctions or export control restrictions, then, depending on the nature of the data, it may not be appropriate to allow access to data to a prospective data user in that territory.

Equally, from a data protection perspective, if data held by the data trust based in the European Economic Area (EEA) contains personal data, then restrictions will need to be satisfied if the data user is located outside of the EEA. Depending on where data users are located, the data trust 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.[115] One option under the GDPR that could be explored is Binding Corporate Rules; which is a global legally binding transfer mechanism allowing data to flow freely between a group of undertakings or enterprises engaged in joint economic activity. As Binding Corporate Rules must be approved by the data protection regulators, they are comprehensive and demonstrate a high level of protection for data subjects. Whether they would be appropriate, however, would very much depend on the structure of the data trust and the relationship between the data trust and data users.

Unless a data trust is set up with restricted jurisdictional scope that confines the data to locations where there are compatible data protection protections, it will have to be flexible and consider the most appropriate transfer mechanism as and when the need arises. This will be an additional administrative and financial burden on the data trust, which should be considered during its formation. While the restriction on cross-border data transfers is a feature of the GDPR, other countries are developing their data protection regimes and some are adopting similar restrictions. This development could not only impair the data trust receiving data from data providers but also impair the data trust giving access to data users.

In addition, competition law considerations may have consequences for a data trust in a number of ways. One determining factor for whether a competition law issue does arise will be the identity of the data providers and the data users.

> The terms and conditions under which that data is made available would need to align with any restricted purpose and limit data usage accordingly.

[110] https://www.fca.org.uk/news/speeches/how-can-we-ensure-big-data-does-not-make-us-prisoners-technology
[111] 'Our data-driven future in healthcare' report, 29 November 2018 by the Academy of Medical Sciences
[112] https://www.nhsresearchscotland.org.uk/research-in-scotland/data/safe-havens-2
[113] https://www.gov.scot/publications/charter-safe-havens-scotland-handling-unconsented-data-national-health-service-patient-records-support-research-statistics/pages/4/
[114] See Wildlife pilot report for more on this example
[115] Articles 44 to 49 GDPR.

4.1.5 The nature of the financial and funding model

A data trust needs to be "affordable and sustainable".[116] 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.

In considering the basis on which data held by a data trust may be accessed, consideration will need to be given to whether a fee will be levied for access to data (and if so what that fee will be) or whether data 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 (if any) adopted.

Whether a fee should be levied is a matter intrinsically linked to the wider question of how the data trust in general will be funded. This includes how the technical solution for data sharing to be used by the data trust will be financed. One matter cannot be considered without the other. If the establishment of a data trust and its on-going operation is funded by a third party, say, a government agency or a financial institution or commercial partner, 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.

Of course, there are existing use cases of organisations making data freely available to third parties to promote innovation and economic benefit. An example of this is Transport for London's (TFL) initiative of making transport data freely available to third parties to promote the development of new products, apps and services for its customers. The guiding principle adopted by TFL regarding access to its data is that it will make non-personal data available free of charge unless there is a commercial, technical or legal reason not to.[117] This has resulted in a number of benefits including the development of over 600 apps relating to TFL services.

However, in the context of a data trust, we expect the data accessed to originate from third party data providers, rather than data originating from the data steward 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 account for the 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 the data trust will be frustrated.

Public sector considerations regarding the financial model

Not only private sector bodies need to consider the opportunity or value cost arising through the provision of data at no or minimal cost. The House of Commons Select Committee[118] has noted the importance of public sector bodies considering the value of their data and the possibility that products and services created using that data may, in turn, be sold back into the public sector on a commercial basis. In its report, the House of Commons Select Committee also referred to Research Councils UK having argued that, subject to legal, ethical and commercial restraints, all publicly funded research data is "a public good and should be made available with as few restrictions as possible".[119]

This can also be seen through the re-use of public sector information rules[120] which require data produced by a public body as part of their 'public task' to be available to third parties to be republished or used to produce a new product or resource, often by combining it with other information. It does not apply to data by a public body if someone else holds the intellectual property rights. The public body can only permit re-use if it holds the intellectual property rights in the information. The re-use regime has a number of rules, including exemptions, regarding how requests are dealt with and licences for the re-use of the 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.

Structuring the financial model

If it is decided that a fee will be charged for access to data a number of other matters need to be considered.

The matters that need to be considered when deciding if a fee will be charged include:

- how will the fee be calculated and by whom? Presumably by the data steward through the governance arrangements established for the data trust. We know that often data has little value in its own right but that when it is analysed or combined with other data its value can increase. The difficulty in attributing value to data was recognised in a report by the British Academy and Royal Society in October 2017 which referred to new approaches being required to assessing the financial value of datasets;[121]
- will it be a fixed fee or will the fee 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 the fee be a one off fee or a recurring fee?;
- 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 the fee be paid operationally and will the data steward have the operational processes in place to support this?; 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, if it is decided that a fee will be payable by data users for access to data this will need to be addressed in the contractual documentation that is put in place to govern access to data.

4.2 Documenting the terms under which data will be made available

Once a data steward has considered the relevant issues identified under Section 4.1, it will be possible to write documents that will form the contractual basis under which data users can access data held by the data trust. The content and complexity of those documents will be determined by the considerations identified in Section 4.1.

If the data held 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 a simple and permissive contractual model comparable to the Creative Commons licensing regime might be adopted, enabling ease of access to data on a decentralised basis through the acceptance electronically of specified data user terms. This access model may be easily scalable and repeatable at low cost with other data trusts that have similar hallmarks.

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 a more bespoke and, inevitably, complex contractual model will be required that addresses risks and issues identified by the data steward and that is more restrictive in nature. This contractual model may sit within a more centralised data trust construct.

Inevitably, in the spectrum between these two extremes contractual models of varying colours and hues may arise. However, whatever contractual model is adopted, we would expect that there will be a number of common features to the terms under which data is made available to data users.

[116] Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017) 46-48, https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk
[117] http://content.tfl.gov.uk/deloitte-report-tfl-open-data.pdf
[118] House of Lords Select Committee Report, Artificial Intelligence Committee, 'AI in the UK: ready, willing and able?' Published 16 April 2017 - HL Paper 10
[119] Ibid
[120] Re-use of Public Sector Information Regulations 2015 (SI 2015 No. 1415) which implement European Directive 2013/37/EU.
[121] 'Data management and use: Governance in the 21st century' a joint report by the British Academy and Royal Society, October 2017 and comments of Professor Jim Norton, Fellow of the UK Royal Academy of Engineering

4.2.1 Common features of data user contracts

There will be certain common features of data user contracts.

Common features of data user contracts include:

- criteria for becoming a data user including any technical requirements;
- process for forming the contract;
- scope of use;
- specific restrictions on data use purposes;
- financial terms (if any);
- grant of licence;
- freedom of information (if applicable);
- technical standards and requirements;
- attribution to data provider and data trust;
- audit rights;
- governance and dispute resolution (including linkage, if appropriate, with data trust governance model);
- personal data protection particulars (including security, data breach reporting obligations, international transfers, on-ward transfers, use of processors, data subjects rights and schedule of particulars)
- warranties and liability (including protection for data steward);
- process for changing the data access terms;
- duration, termination and return of data; and
- governing law.

The data steward will also need to establish the process through which the data access contract will be formed. At the most basic level that may be a subscription process under which a data user will enter into a data access contract with the data steward by accepting standard access terms on the data trust website. At the other end of the spectrum, it may be possible for the data steward, through its governance model, to establish a multi-party contractual arrangement akin to a code, which governs the provision and use of data and to which the data steward, all data providers and all data users subscribe.

As a rule, we would not anticipate that the terms under which the data steward enables access to data will be negotiable. There are good reasons for this, not least the benefit of a standard approach across data users and the need to ensure data access terms are consistent with the terms and conditions under which data is provided.

Consideration will need to be given to the process through which changes to the standard data access terms are agreed. We would expect that this process would interact with the governance arrangements established for the operation of the data trust – for example, a panel might be established to consider proposed changes to the terms under which data is made available. In the case of the Smart Energy Code (a multi-party contract), a panel has been formed to consider changes proposed by parties to the Code.[122] We expect that the data access framework and approach to dealing with change needs to be sufficiently flexible to take account of changes in the nature or volume of the data held by the data trust and the purposes to which that data may be put.

4.3 Technical considerations

Any restrictions to be applied to access to data need to be capable of being implemented technically. Technical considerations regarding how data is provided, stored and accessed need to form part of the overall design of the data trust and will drive what type of technical solution is needed for the data trust. That technical solution, and associated operating processes, needs to be economically viable, sustainable and scalable. Any technical and operational barriers could prevent the aims of the data trust being achieved.

For reasons identified in this Section, it is possible that in certain cases restrictions will need to be applied to access to data. It may also be the case that data use is tracked in some way. If different restrictions are to apply to how data can be used, there will be a need for data segregation to be implemented technically. In addition, where data use needs to be tracked, the technical solution adopted for the data trust will need to be capable of supporting this. Upfront assessment will be required to understand whether these requirements can be achieved both technically and operationally.

Similar consideration will also be needed in respect of the process for providing and accessing data. Processes will need to be straightforward and practical for data providers and data users alike and the data available must be usable otherwise participation in the data trust will be detrimentally affected. Examples of potential technical barriers include incompatible data formats; the language the data is in; the volume of data; how easy the data is to interpret on a standalone basis or whether it requires access to metadata or other materials to interpret; and interoperability issues regarding the systems used by the data provider, data trust and data users.

A House of Lords Select Committee[123] noted that data format is a live issue and a significant barrier to opening up data access, within the public sector in particular. One of the most significant challenges for the data trust may indeed be establishing a common set of technical criteria that data providers and data users alike can satisfy and that enable the efficient provision and use of data. If access and use of data is subject to applicable technical considerations and standards, then this will need to be addressed in the contractual terms under which data is made available.

In considering how data will be supplied to data users, it will be important to consider the access model for data and whether access will be a controlled access model (with access controlled by the data steward or a third party) or an open access model (with data being available via APIs, data feeds, downloadable format or other format). The former (centralised) model will likely be more appropriate for circumstances in which data is of a sensitive nature or is capable of being misused. The latter (de-centralised) model is more consistent with a true open data model in which open access is granted on a (largely) universal basis with minimal restrictions and legal or technical barriers to use.

It will also be important to consider the role, if any, the data steward should or may need to play in authorising or facilitating access to data and how quickly data users may need access to data. How quickly data is needed will inevitably vary on a case by case basis depending upon the purpose of the data trust and how the data users intend to use the data. A data trust needs to be capable of adapting to meet these needs. If it cannot, data providers and data users will be dis-incentivised from participating.

4.4 Competition law and State aid

If a data trust is to achieve its aims restrictions must be placed both on data providers and, most saliently, on data users. Those restrictions will mainly be for the benefit of the wider social interest of the data trust, but may sometimes be designed to protect the interests of data providers or data users.

All restrictions of this kind have the potential to limit competition in the market, and may thus face challenges from competition law. In particular, competition authorities are focusing heavily on the use of big data and its potential to be used for anti-competitive means. For example, the use of self-learning pricing algorithms, which have access to large quantities of information, could result in anti-competitive results even without the knowledge of the parties. Such theories are on the forefront of competition law enforcement policy.[124]

Competition law is too complex for detailed examination here, but it is an issue which will need to be considered when devising rules for data sharing and re-use in data trusts.

A different kind of competition problem arises where public bodies participate in data trusts. Under the European Union rules it is unlawful for State bodies to provide assistance to entities carrying out economic activity where this would distort fair competition. This assistance is called State aid, and the rules barring it are enforced by the European Commission and national courts. As with competition law, the rules are too complex and extensive for examination here, but they also need to be considered where public bodies participate in data trusts. Annex A sets out a more detailed analysis of some of the key issues that may arise under both competition law and State aid rules.

[122] https://smartenergycodecompany.co.uk/about-sec-change/
[123] House of Lords Select Committee Report, Artificial Intelligence Committee, 'AI in the UK: ready, willing and able?' Published 16 April 2017 - HL Paper 10
[124] In 2018, the UK competition authority invested in its own specialist data analytics team to ensure it stays ahead in the fields of data engineering, machine learning and artificial intelligence techniques.

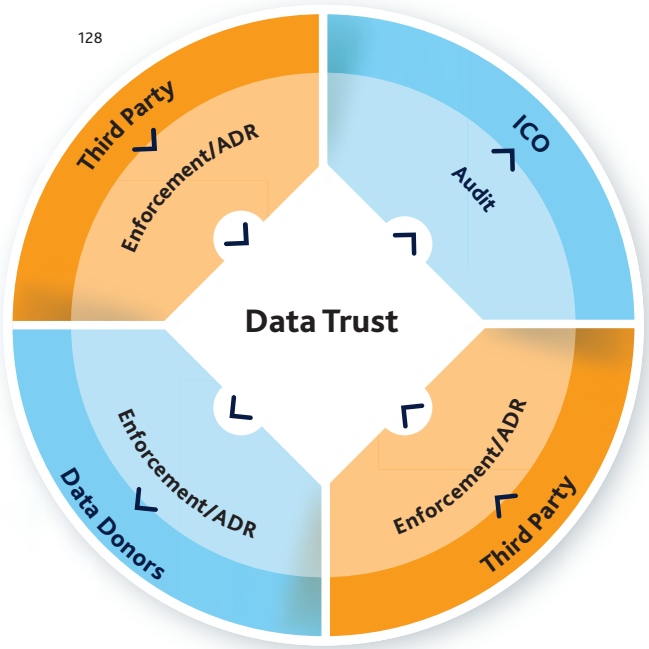
> One of the most significant challenges for the data trust may indeed be establishing a common set of technical criteria that data providers and data users alike can satisfy and that enable the efficient provision and use of data.

SECTION 5
Ensuring compliance with the trust rules

Essential to the integrity of a data trust are the ability of data providers, and the functionality of the data trust itself, to ensure that there is strict compliance with the prescribed objectives of the data trust. There are two relevant considerations. First, data providers and other stakeholders such as owners of intellectual property rights, must feel confident that their data will not be misused by the data trust. Thus, data providers must have confidence in the method of redress against the data trust to ensure it is complying with the given purpose for which data providers consented that their data could be used. Also, the data trust must have a method by which it can enforce breaches by the data users (and possibly other third parties who have access to the data), but are using that access for a purpose that falls outside of the remit permitted by the data trust. This could be achieved either through the internal mechanisms of the data trust itself or through some hypothetical organisation or individual that provides independent third party oversight.

It is important for a data trust to ensure that there is both a method of redress against individuals in breach both for data users who obtain data directly from the data trust and therefore are in some form of agreement with the data trust, and indirect data users who obtain data from the data trust without the direct agreement of the data trust itself. This could encompass employees of data users or third parties who have accessed the data without consent or illicitly, or even organisations to which a data user who has received data from data trust then passes that data on, without ensuring that the recipient is bound by the data trust rules. Enforcement by direct data users will be the most straightforward as any breach can be enforced under whatever form the agreement takes, whilst enforcement of a breach by a data re-user, where there is no overt agreement in place, will need to be carried out under rights granted under legislation and common law principles. If a data provider is in breach of its obligations under the license, which is a less likely scenario as they are providing data to the data trust, then either the data trust can enforce the breach under the terms of the license or a data user could enforce under any data trust rules.

It should be noted that, as mentioned above, data is not considered a material asset therefore is not capable of theft.[125] This means that any "theft" of data, or breach of data trust rules cannot be penalised through criminal sanctions for the crime of theft. An equal principle applies to "theft" of database information as a whole.[126] It is possible to be convicted of gaining unlawful access to a computer (i.e. via phishing or hacking) but this stands apart from the actual theft of any data.[127]



5.1 Enforcement

5.1.1 Enforcement against the data trust

If the data provider is an individual and the data trust has breached its obligations under the data trust rules an individual could enforce under the terms of the agreement by which it provided its data to the data trust, much in the same way as a commercial organisation might (see below). If individual data providers have agreed to the data trust rules upon providing their data, then any breach of these rules by another party that causes a loss to the aggrieved party, can be enforced under this agreement.[129] The normal position, under the doctrine of privity of contract, is that anyone who is not party to the agreement cannot enforce a breach of it. Depending on the construction of the agreement however, the contract can also grant rights (and therefore a method of enforcement), to a named person or group of people who are not party to the contract.[130]

5.1.2 Enforcement under the GDPR

Such direct enforcement is generally applicable to enforcement against direct data users. For enforcement against indirect data users, breaches can be enforced under rights granted under legislation or common law principles. Depending on the breach this could be data protection laws, competition laws or breach of confidence to name a few. Otherwise the data provider could enforce legislatively using provisions contained within the GDPR. Each EU member state appoints its own supervising authority that operates this function[131], of which the UK's is the Information Commissioner's Office ("ICO").[132] Additionally, beyond any penalties that the ICO can impose under the GDPR, an aggrieved individual can also use breach of the GDPR as a cause of private action against the data trust.[133]

The ICO has powers to investigate, correct, authorise and advise organisations.[134] Under these powers the ICO can impose a fine of up to 20 million euros or 4 per cent of annual turnover (whichever is higher).[135] If a data subject wishes to be itself compensated however, it would need to pursue the matter by bringing a claim through the courts[136], which is an expensive and lengthy process. Additionally, if the data trust can show that it complied with its GDPR obligations[137], for example by having suitable preventative or technical measures in place, then a claim for compensation could be unsuccessful (although this is not always the case).[138] Also, a data subject would need to show material or non-material damage (such as distress) as a result of the breach.[139] It should also be noted that under the GDPR, a data subject has a right to request that its data is removed from the data trust[140], restrict use of its data[141] and it has a right to object to the use of its personal data.[142]

A commercial organisation however could not enforce under the GDPR as it is not an identifiable living individual. Thus data about the organisation cannot be personal data (although data about its employees, directors or shareholders would be).[143] Rather they would either have to pursue a court claim for breach of confidentiality or for an order enforcing compliance with the terms of any agreement for the licensed use of data.

5.1.3 Enforcement under breach of confidential information

To claim under breach of confidential information, the aggrieved data provider would first need to show the information was confidential (by the data having the "necessary quality of confidence and being disclosed in circumstances imparting an obligation of confidence")[144] and that it was disclosed to unauthorised recipients or used for an unauthorised purpose.[145] Remedies are an injunction to prevent the use of data[146] or to have the data deleted[147], a damages payment[148] or an account of profits[149]. This would similarly involve a court claim being brought unless settled prior to this being necessary.

[125] Oxford v Moss [1978] 68 Cr App Rep 183
[126] Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281
[127] Sections 1-3 Computer Misuse Act 1990
[128] It should be noted that the ICO will not necessarily be the organisation to provide independent, third-party oversight as the ICO's general focus is probably too narrow to cover all aspects of compliance. Additionally being a UK government organisation it might not be appropriate to oversee transnational data trusts and commercial organisations could possibly resent a public body overseeing compliance with data trust rules
[129] Clarke v Dunraven [1897] AC 59
[130] The Contracts (Rights of Third Parties) Act 1999
[131] Article 53(2) GDPR
[132] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
[133] Article 82 GDPR
[134] GDPR Article 58
[135] Data Protection Act 2018 section 155 to 159 and Schedule 16
[136] Article 79(2) GDPR
[137] Article 82(2) GDPR
[138] https://www.lawgazette.co.uk/law/court-of-appeal-upholds-surprising-morrisons-data-leak-ruling/5068043.article
[139] Article 82 GDPR
[140] Article 17 GDPR
[141] Article 18 GDPR
[142] Article 21 GDPR
[143] Article 4(1) GDPR
[144] Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31
[145] Seager v Copydex Ltd [1967] 2 All ER 415
[146] Penwell Publishing (UK) Ltd v Ornstein [2007] EWHC 1570 (QB)
[147] Arthur J Gallagher (UK) Ltd and others v Skriptchenko and others [2016] EWHC 603 (QB)
[148] Universal Thermosensors Ltd v Hibben [1992] 1 WLR 840
[149] Seager v Copydex (No 2) [1969] 1 WLR

5.1.4 Breach of license and shareholder claims

A mechanism in the terms and conditions can be included either as the basis under which to bring a claim through the normal court process for breach of the licence, or else to provide a mechanism of alternative dispute resolution (see below). This could be applicable to both commercial organisations or individuals and might present the most expedient and cost effective method of redress and the one that would likely instil the most faith in stakeholders as disputes could be resolved internally and without the involvement of the courts. These methods are generally faster and cheaper as they bypass the normal court process, and all the time, and therefore expense, that involves, in favour of more collaborative streamlined processes. Generally they are also less adversarial and therefore support resolving decisions where it is important to maintain a continuing relationship. In the context of a data trust this would be where continued sharing of data is desired once the dispute has been resolved.

If the corporate model is followed for a data trust, for example if the data trust takes the form of a CIC, then the "shareholders" can bring a derivative claim against the company for it acting outside its power or fraudulently. This is a higher threshold under which to claim, and would relate more to a more systemic abuse by the company rather than on a case-by-case basis.[150] As an extra layer of protection, the shareholders of the data trust could have a shareholders agreement, which is a document dictating the relationship between shareholders and can be enforced under standard methods for breach of contract (i.e. a court claim). The issue here is that, as a contractual document that shareholders have to sign to be party to it, a new version would have to be re-signed every time there is a new shareholder if they are to enjoy the same protections as all of the other shareholders. This could be administratively tricky if new data providers were being added to the data trust with any kind of frequency.

5.1.5 Enforcement by the data trust

The data trust will also wish to prevent third parties such as indirect data users (referred to above) accessing the data trust information and using it for a restricted purpose beyond what the data trust prescribes, and for which its data providers have consented. Data providers would be able to bring court claims against third parties in breach, under the same claims of breach of confidentiality (so long as the third party was aware that the data was confidential)[151] or, where personal data is involved, the GDPR[152] regulations referred to in the previous section.

Any licensing agreement would be between the data trust and the third party. Therefore any data provider would not have standing under which to bring a claim; although evidently the data trust could enforce the licence terms against a third party in breach. Strict, specific provisions in the licensed terms of use for third parties using data will need to be in place in order to allow data trusts to monitor and control access to the data. To instil confidence on the part of the data providers a unilateral right to cancel a third party's access to data will likely also need to be in place. This could, however, cause logistical difficulties, especially if the data has already been used for a specified purpose.

A data trust may[153] also be able to use, as a cause of action, database rights, if there is a global extraction of data from the data trust database beyond specific pieces of information. These can either be under breach of copyright[154] or under breach of the Database Regulations.[155] Evidently as with the other causes of action referred to, the data trust would have to seek to enforce these rights through standard litigation procedure.

5.2 Audit

The ideal for data trusts, their data providers and stakeholders, rather than wait until an issue arises and enforcement becomes necessary, is to ensure strict measures are in place to carefully manage the data within the data trust's care.

If the corporate model of data trust is followed, then it will be subject to audits of their annual accounts in the same way as any other company.[156] In relation to a data trust however there should also be an audit to ensure that data is being stored and managed in an appropriate manner. This is already recommended by the ICO to ensure compliance with the GDPR, the Freedom of Information Act 2000 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.[157]

If the data trust is holding personal data then it will need to comply with any audits conducted by the ICO, although it should, as a matter of good practice, also have its own provisions in place to carry out its own regular data audits. The audit will aim to ensure that legislative requirements are followed, that data is kept for no longer than is necessary for the stated purpose[158] and that the use of the data does not fall outside of the scope for which it was provided.[159]

The ICO itself will conduct data audits to check compliance with the legislation referred to above and an executive summary and comprehensive report are prepared subsequently. Audits can either be consensually arranged or compulsorily depending on circumstances and the level of engagement of the data trust.[160] Audits generally do not set out to bring enforcement action against organisations as a result of their audits, however auditors do have a discretionary power to impose fixed monetary penalties on organisations for breaches of £1,000[161], which can either cover all breaches or be cumulative for multiple breaches.[162] This is in addition to the ICO being able to pursue traditional enforcement action for breach of the legislation.

If it were a hypothetical independent, third-party organisation that provided the oversight/audit function, then the data trust would have to comply with the data trust rules regarding this, which would ensure the ethical and fair sharing of data and data security for all participants. If this is not a public body then the powers given to the auditing body to ensure compliance would be under a contractual arrangement, or else voluntary acceptance by the data trust of any breaches and subsequent corrective action, something that a data trust that is in fault is unlikely to acquiesce to.

To ensure compliance on behalf of the data trust, appointing a data processing officer will be key. This will provide a person to continuously oversee the operation of the handling of data within the data trust. If, due to the size of the particular data trust, a dedicated individual is not appropriate, an external individual can be appointed to fulfil such an auditor type role.

[150] Part 11 of the Companies Act 2006 and Foss v Harbottle [1843] 2 Hare 461
[151] Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31
[152] Article 82 GDPR
[153] Under British Horseracing Board Ltd and others v William Hill Organisation Ltd (Case C-203-02) [2004] ECR I-10415, the data trust can only claim these rights if there has been a "substantial investment" in the compilation of the data into the data trust database
[154] Forensic Telecommunications Services Ltd v Chief Constable of West Yorkshire.
[155] Regulation 16(1) Copyright and Rights in Databases Regulations 1997 (SI 1997/3032)
[156] s.394 of the Companies Act 2006
[157] https://ico.org.uk/for-organisations/resources-and-support/audits/
[158] Article 5(1)(e) GDPR
[159] Article 5(1)(b) GDPR
[160] https://ico.org.uk/media/about-the-ico/documents/2258653/summary-of-best-practice-audits-research-report-161017.pdf
[161] https://ico.org.uk/for-organisations/guide-to-eidas/enforcement/
[162] https://ico.org.uk/media/2784/guide-to-ico-pecr-audits.pdf

To ensure compliance on behalf of the data trust, appointing a data processing officer will be key.

5.3 Alternative dispute resolution

As referred to previously, enforcement via litigation in court is an expensive, time-consuming and, by its nature, contentious process. This is traditionally recognised in law and there are mechanisms for a number of alternative dispute resolution methods enshrined in various concepts of law. Due to the assumed nature of a data trust as an organisation which lends itself the characteristics of trustworthiness and openness, a less contentious and more pragmatic version of dispute resolution might be beneficial (although evidently with third party "bad actors" who are unwilling to engage, or flagrant in their breach of the rules, traditional enforcement might be better).

The following are the potential options for alternative dispute resolution for a data trust:

- **negotiation**: discussion without the assistance of a third party;
- **mediation**: a neutral third party is used to facilitate an agreement;
- **med-arb**: ("mediation-arbitration") if mediation fails then parties agree that mediators role becomes that of an arbitrator who issues a binding opinion;
- **executive tribunal**: ("mini-trial") "executives" from both parties and an independent chairperson hear submissions from each side, the chairperson will not make a binding determination unless parties direct that he should;
- **conciliation**: similar to mediation except the third party takes a more active role in settling the dispute;
- **early neutral evaluation**: independent person gives a non-binding opinion;
- **expert determination**: expert produces a contractually binding determination to the parties
- **adjudication**: third party adjudicator provides binding decisions on disputes as they arise during the course of a contract;
- **dispute review board**: panel of (typically three) neutral persons appointed at the outset before any issues, provide periodic determinations to disputes by interim binding decision (decisions can be challenged by arbitration or litigation); and
- **arbitration**: independent, mutually appointed arbitrator appointed who gives a binding verdict.

These methods are comprehensive. However, few will be appropriate for the data trust model. Options 1-6 are non-binding and therefore, as it less likely that the party in breach is automatically going to admit fault, is less effective as a universal form of dispute resolution that could be applicable to all data trusts. Options 7 and 8 are more appropriate with regards to technical disputes and option 10 tends to be used for significant disputes due to the cost involved and its similarity to the litigation process.[163]

Option 9, dispute review boards ("DRB"), are ordinarily seen under construction contracts and exist for the length of a particular project.[164] These are put in place by contractual arrangement and governed by the International Chamber of Commerce Board Rules.[165] The model however could equally be applicable to disputes arising out of a data trust if similar DRB provisions were to be put into the terms of use for the providing or licensing of data. The DRB model allows three or more independent third parties to be appointed, for example at the outset of creation of the data trust. They can attempt to mediate a solution between the parties but can ultimately make an interim-binding decision on the parties. This is contractually binding on the parties, however it can be disputed through normal arbitration or litigation procedures if the party at fault believes the determination to have been made in error.

The DRB model has the advantages of: **i)** mediation in that conciliation is attempted to be made; **ii)** arbitration in that the decision is binding (albeit only contractually); and **iii)** yet it also has a backstop of being able to make a challenge by arbitration or litigation if the relevant party wholeheartedly believes the award was made in error. DRBs are also cheaper to appoint and more straightforward to follow than a litigation process and, if appropriately independent and knowledgeable about data trusts, will likely have a greater vote of confidence from the public who arguably have an entrenched distrust of lawyers and the legal system.

[163] Arbitration Act 1996
[164] https://iccwbo.org/media-wall/news-speeches/new-icc-dispute-board-rules-emphasizing-dispute-avoidance-enter-into-force-on-1-october/
[165] https://iccwbo.org/dispute-resolution-services/dispute-boards/

Pinsent Masons

SECTION 6
Governance structure and operations

It is no accident that the term "data trust" is that most commonly adopted, when talking of data-sharing arrangements that contain some degree of autonomy. This is not because of any supposed affinity between a data trust and a legal trust, as that concept is currently understood under English law, but because trust – in its plain English sense – is critical to the proper functioning of any such arrangement.

A typical dictionary definition of "trust" holds that it is "a firm belief that someone or something is reliable, true, or able to do something" – and its corollary, "trustworthiness", is defined as "the ability to be relied on as honest or truthful". The less able we are to trust in any data-sharing arrangement – to do basic things, such as to protect our data or to use it only for an agreed set of purposes – the less comfortable we will be, to provide data in the first place. A sense of trustworthiness is, therefore, 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, 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 and, as is stated in the Decision-Making Report[166], the way in which a data trust makes decisions is crucial to its legitimacy. We track stakeholder representation in more detail in Section 6.2 below.

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 within a governance framework, interested parties will, in certain circumstances, inevitably need access to other external forms of redress and enforcement.[167] These are dealt with in more detail in Section 5. As the Decision-Making Report states, a data trust's legitimacy will derive not only from how it makes decisions - and the governance that underpins this - but also on striking a balance between accountability and effectiveness.

6.1 Governance structures

As we saw in Section 2, a number of legal forms are potentially capable of housing a data trust. In this Section, we do not presuppose any choice of legal form, but seek instead to identify those functional elements that we believe to be critical to the proper functioning of a data trust, and that can be applied irrespective of legal structure (although, admittedly, some creativity may be required in this respect if certain forms are adopted).
Nor do we deal here with the 'ownership' of a data trust. We might think that a data trust owned and run by Google should be treated differently to one that is owned and run by a government - but then again, maybe not.[168] Generally speaking, the fate of an organisation may be determined by its owners. The question here is not who those owners are, but rather, what robust structures need to be in place to underpin the efficient operation of a data trust and ultimately, the data trust's "trustworthiness", thereby maximising the likelihood of stakeholder engagement and the chances of the data trust fulfilling the purpose for which it was established.

6.1.1 Open Data Institute definition

This project's working definition of a data trust is "a legal structure that provides independent stewardship of data".

There are a couple of elements here, each of which is intended to engender trustworthiness and which will need to be considered in the context of a governance structure; namely:

- independence; and
- stewardship.

What does "independence" mean in this context? Should the data trust be independent of its owners? Should it be independent of data providers, data users and all its other stakeholders? Given that a data trust will require engagement from stakeholders in order to function; this would seem an odd assertion. In our view, a more compelling interpretation of "independence" in this context is that, rather than being wholly excluded from a data trust's direction or decision-making, no one set of stakeholders should be able to dominate or dictate a data trust's direction or decision-making.
A further element of independence might be a commitment to respect the wider interests of the data trust's community of stakeholders, by making governance decisions which respect individual rights and interests rather than deciding purely on a majoritarian basis. The term "stewardship" implies the taking care of something that belongs to someone else. For present purposes, we are interpreting this to mean that while a data trust will not seek to benefit from the use of the data to which it provides access, it is not prevented from benefitting (and potentially profiting) from its role as a steward of that data.

Finding the optimal governance structure for a data trust will involve finding a balance between the various stakeholders. As Bob Garratt has pointed out, the word "governance" derives from the ancient Greek word *kubernetes*, which has two meanings: firstly, the giving of direction and secondly, the giving of rapid feedback as to

the effectiveness of that direction.[169] If a data trust's governance is insufficient to generate a sense of trustworthiness stakeholders will simply not engage, and non-engagement is both immediate and definitive feedback.

The Decision-Making Report breaks down the decision-making process for data trusts into four stages: formulation, design, operation and evaluation (including, potentially, the closure of the data trust). The governance model will be designed in the course of the first two of these phases and, following implementation, will govern the functioning of the data trust in the course of its operation and evaluation phases. It is likely that any governance model will be subject to refinement in the course of a data trust's operation, but the way in which such refinements may be made, should itself, form a part of the initial governance model. This is discussed in more detail in Section 6.1.3.

For the purposes of this Section, we use the term "stakeholders" to mean those persons or organisations whose interests are potentially affected by the use of the data held under the data trust, or to which the data trust is able to grant access; for example a data provider, a data subject or a data user. Conversely, we use the term "participant" to refer to a subset of stakeholders: those data providers and data users who are actually engaged with the data trust; that is, who are providing data to or using data provided by, the data trust.[170] It is conceivable that some persons or organisations might fall into both categories, such as a data provider who owns intellectual property rights in the data provided.

6.1.2 Purpose and rules

Any data trust should begin with a clear statement of its purpose.
This will be the case, whether a data trust is envisaged either as a profit-making body or a not-for profit organisation. We have, in recent times, seen increasing demand from customers, consumers and employees, for brands to stand for more than the simple making of profits. To this end, private sector companies have been looking beyond their traditional shareholder horizons, in an attempt to articulate what they stand for. Those companies that have succeeded in doing this have registered not only positive public sentiment, but also increased growth rates.

There is a lesson to be learned here. Not only will a compelling statement of purpose engender trust amongst stakeholders, but it will provide the ultimate measure against which governance bodies and stakeholders alike can check periodically, to ensure that the data trust remains true to its purpose. As stated in the Decision-Making Report, moreover, an agreed purpose is one of the key elements on which an effective decision-making process will need to rest.

[166] Decision making report (http://theodi.org/article/data-trusts-decision-making-report/http://theodi.org/article/data-trusts-legal-landscape-review/).
[167] There is a substantial theoretical literature which suggests that trust has two fundamental bases: an emotional trust, based on an existing relationship or reputation (strong and semi-strong trust); and a calculative trust, based on the likelihood that another can be forced or incentivized to do what they ought to do (weak trust). For a useful overview see Elias L. Khalil (ed.), Trust (Edward Elgar, 2003).The role of governance is primarily to foster weak trust, by providing rules and enforcement mechanisms for those rules, but it can also foster semi-strong trust by helping establish a reputation that an organisation is trustworthy.
[168] This is not to ignore the fact that a public sector data trust may be subject to restrictions that would not apply to a private sector data trust, such as those imposed by virtue of statutory powers or treaty obligations.
[169] Bob Garratt, The Fish Rots from the Head (Profile Books 2010).
[170] It should be noted, however, that stakeholder classes are not necessarily, mutually exclusive. It may well be the case that a data provider will also be a data user (and vice versa) and indeed, a data subject (that is, an individual whose personal data forms part of the underlying data to which the data trust provides access) may be both a data provider and a data user.

Beneath (and underpinning) a data trust's purpose, will sit its rules. These will set out in more detail, the way in which the data trust 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 the operations of the data trust, 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 the basic operations of the data trust; 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 values or principles, such as the data trust's independence. Other examples might include the five data access 'control dimensions' commonly referred to as the "Five Safes"[171] or, in the context of personal data, the core principles contained in Article 5 of the GDPR.

The rules should bind the data trust and all participants in the data trust. 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 the operational agreements that we describe below, for example, a data provision agreement or data use agreement.

In addition to the basic operations described above, the rules should cover:

- the technical architecture of the data trust (for example whether the data will be decentralised and retained by data providers – with the data trust, consequently, performing more of an oversight role – or whether the data will be stored centrally by the data trust itself or in the cloud) and the consequent role the data trust will play in the storage and processing of relevant data;
- interoperability between the data trust 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 the data trust 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 the data trust;
- the obligations of each participant and the data trust (such as the extent (if any) to which the data trust is expected to engage in any form of monitoring or audit of data use, particularly in respect of any personal data);
- information security;
- any applicable service levels; and
- any significant departures from the data trust's standard form data provision agreements and data use agreements.

Depending upon the nature of the data trust and the sector within which it operates, there may be a number of other areas which the rules should also cover. By way of example, these might include compliance with any statutory requirements, sector-specific regulation and the ethical basis on which the data trust will operate. Rules could also cover issues of accountability and liability, although these might sit more comfortably in the relevant operational agreement(s) (see below).

6.1.3 The status of the purpose and rules

Hand in hand with any discussion of the content of a data trust's purpose and rules, go the issues of:

- who is entitled to establish the purpose and rules and subsequently, to make any changes to them;
- the basis on which such persons are entitled to make any such changes;
- the process that must be followed in order to make any such changes; and
- how any disputes as to the content or interpretation of the purpose and rules will be resolved.

Clearly, any data provider will want to know up-front, the purposes for which such data may be used. Past experience has shown us, however, that we might not yet know the answer to this. Data can be used in a variety of ways and it is not unusual for data to prove to have a value that was not immediately foreseeable, at the time that it was collected. We would not want to preclude some genuinely valuable use of the relevant data simply by virtue of adopting a governance model that is too rigid to allow this to happen. For these reasons, among others, the data trust's rules would need to cover the above points in a clear and transparent manner, so as to reassure stakeholders as to the steps that would need to be taken, before any development or extension of a data trust's purpose or rules could be adopted.

The purpose and rules will be of varying importance and it is logical, therefore, that the varying of some would require greater formality than others. By way of analogy, in general, a private limited company in the UK must pass a special resolution (requiring the approval of the holders of 75 per cent or more of the shares voted) for any amendment to its constitution while only an ordinary resolution (requiring the approval of the holders of a simple majority of the shares voted) is required to appoint or remove a director. Similarly, we would expect a change to a data trust's purpose or a key rule, to have to meet a higher threshold of stakeholder engagement than, say, a change to a time limit or other procedural matter.

At the end of this Section, we set out a potential governance structure for a data trust which comprises a hierarchy of governance bodies. The governance structure will ultimately be driven by the individual dynamics of the relevant data trust and, critically, by the attitudes of the relevant stakeholders. In particular, stakeholders should be consulted to ensure that any proposed governance structure is sufficient to underpin the trustworthiness that a data trust will require in order to function.

The Decision-Making Report points out that the adjudication of competing interests which any data trust will likely need to undertake, is a complex trade-off that can only be solved on a case-by-case basis. This will inevitably limit the extent to which any decision-making process can be truly standardised or made repeatable.

6.1.4 Documentation

There are several methods by which the purpose and rules of a data trust may be set out and applied. These can vary from soft obligations (for example informal agreement on ways of working) to hard obligations (for example contractually enforceable obligations where failure to comply may result in some form of liability). In general, the more material the obligation, the better suited it will be, to be a legally enforceable obligation. Again, by way of analogy, a company's articles of association comprise a legally binding contract as between a company and each of its members. Similarly, a data trust's purpose and its key rules should be capable of being enforced by its participants.

Depending on the context of a particular data trust and its aims, it may be that, rather than any one participant being able to enforce a particular governance obligation, the agreement of a minimum number of participants would be required, before such an obligation might be enforced.

Depending upon the nature of the vehicle, the purpose and rules could be enshrined in a number of different documents:

- **stakeholder agreement** or **membership agreement**. A data trust might require participants to enter into a membership agreement. This might involve the payment of a subscription fee and establish the purpose and certain of the data trust's rules, as legal obligations which might be enforceable by participants individually, or by a minimum number of participants;
- **articles of association** (in the case of a company). As stated above, a company's articles comprise a binding contract between a company and each of its members (i.e. its owners) and its articles are not, therefore, necessarily analogous to a data trust's rules, as we are distinguishing ownership from governance in this context; and
- **ancillary documents**. These may or may not be legally enforceable and could include internal policies (such as in respect of competition and whistle-blowing) and guidance notes.

One approach to the terms on which the data trust contracts with its data providers and data users, would be to codify those terms into a multi-party contract. This approach would have the benefit of transparency while minimising the scope for individually negotiated deals.

We have seen something similar to this in the context of patent pools. Patent pools are agreements between two or more patent owners to license one or more of their patents to one another or to third parties. The pools are often associated with complex technologies that require complementary patents in order to provide efficient technical solutions. In a patent pool, patent rights are aggregated amongst multiple patent holders.

[171] The "Five Safes" comprise: safe projects, safe people, safe data, safe settings and safe outputs. See further, Ritchie: "The 'Five Safes': a framework for planning, designing and evaluating data access solutions".

> 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.

Pinsent Masons

Then, the pooled patents are made available to member and non-member licensees and typically the pool allocates a portion of the licensing fees it collects to each member in proportion to each patent's value.

It is worth noting in this context, that if a patented technology becomes part of a standard (for example 4G or IEEE 802.11) and it is mandatory to implement that particular feature, such patents are considered standard essential patents (SEPs). The trade off to your technology being included in the standard is that the holder of a SEP must license on fair, reasonable and non-discriminatory (FRAND) terms.

By analogy, a company holding a large quantity of data might acquire a dominant market position that is arguably comparable to that of a SEP holder. Some datasets may be critical – for example, data generated by a transport provider in a smart city context. The holder of data might abuse this position either by refusing to grant access to this data or by granting access only selectively or under onerous conditions. One answer to this could be the imposition of a FRAND licensing obligation on data providers to ensure equal treatment. If a "data pool" is generally open for third parties to join, the FRAND obligation would provide for equal non-discriminatory treatment of all participants.

An alternative approach would be to deal with the terms on which a data trust contracts, by way of separate operating agreements. In this case, the extent to which a data trust might depart from its standard terms and conditions, absent some form of stakeholder consent, could usefully be set out within the rules.

On the basis of this approach, we would envisage the data trust entering into the following contracts with participants that would be enforceable by those participants against the data trust and vice versa:

- **data provision agreements** (under which a participant provides data to the data trust); and
- **data use agreement**s (under which the data trust provides a participant with access to data for certain pre-agreed purposes).

Amongst other things, these agreements could cover data quality and format. In the case of a data provision agreement, the data provider would be expected to warrant that the data provided is legally provided and may be used for the ongoing purposes of the data trust and its data users. They would also need to set out clearly, each party's role in the context of data protection (for example whether a party is a data controller or processor for the purposes of the GDPR).

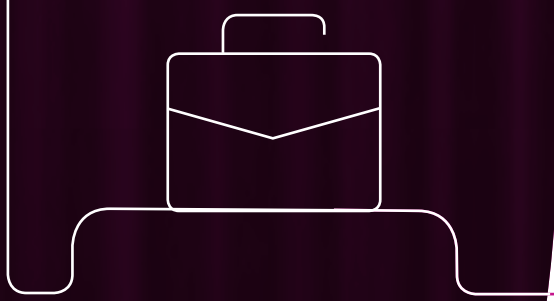
A final point to note is that there will be certain overarching legal principles which will apply to a data trust and with which its governance organs will wish to ensure compliance; not least because a failure to do so will undermine its trustworthiness. These will include rights and obligations relating to intellectual property, confidentiality and data protection.

6.1.5 Liability flows

In the context of participant relationships, liability flows will need to be considered carefully. This is particularly important if personal data is to be included in the data trust, as the GDPR provides for joint and several liability in respect of compensation, as well as the possibility of fines for infringements.

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

> Any data trust should begin with a clear statement of its purpose.



That said, as the data trust 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 a data trust will be wholly able to escape responsibility for decision-making, or liability to a regulator or data subjects.

A data trust, as a steward of personal data, will also have responsibilities under the GDPR. For example, a data subject might make a subject access request to the data trust in respect of the personal data it holds, or seek to exercise other rights over that data, such as erasure.

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 data trust in certain circumstances) will help to improve a data trust's risk profile, a data trust will not simply be able to shift all potential liabilities onto a data provider or a data user. We have recently seen examples of regulators seeking to fine organisations in a data chain for their own failings[172] and, as a matter of public policy, it is questionable whether a contractual indemnity will be effective in respect of a regulatory fine.

The data use and data provision agreements will also need to deal with other regulatory action, such as enforcement notices, which could lead to a data provider being instructed to cease processing personal data, which has already been provided to the data trust.

6.2 Representation of stakeholders

The precise list of a data trust's stakeholders will depend upon the nature of the data trust.

The list of a data trust's stakeholders might include:

- data providers (which may include data subjects);
- data users (again, which may include data subjects);
- the data trust itself, as the steward of data;
- owners (to the extent a data trust has separate legal personality); and
- third parties (i.e. those parties not 'within' the data trust and therefore not bound by the rules of the data trust), such as:
  - the general public who, for example, may benefit from the use of the data;
  - data subjects whose personal data will be in the data trust; and
  - regulatory and other industry bodies.

In analysing the representation that these groups of stakeholders might require in the context of a data trust, it is useful to look first, at some of their likely motivations and concerns, and knowledge of data use (in particular, its use for advanced analytics or AI) or other relevant subject matter expertise.

6.2.1 Data providers

Data providers will vary in nature but will likely only be comfortable providing data if they know such data will be:

- used ethically, lawfully, in accordance with agreed rules or principles and for the stated purpose of the data trust; and
- stored safely and securely and disposed of appropriately (or retained in accordance with an agreed retention policy) upon cessation of the right to use that data[173], or of the trust itself (see Section 7).

As stated above, we envisage that a data provider will have the benefit of rights arising under a data provision agreement; that is, the arrangement pursuant to which they contribute data to the data trust. These rights will, if the data steward has legal personality, be against the data trust, as the steward of the relevant data. Otherwise, these rights will lie against such of the stakeholders as may have been agreed in any agreement constituting the data trust.

In the course of interviews conducted in connection with the various data trust pilots, a number of potential data providers referred to the attractiveness of rights of veto over potential data users. As the Decision-Making Report points out, however, a data trust will need to balance accountability and effectiveness, and rights of veto of this nature may hinder its ability to operate.

One potential sanction that a data provider might seek to employ in the event of breach or misuse of its data, is the removal of its data from the data trust. From an operational perspective, however, this is likely to be problematic, both for the data trust and also the data users. The data trust's dataset might be significantly devalued by the withdrawal of a significant data provider. Data users, some of whom may have incurred significant expenditure in connection with the ongoing or proposed interrogation of the dataset, may be materially disadvantaged by such a withdrawal. For this reason, it is likely that a data trust will look for a minimum time commitment for the use of the data, or a minimum notice period from a data provider, before which it may not withdraw its data from the data trust. We deal with withdrawal and its potential impact on ongoing projects and derived data, in more detail in Section 7.

We note, for the sake of completeness, that data subjects will have rights against the data providers who contribute their data to the data trust (see further, Section 5). Data subjects will also, as stated above, have rights against the data trust (as the steward of the data) and the data users. These rights sit outside this analysis.

[172] https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/ (accessed 28 February 2019) for details of enforcement actions taken against different data controllers and data processors for infringement of data protection legislation.

[173] The terms on which a data provider will be willing to provide data will vary, depending on the circumstances. Some providers may be willing to provide data only for a specific project and would therefore require that all rights to use that data would cease upon completion of the relevant project.

Pinsent Masons

6.2.2 Data users

Data users, also, will vary in nature, but will want to know that:

- data access will be granted on the basis of clear and transparent principles and terms and conditions (as mentioned in Section 6.1, there may be an argument for considering the application of a regime similar to that which requires the licensing of SEPs on a FRAND basis);
- any data (in particular personal data) can be lawfully used for the data user's intended processing purpose(s);
- the quality and volume of data held within the data trust will be sufficient to merit potentially costly analysis (and be capable of supporting potentially critical decisions) which may, for example, include consideration of data bias; and
- any analysis on the data carried out by the data trust itself, and made available to users, will be reliable and fairly reflect the data provided by the data providers.

6.2.3 Data trust

To the extent a data trust has legal personality, various additional issues will need to be addressed.

A data trust may want (along with its executive management) the ability to:

- facilitate the achieving of its purpose;
- decide upon the entry of a new participant as data provider or data user;
- oversee compliance by its participants with its rules;
- hold participants accountable and enforce compliance with its rules;
- if a profit-making entity, to make and apply or distribute its profits; and
- move value from the data trust to the data trust owner(s), whether by dividend or otherwise.

6.2.4 Owners

The degree to which owners are likely to require some form of representation within a data trust will depend upon the form of legal structure adopted. By way of example, a significant shareholder in a profit-making enterprise will likely expect a greater degree of representation than, say, a member of a company limited by guarantee, any profits of which are applied to further the company's purpose.

In general terms, the owners of a company are, collectively, able to determine the fate of that company. As discussed above in Section 6.1.1, however, we do not believe that any one set of stakeholders should be able to dominate or dictate a data trust's direction or decision-making. Were one set of stakeholders to be dominant, this would likely have a negative effect upon the willingness of other stakeholders to engage with the data trust.

While we do not believe that the model of a privately-owned and profit-making enterprise is necessarily incompatible with this project's working definition of a data trust, we are conscious of the views expressed by interviewees on the various data pilots, on the importance of a data trust's independence (although, to a degree, "independence" meant different things to different people). In light of this and as discussed in Section 6.1.1, we believe that a robust and effective governance structure will be the key to achieving a balance between stakeholders, and engendering trust in the data trust.

6.2.5 Third parties

The degree to which third party representation in a data trust will be appropriate, will depend upon the nature of the data trust and, in particular, the data trust's need to engender trust among stakeholders. In the context of a data trust which contains or provides access to a significant amount of personal data, for example, it may well be prudent to grant the data subjects, whose personal data forms the underlying subject matter of the data trust, some form of representation within the data trust. This is discussed further in Section 6.2.6 below.

In the course of interviews conducted in connection with the various data trust pilots, a number of potential data providers referred to the attractiveness of rights of veto over potential data users.

6.2.6 Representation

Data providers and data users will likely require that safeguards along the lines of those set out above, be incorporated into the functioning of the data trust. These could be incorporated into the data trust's rules and, if thought desirable, entrenched in a variety of ways. By way of example, any change to the basis on which access is granted might first require the prior consent of the data users. An alternative model might require a prior consultation with all participants and a representative of data subjects (if any) whose data is being processed by the data trust.

The method by which any consent could be given, might take any one of a variety of forms, depending upon the governance structure adopted. We set out at the end of this Section, a potential governance structure.

By way of example, consent in these circumstances (i.e. to change the basis on which access to data is granted) might be given by:

- a simple or enhanced majority vote of all data users (in person or in writing);
- a unanimous or majority vote of a representative committee of data users;
- a unanimous or majority vote of a data access committee, comprising representatives of data users, data providers and data subjects (if applicable); or
- the formal approval by a "data user director" or "data subject director" (if applicable), who sits on the main governance organ of the data trust.

The approval mechanism would be set out in the rules and any change to that mechanism would, itself, be protected in a similar manner. As stated above, the more material the matter in question, the greater the degree of formality the approval is likely to require.

Data subjects, even if not direct participants in the data trust, could also be granted access to the decision-making process by virtue of representation on the data trust's main governance organ or some form of advisory committee.[174] This could be in the form of individuals or, potentially, by way of some form of privacy or consumer protection organisation.

There will also likely be a need for subject matter experts who are versed in, for example, data collection and processing.

There is no (at least not yet) "market standard" for the level of representation participants might enjoy and in the final analysis, the key driver for this will be the desire to engender trustworthiness which will in turn drive stakeholder engagement.

The Decision-Making Report points out that a data trust's 'social licence to operate' must be earned rather than assumed, and proposes the use of a deliberative decision-making process, as a means of maximising engagement among stakeholders (see further, Section 6.3).

It is worth noting that the directors of a company in England or Wales are subject to a duty to promote the success of that company "for the benefit of its members as a whole".[175] "Members", in the case of a company limited by shares, means a company's shareholders. Clearly, there is a tension here, between this duty, which, as a matter of law, will be owed by the directors to the company and its shareholders (or creditors, if the company is insolvent) on the one hand, and the promotion of the rights of the data trust's stakeholders and participants, on the other. To the extent, however, that the purposes of a company as set out in its constitution, consist of or include purposes other than the benefit of its members, the directors are required to act with a view to achieving those purposes.[176] For this reason, it may be worth entrenching within the data trust's articles, some form of additional duty on the data trust's directors, such as an obligation to take into account the interests of the data trust's participants alongside the interests of the data trust.

6.3 Achieving legitimacy

As stated above, in designing the form of a data trust, it will be critical to take into account the attitudes of the relevant stakeholders.

The Decision-Making Report proposes a deliberative decision-making process as one means of achieving legitimacy among stakeholders. The key aspect of a deliberative decision-making process is that the participants' own input forms the basis of the results and findings, thus increasing the perceived legitimacy of the process.

We should also not lose sight of the fact that it is not only current providers and users of data that the data trust will want to attract, but also future users and providers of data, together with data subjects whose data might be placed under the governance of the data trust.

The key drivers for achieving a strong governance structure to engender trustworthiness are:

- a compelling and persuasive statement of purpose;
- a clear and transparent set of rules on the basis of which the data trust will operate;
- reassurance that data will be kept securely and only be dealt with in accordance with agreed principles;
- a clean and transparent decision-making process that balances and protects the interests of the various stakeholders; and
- engagement with those stakeholders in the design of that governance structure.

[174] cf. Genomics England's Participant Panel which advises the Board and to which a certain number of seats are reserved on various committees. See also e.g. Tim Clement-Jones's comments in the House of Lords Select Committee Report, "AI in the UK: Ready

[175] Section 172(1) of the Companies Act 2006.

[176] Section 172(2) of the Companies Act 2006.

The data trust and its representatives will need to be accountable to the data trust's stakeholders. This accountability can take a number of forms, but will inevitably involve legal rights and obligations in respect of key elements. These rights and obligations might be capable of being enforced by individual data providers or data users or, in certain cases, acting through representatives appointed to the board or committees of the data trust. If personal data is held by the data trust, data subjects will also likely have a direct right of action against the data trust.

As we mentioned above, a withdrawal of significant data from a data trust may impact negatively upon both a data trust and its data users. For this reason, we believe some form of minimum commitment will be desirable from data providers to ensure the stability of the underlying dataset.

One final point to note here is that data subjects (i.e. any individuals whose data may form part of the data trust's dataset), will need to feel comfortable that their data is adequately protected and that it is being used appropriately. This will be the case whether or not it is the data subjects themselves who have provided their data to the data trust. To the extent the data subjects are unhappy, the less likely it is that data providers will be willing to provide their data to the data trust. To this end, the data trust should establish a standard of best practice in respect of data protection and privacy rights. This should be publicly available and the subject of periodic audits to check compliance.

An interesting comparison can be made between data trusts, as described in this report, and trust ports. Trust ports are independent statutory bodies within the UK that are governed by their own legislation and run by independent boards who manage the assets of the trust (i.e. the port) for the benefit of stakeholders.[177] While the board of a trust port is expected to make decisions on a commercial basis, it is also entitled to recognise the local community as one of the trust port's stakeholders and consequently, at least in part, it can be said to be managing the port for the benefit of the local community. Trusts ports differ from the data trusts we have considered here in that they are creatures of statute which are designed to hold local monopoly rights. That said, it is interesting that trust ports may, should market conditions so dictate and notwithstanding their broad stakeholder base, choose to diversify into areas such as leisure.[178] A parallel can be drawn here, between this flexibility and the circumstances in which a data trust might be entitled to amend its purpose and rules (see further, Section 6.1.3 above). In both cases, stakeholder engagement will be one of the key means of achieving legitimacy, in the eyes of stakeholders.

6.4 External oversight

One further method of achieving legitimacy is through regulatory oversight. In particular, in the fintech space, we have seen a number of new entrants fare better in the market once a regulatory framework has been established within which they are able to operate.

The obvious issue for a prospective data trust, is that there is no regulator which is, at present, capable of taking an oversight role, other than in respect of its direct responsibilities. Such a regulator, were it to exist, could act as a proxy for the public interest and potentially assist in engendering public confidence in data trusts in general.

Nor is there any statutory framework for data trusts and their stakeholders. There is no doctrine, by way of example, whereby a data trust meeting certain standards would be exempt from certain liabilities because we, as a society, acknowledge the good that can come from the increased sharing of and access to data.

There is no core structure, recognised by statute, with accepted rights and obligations as between a data trust and its stakeholders, which could be easily adopted as a starting point for any new data trust.

What we have been looking at here, therefore, is a potential template that would have to be reproduced and tailored to the specifics of any data trust. It will have to be agreed, in each case, as between the data trust and its stakeholders and a significant amount of market testing may be required before any solution is capable of being adopted.

The need to create bespoke arrangements will inevitably lead to delays in achieving some of the benefits of which we have spoken in this report and increase costs.[179] It will also leave open, moreover, the risk that some data trusts may adopt governance models that are not as robust as they should be and consequently damaging the public confidence in data trusts, as a whole.

We have recently, however, seen the advent of monitoring bodies which have been established to monitor compliance with personal data protection codes of conduct in the cloud computing space. These codes have been designed for business-to-business use and are helpful in demonstrating compliance with the GDPR. They have not been prescribed by regulatory authorities, but have instead been drawn up by industry players to assist with the GDPR compliance. Similarly, here, a code might be one way to demonstrate that a data trust, along with its providers and users of data, will behave

[177] See, for example, "Modern Trust Ports for Scotland – Guidance for Good Governance", published by Transport Scotland in November 2012.
[178] Ibid, page 5.
[179] This concern was expressed in Wendy Hall & Jérôme Pesenti, Growing the artificial intelligence industry in the UK (UK DCMS and BEIS October 2017), https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk
[180] An example of this is the UK government's ability to share personal data across organisational boundaries to improve public services, pursuant to various Codes of Practice established pursuant to the Digital Economy Act 2017. Another example is Publicly Available Specification (PAS) 183, drawn up by the bsi with a view to establishing a decision-making framework for sharing data in the context of smart cities.
[181] Other examples of frameworks and contractual relationships, etc. in this regard include SVRDT, Ocean Protocol Foundation, Social Economy Data Lab, Safe Havens, Genomics England, SAGE Bionetworks, UK CRIS, JISC, HESA, DAWEX, Datapitch, Smart DCC, TeX and Truata.

in accordance with a public set of core principles. As is the case in the cloud computing space, an independent monitoring body would be able to monitor compliance in return for the payment of some form of subscription fee, potentially on a sector by sector basis. Some form of accreditation for such bodies (similar to ICO's accreditation of the monitoring bodies referred to above) would further strengthen the public perception of such bodies' independence.

Increasingly, we are seeing codes of practice, guides and frameworks, being drawn up and implemented, with a view to enabling the wide-ranging benefits that can arise from the appropriate and regulatory compliant, sharing of data. The fact that we are seeing this across a number of different sectors[180], suggests that we may be seeing the first steps towards a common framework for data sharing, although these steps are still being taken on an ad hoc basis.[181]

Two potential basic governance structures for a data trust

Figure 1

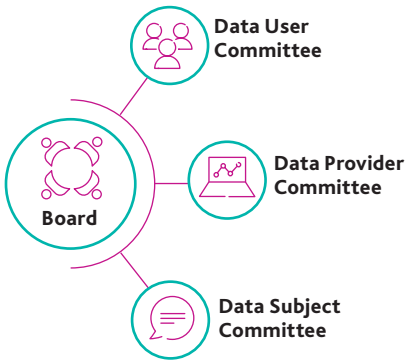
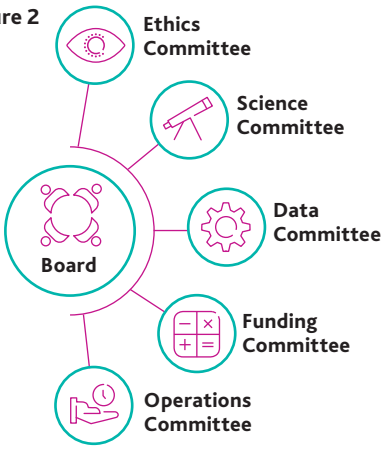


Figure 2



In Figure 1, three advisory committees report to the board; one committee for each of the basic participant groups of the data trust and one for those data subjects whose data forms part of the underlying data to which the data trust is entitled to provide access. In Figure 2, however, various subject-specific advisory committees report to the board, each of which might comprise representatives from each of the data trust's participant groups. The suggested roles of the board and advisory committees are set out below.

> Data subjects, even if not direct participants in the data trust, could also be granted access to the decision-making process by virtue of representation on the data trust's main governance organ or some form of advisory committee.

A. Board

Role

Within the context of a data trust's purpose, the board manages and is responsible for setting the overall strategy of the data trust. It may delegate certain of its responsibilities to executive management and/or one or more committees. Depending upon the vehicle that is chosen to house the data trust, the members of the board may owe fiduciary duties, to act in the interests of that vehicle.

Membership

A board may be wholly non-executive or consist of a mix of executive management and non-executive members. The non-executive board members should have the ability to outvote the executive management members (if any) on any contested decisions. Non-executives may be appointed either for their expertise and/or independence, or as representatives of stakeholders. Advisory committees may, potentially, be entitled to appoint one or more representatives to the board. The bottom line here is that the membership of the board will need to be sufficient to underpin the legitimacy of the data trust, as a whole.

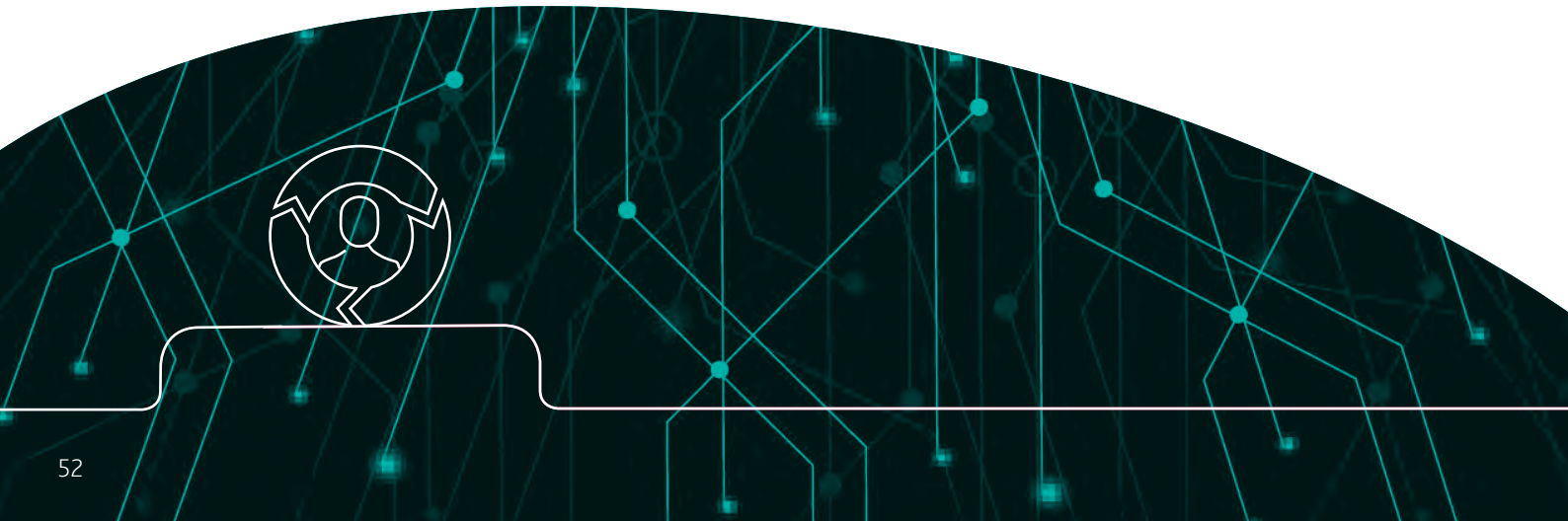
Who appoints board members?

In the context of a typical private company, it is generally the owners (shareholders) who have the ultimate say on who is appointed to a board. In the case of a data trust, however, while there may be a case for the owners to have a say in appointing the board, bearing in mind the need for the data trust to engender trustworthiness and seek engagement from stakeholders, it will likely make sense to broaden this to encompass representatives from each of the stakeholder groups; namely, data providers, data users and, potentially, data subjects. To the extent a consensus will need to be forged for the making of key decisions, a clear dispute resolution process will need to be agreed upfront in the event of a deadlock or inability to make those decisions.

What decisions can the board make?

As mentioned above, we would expect a greater degree of formality to attach to some decisions than to others. While the board would bear the ultimate responsibility for the data trust's strategy, it might be required to consult its advisory committees – for example, the data provider committee, on decisions of particular relevance to the data provider community. Depending upon the materiality of the matter, this might amount to no more than an obligation to consult, but in certain circumstances, it might require the board to obtain the prior consent of the relevant advisory committee.

It should also be noted that the board's discretion in the setting and implementation of the data trust's strategy, should always be within the context of a data trust's purpose. The board should not be entitled to amend or extend the data trust's purpose, without the consent of the data trust's stakeholders. By analogy, an action that would require a special resolution of shareholders in the context of a private company, might here require a positive vote of a data trust's participants. The formal requirements for such a vote, would be set out in the rules of the data trust.



B. Executive management

Role

It is not a given that a data trust would have an executive management, however, if it does, the executive management would be responsible for the day-to-day operations of the data trust and would report directly to the board.

Who appoints executive management?

The board would be responsible for appointing and dismissing the senior executive management (for example the chief executive and finance director) and setting their remuneration. The senior executive management would then be entitled to appoint other members of the executive management. If thought desirable, certain appointments could be reserved to certain participant groups.

What decisions can executive management make?

Executive management would be entitled to take decisions in respect of the operation of the data trust, to the extent such decisions are not reserved to the board or would require the approval or consultation with, any participant groups or advisory committees.

C. Advisory committees

Role

The number and nature of any advisory committees that report to the board, will depend upon the nature of the individual data trust, itself. Figures 1 and 2, above, show two different possible models for this. In both cases, a key question will be the degree to which any such committees must be consulted and indeed, whether a positive vote of a committee may be required, before the board is able to decide upon a particular course of action.

Membership

The membership of a committee will depend upon its subject matter. In a committee of data users, for example, a data trust will likely want to ensure that a potentially diverse user base is adequately represented, potentially through some form of proportionate representation. In a science committee, however, the expertise of the relevant individuals will likely be of more importance, so as to ensure that the data trust is able to benefit from expert views from across a range of different disciplines within which it operates.

Who appoints advisory committee members?

Again, the answer to this question will depend upon the nature of the advisory committee. Members could be appointed by a mix of the board and stakeholder representatives. Once again, the data trust will be seeking engagement from stakeholders and adequate representation on committees is one way of facilitating this.

What decisions can advisory committees make?

Again, this will depend on the nature of the committee. As mentioned above, however, a key issue will be whether the committee is advisory, or whether it will have the ability to veto or consent to various courses of action.

To the extent advisory committees are representative in nature (i.e. representing categories of stakeholder rather than, say, holding particular expertise), an advisory function is likely to be more suitable than a delegation of board authority, as one of the key functions of the board of a data trust, will be to balance the interests of the various stakeholders.

Pinsent Masons

SECTION 7
Termination and winding up

In the previous Section, we discussed that a sense of trustworthiness is essential to enable any data trust to operate. In order to be considered trustworthy, a data trust will, inevitably, need to have considered what will happen when it ceases to operate – whether this occurs voluntarily or involuntarily.

As discussed, data providers will likely require certain assurances in respect of security and use of data, before they are willing to provide such to a data trust or its data users. They will also want these assurances to extend to a scenario where the data trust runs into financial difficulty and/or is wound up.

It may be the case that a data trust is set up for a specific purpose or a finite time – and when that purpose has been fulfilled or the relevant time has expired, it will be wound up in accordance with its rules. Alternatively, a data trust might be open-ended, with a broadly defined purpose and no fixed timeline.

The considerations we discuss here are relevant to both of these cases. Even in the case of a data trust with a clearly defined (and achievable) purpose, we will need to consider what will happen to the data it holds (or to which it may be entitled to grant access) if, say, it commences operations but is unable to fulfil its purpose owing to an unforeseen shortfall in funding.

The legal form a data trust takes – and, in particular, its ownership and funding – are particularly relevant in this context. If, for example, a data trust is state-owned, you might argue that whatever its balance sheet may look like, data providers can take comfort from the fact that a government is unlikely to let a state-owned entity fail in such a way as would result in an embarrassing transfer of rights in its citizens' data, to a third party.

Or you might take the view, as a potential data provider, that a not-for-profit organisation, that may be overly reliant on state funding and that may find it difficult to obtain commercial funding, is not nearly as good a bet as a commercial entity, driven by market incentives and accountable to its shareholders.

The point here, is that different stakeholders will make different judgments, depending on their own views and values. In Section 6, we sought to find a governance model that could be applied across a variety of legal forms. Similarly, here, we recommend that, irrespective of form or ownership, an industry standard should be developed to avoid a scenario where insolvency may result in rights in data being transferred to third parties against the wishes of data providers and/or data subjects. A failure to address this issue upfront will run the risk of a public backlash with a potentially disproportionate impact upon the public appetite for data trusts, as a whole.

7.1 Voluntary and involuntary winding-up

In a commercial contract between two parties, it is often the case that each party will have the ability to terminate that contract if an event of insolvency occurs in relation to the other. This would also seem sensible in any data provision agreement, on the assumption that what is being granted to the data trust by each data provider, is a licence to use certain data.

Any termination would need to be backed up with positive obligations on the data trust to delete relevant data (or retain such only in accordance with an agreed data retention policy) and also to take such steps as may have been agreed, to remove the data from the ambit of any projects undertaken by data users. The extent of these obligations will depend upon the terms agreed in the data provision agreement. It may be the case, for example, that a data provider is willing to agree to the ongoing use of data that it has provided in respect of projects which have already been completed or which are already in train as at the time of termination, but not in respect of any projects that are launched following termination.

In respect of personal data, there will be a further nuance here, in that if the use of that data can no longer be said to be necessary for the purpose for which it is held, it must be deleted (or retained only in accordance with an agreed data retention policy). Absent specific agreement between the data provider and the data trust in this respect, this would arguably be the case upon termination of the data provision agreement. For this reason, among others, the data provision agreement will need to specify clearly, any rights that the data trust (and through it the data users) are intended to have post-termination of the data provision agreement.

The details of any insolvency process will depend upon the underlying legal form of the relevant data trust. Even in an insolvency process, there is always the possibility that such rights as the data trust has, to provide access to data, may be of value to an acquirer. In a scenario where each data provider has the option to terminate its agreement with the data trust upon an event of insolvency, however, the value of these rights will be limited and a potential acquirer may need to strike new deals with each of the data providers.

The terms of the data provision agreements will also impact upon the ability of a data trust to raise debt funding. Whether this is material will obviously depend upon how the data trust is to be funded. If debt funding is sought, lenders will likely want security over the business and assets of the data trust. However, if, for example, all rights of the data trust to data are stated to cease upon an event of insolvency, there would be little over which a lender could take security, as the contracts would fall away at the very moment that the lender wished to realise value in them.

That said, if certain data rights are stated to survive termination of the data provision agreements, there may be ongoing revenue streams from existing projects that may be attractive to lenders. Absent rights to data, a lender's security might provide access to some hardware and potentially some intellectual property, but this is likely to be of marginal interest only, in the context of where the real value of a data trust is perceived to lie. In practice, this means that debt funding will be difficult to obtain.

One final point to note is that, in circumstances in which the data trust is operated and controlled by a limited company, the fiduciary duty of a company's directors to the company and its shareholders (see Section 6) will switch, in the event of insolvency, to a company's creditors. We suggested in Section 6, that certain provisions might be incorporated into a company's articles of association to improve the position of a data trust's stakeholders vis-à-vis its owners. This approach would not be effective, however, to improve the position of the stakeholders vis-à-vis the data trust's creditors, as the duty owed by the directors to the company's creditors will trump anything in the articles of association to the contrary.

7.2 Return and deletion of data

In summary, data providers may wish to withdraw their data from an insolvent data trust. Whether they are entitled to do so will depend upon the terms on which they initially provided data to the data trust.

Similarly, data subjects may wish to request deletion of their personal data in this circumstance. Their rights in this respect will be governed not only by the terms on which they provided their data to the data trust, but also by the GDPR. If the data trust's rights to data are sold on to another entity, there may need to be an assessment in respect of personal data, as to whether the data will be used for the same or a different purpose. Will this still be fair to the data subjects? Under the GDPR, there is an obligation not to retain personal data for longer than needed. If the data trust is no longer in existence, then there must be a question as to whether that 'purpose' still exists.

There will also need to be an assessment as to whether data users are entitled to retain the data to which they have access and on which the value of their projects may depend.

The bottom line here is that all of these issues should be considered at the design stage of a data trust. A balance will need to be struck between the data trust and its stakeholders that respects their concerns and wins their trust, while maximising the ability of the data trust to fulfil its purpose.

In this context, it is worth looking at some of the learnings that have come from the financial sector in recent years and, in particular, the requirement for various financial institutions to draw up so-called "living wills". Under these arrangements, major banks were required to draw up recovery plans, setting out measures that they would take to restore their viability should their financial situation deteriorate. As a part of this, they were also required to consider the restructuring and winding down of their operations.

While it is unlikely that a data trust, in its early stages, would be characterised as "too big to fail", a data trust still needs, from inception, to engender a sense of trust amongst participants that sets it apart from many other organisations. While a "living will" along the lines of those drawn up by the major banks would be overkill in the context of a start-up data trust, in order to reassure stakeholders, these issues should be addressed sooner rather than later. Issues that might be covered in a "living will" include:

- deletion or retention of data pursuant to an agreed data retention policy;
- an obligation to inform data subjects of any proposed change of ownership or winding up;
- the circumstances and the terms on which such a change of ownership or winding up might occur; and
- the ability (or not) of data users to retain and continue to use data in these circumstances, taking account of the consequences, practical, financial or otherwise, to those users if rights of data access are lost.

An alternative approach might involve some form of state guarantee such as the 'Crown Guarantee' that exists in respect of the BT pension scheme and that would kick in in the event of a winding up of BT plc. One of the principal aims of the "living will" arrangements, however, is to allow for an orderly wind down without any need to resort to taxpayer funds.

7.3 Limited continuing use

Upon any winding up (or indeed, upon any termination of a data provision agreement, where that data has been used by data users), we distinguish three different categories of project:

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

Where any project has been completed, a winding up of the data trust or the termination of a data provision agreement, should have only minimal impact upon the relevant data users. While they may no longer have access to the underlying raw data, they will remain entitled to their findings that were based upon that data.

Where projects are in course, subject to funding (see below), data users should be entitled to complete those projects. Those data users will have relied upon the data being available on the terms offered by the data trust and may already have provided consideration for such.

Conversely, no new projects should be commenced following a decision to wind up the data trust. In the case of a termination of any data provision agreement, no data user should be entitled to use the data that forms the subject matter of that agreement for the purposes of a new project, following the giving of notice to terminate that agreement.

Terms to this effect could be included in the data provision agreements and data use agreements; however, whether or not these outcomes are achievable in any given case will depend upon the financial position of the data trust and the relevant participants.

7.4 Costs

If the data trust is solvent at the relevant time, then the position set out in Section 7.3 above, should be achievable. If the data trust is insolvent, however, this may be problematic.

We have already mentioned the use of "living wills" in the financial sector. One way to offset the risk of insolvency here, would be to require the data trust to maintain an amount – similar to the capital maintenance requirements on banks – sufficient to allow for the completion of its current projects. Any such amount would need to be ring-fenced in some way so as to ensure that it was available for these purposes, rather than for the data trust's secured and unsecured creditors, generally.

A balance would need to be struck between the needs of the data providers and the data users. It would, for example, be inequitable for the rights of the data users to be guaranteed or preferred in this way, if data providers remained unpaid or partially paid for the use of the data on which those current projects (and indeed, completed projects) are based. Any analysis of the adequacy of this capital amount should, therefore, take into account amounts due to data providers, as part of the data trust's running costs.[182]

A further possibility to protect the ongoing rights of data users, would be to make the relevant data subject to some form of escrow arrangement with an independent escrow agent. This might allow data users to have limited rights for continuing use, along the lines we discussed in Section 7.3, in the event of a data trust's insolvency. The terms of any such escrow would need to be agreed upfront and made known to data providers and incorporated into the terms of any data provision agreements. The costs of any such arrangement would need to be considered carefully, as the data trust would be unlikely to have sufficient funds to pay for this at the relevant time.

We have also talked about the potential use of some form of state guarantee, as an alternative to a "living will".

Absent any of these options, if there is a potential acquirer of the data trust or of its business and assets, then, as mentioned in Section 7.1, there may be scope for the agreement of individual deals with the acquirer on an ad hoc basis.

We should bear in mind, here, the potential existence of so-called "ransom creditors". In an insolvency scenario, these are generally suppliers, whose supplies are vital to the insolvent entity and which it would be hard to source elsewhere. These creditors may, in light of their bargaining position, be able to negotiate terms which are preferential to those available to other creditors. In the context of a data trust, this might be a supplier of key data or, potentially, a supplier of technology infrastructure or hosting services.

There is no silver bullet for insolvency but sound planning can mitigate its worst effects and provide some reassurance to the data trust's participants in respect of the meeting of their respective expectations.

> One way to offset the risk of insolvency here, would be to require the data trust to maintain an amount – similar to the capital maintenance requirements on banks.

[182] In this context, it is worth noting that a data trust with a "decentralised" technical architecture – providing access to data which is provided and hosted by others – will likely have lower running costs than a data trust which itself hosts all of the data provided to it by data providers.

Queen Mary University of London

SECTION 8
Conclusions

8.1 Bespoke legal structures

One important conclusion from our research is that each data trust will need its own, individually designed, legal structure. It is not possible to recommend any single form of legal structure or even to produce a set of templates from which data trusts could choose. This is because a data trust's legal structure needs to be designed so as to accommodate the rights and interests of all potential stakeholders. This includes:

- data providers (including future and as yet unknown data providers);
- data users (present and future);
- owners of rights in data;
- data subjects; and
- potentially at least, the wider public.

It is the interaction of those rights and interests which will determine the best legal structure for the data trust. An attempt to shoehorn the data trust into a legal structure which is chosen before these rights and interests are analysed runs the risk of failure, or at best some complex and unnecessary legal documentation to make the chosen structure fit more closely to the needs of the data trust.

That said, we think it likely that most data trusts will adopt either a purely contractual structure or a corporate structure supplemented with contractual agreements. A contractual structure might be suitable for a data trust which consists of a small group of data providers and data users who are already trusted by stakeholders to behave appropriately in respect of the data. One example might be the sharing of data between hospital trusts and academic researchers. If, though, some of the data trust's participants are commercial organisations or plan to use the data for commercial gain, or if the data trust is complex, we think it likely that a corporate structure will be needed. A corporate structure has formal governance mechanisms which are reinforced by company law, and these can be crafted so as to engender trust by stakeholders, and in particular to strike a balance between the different interests of the data trust's participants. It is also important to remember that a corporate structure will be supplemented by contractual agreements.

In the long term we think it probable that a number of standardised legal structures for data trusts will emerge, most likely focused on particular sectors of activity. Even then, these standardised structures will merely form a starting point for the creation of a new data trust, and will inevitably need some customisation to fit the data trust's aims and the interests of stakeholders.

8.2 Trust law and fiduciary stewardship

Some commentators on data trusts have expressed very strongly the view that the existence of fiduciary duties imposed by a legal trust law is a fundamental prerequisite for any data trust. As we have explained in Section 1, and in detail in Section 2, we disagree about the role of trust law. As we point out, the fiduciary duties imposed by trust law would require the trustees to allow data to be shared only for the benefit of a defined group of beneficiaries, so that wider sharing for the public benefit would be a breach of duty unless the legal trust were a charitable trust.[183] Trustees must return any benefits they make from trust property to the legal trust, unless the trust deed provides otherwise, and thus any data provider or data user which planned aimed to generate profits from the data would be disqualified from taking part in the governance of the legal trust, with the result that an important group of stakeholders would not be represented. Data is not a recognised category of property which can be legally owned by trustees, and so substantial changes to trust law would need to be made (see Section 8.3.2).

This does not mean, though, that we reject the concept that those who are stewards of data should owe duties to those who have rights and interests in that data. As we have explained throughout, the existence of such duties is fundamental to achieving the trust which a data trust needs to meet its aims and objectives. Our point is that the mechanism of trust law is an inappropriate way of attempting to impose those duties, which are more effectively dealt with in a data trust's constitutional documents, operational rules and framework of contractual agreements.[184] Duties need also to be owed to participants who would not qualify as beneficiaries under trust law, and these can be imposed in the same way.

8.3 Law reform to facilitate the use of data trusts

8.3.1 Data protection – repurposing and legitimate interest

Where data which is to be shared includes data which is, or might potentially be,[185] personal data, data protection laws present challenging barriers to that sharing and re-use. Such sharing and re-use requires a legal justification in accordance with Article 6 of the GDPR. Consent by the data subject is always a sufficient justification if it is "freely given, specific, informed and unambiguous"[186], but obtaining such consent retrospectively from all the data subjects represented in a dataset is usually an impossible task. And seeking consent when data is first collected to its subsequent use for as yet unknown purposes can never be specific, informed and unambiguous, because those purposes cannot be explained when the advance consent is sought.

Public authorities, such as the Borough of Greenwich and the GLA in one of the pilot studies, are currently able to use and process data

for new purposes if that processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".[187] Although the limitations on this justification are complicated[188] it is applicable to a wide range of public sector data re-use. The difficulty is that the justification is only clearly available to a public authority – if control of the data is ceded to a data trust or, via the data trust, to a data user, then the justification is only available if the new controller is also a public authority, or if the new controller is able to "specify the relevant task, function or power, and identify its statutory or common law basis".[189] Therefore, there is a risk that by sharing data via a data trust, the ability to rely on the public task justification might be lost.

An alternative justification for re-use without the consent of data subjects is that the re-use is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".[190] In order to take advantage of this justification the data trust will need to assess the proportionality of the legitimate interest in relation to the interests of data subjects, and be able to demonstrate both (a) that the legitimate interest is strong enough to outweigh the interests of the data subjects in being given the opportunity to give or deny consent, and (b) that there are adequate safeguards in place to protect the interests of the data subjects. This is discussed further below.

[183] Charity law has not been investigated in depth for this report, but it will inevitably restrict substantially the activities of data trusts. In particular, it is likely to disqualify some categories of stakeholder, especially commercial organisations, from playing a part in the data trust's governance because of potential conflict of interest. See further Charity Commission, Conflicts of interest: a guide for charity trustees (May 2014, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636091/CC29.pdf).
[184] See further Kieron O'Hara, Data Trusts – Ethics, Architecture and Governance for Trustworthy Data Stewardship, WSI White Paper #1 February 2019 (https://cdn.southampton.ac.uk/assets/imported/transforms/content-block/UsefulDownloads_Download/0326D18DCC9E4BD08816BB5F994FCA76/White%20Papers%20No1.pdf).
[185] The definition of "personal data" in GDPR art. 4(1) includes data from which an individual can be identified indirectly. Data which does not identify an individual can become personal data if its controller also controls other data which, in combination with the first data, can be used to identify her or him. The aggregation or combination of datasets via a data trust can thus result in data becoming personal data, even if there is no intention to use it to identify individuals.
[186] GDPR art 4(11).
[187] GDPR art 6(1)(e).
[188] See eg Medical Research Council, Guidance note 4: General Data Protection Regulation (GDPR): Public interest, approvals and 'technical and organisational measures' (23 May 2018, https://mrc.ukri.org/documents/pdf/gdpr-guidance-note-4-public-interest-approvals-and-technical-and-organisational-measures/).
[189] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/.
[190] GDPR art 6(1)(f).

We think it likely that most data trusts will adopt either a purely contractual structure or a corporate structure supplemented with contractual agreements.

A superficially attractive way to remove the uncertainty inherent in using these two justifications would be to call for substantive law reform, specifically providing that sharing data via a data trust is an additional justification for processing personal data, or as an alternative providing that sharing via an appropriate form of data trust constituted performance of a public task or was a legitimate interest of the data trust members who controlled personal data. Such law reform is not possible because, as this report has shown, there is no single model of data trust which could form the basis for such a provision. If "data trust" cannot be defined sufficiently precisely, the concept cannot be used in legislation.

However, uncertainty could be substantially reduced by guidance from data protection supervisors. Although such guidance is not law, compliance with it avoids the possibility that a supervisor might take enforcement action (though of course guidance can change, and a data trust would have to modify its workings if this occurred). We suggest that the ICO should consider producing specific guidance about how data trusts could enable the re-use of personal data without needing to seek consent from data subjects, using these two justifications.

That guidance would be based on the jurisprudence of the Court of Justice of the EU in the cases of *Digital Rights Ireland and Schrems*[191] and on the Advocate General's Opinion in *PNR-data*.[192] In all those cases, personal data was transferred to the control of a person other than the original controller (and, although it is not relevant for this discussion, outside the EEA and thus outside the territorial jurisdiction of EU law). The effect of the transfer in each case was to reduce the means available to protect the rights of data subjects, but to introduce different safeguards for those rights which were, arguably, less effective. In *Schrems* the transfer had the effect of completely removing some rights which data subjects would have under EU law, and for that reason the court held that the transfer was not legally permissible. But in both *Digital Rights Ireland* and *PNR-data* the court held that so long as no "core" or "essential" rights were taken away, the substitution of different means for protecting them could be permissible if there were a countervailing societal benefit, and the balancing of the reduced effectiveness of means of protection was proportionate to that benefit.

This is exactly how data trusts should work. The ability of data subjects to withhold consent for re-use is a measure which protects their core rights, and the data trust would substitute for that measure a different set of protections, set out in the data trust's rules for re-use and its mechanisms for securing compliance to those rules. The focus of guidance should thus be on how data trusts should develop data sharing rules which preserve the core rights of data subjects and on how they should balance the societal benefits from data sharing against the interests of the data subjects when deciding whether to allow such sharing.[193]

8.3.2 Trust law

If a government were to take the view that it is important to impose trust-derived fiduciary obligations on those who have a data stewardship role, trust law would need to be amended. The main changes which would be needed are:

- A redefinition of trust property so as to include data, and potentially other digital assets. Such a redefinition would be highly problematic because, unlike other kinds of property, there is as yet no clear picture from case law and legislation in other fields about what aspects of data and digital assets are capable of being "owned", and what the legal effects and consequences of ownership might be. A redefinition would affect the whole law of trusts, and so would require extensive public consultation. Such an exercise would most appropriately be carried out by an established law reform body such as the English and Scottish Law Commissions, and would be likely to take years rather than months to complete. Thus, even if law reform were contemplated, for the time being data trusts would need to adopt some different model, and most problematically, would need to devise it in such a way that it could be converted to the new trust law model once law reform was completed.
- Devising a new category of legal trust which can engage in stewardship of data for some wider public benefit, but without the restrictions imposed by the law of charitable trusts, particularly the restrictions on receiving benefits from trust property. Again, this is likely to require extensive consultation and would be a long-term project.

Because, as explained in Section 8.2, it is possible to use contracts and corporate governance documents to impose equivalent obligations to those imposed on fiduciaries under trust law, we suggest that such a law reform project is unlikely to be worth embarking on.

8.4 Governance as a trust-enhancing mechanism

Finally, we think it important to reiterate the overarching role of appropriate governance. Data trusts need to make a wide range of decisions, including in particular:

- the data trust's main aims and purposes and how it plans to achieve them;
- who is to take part in the management, operation and governance of the data trust, and how potential conflicts of interest are to be managed;
- who can be admitted to the data trust as a data provider;
- who is allowed to receive data via the data trust;
- the limitations on use of data received from the data trust;
- the financing structure of the data trust and any payments from or to data trust participants;

[191] Joined Cases C-293/12 and C-594/12 Judgment of the Court (Grand Chamber), 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238; Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650.
[192] Opinion 1/15 of Advocate General Mengozzi, Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 8 September 2016.
[193] The main factors to be considered are set out in GDPR art 6(4).

- how funds received by the data trust are to be applied or distributed; and
- obligations to return or delete data, or to bring new data within the ambit of the data trust.

As we have shown throughout the report, all these decisions have legal implications, and all of them engage the interests of the wider group of stakeholders in the data trust. The governance structure which a data trust adopts, and the mechanisms it adopts in order to ensure that its decisions respect the interests of its stakeholders, are therefore critical to ensure the data trust meets its legal obligations and achieves its aims.

Because each data trust will be a bespoke operation, as explained in Section 8.1, each will also need a bespoke governance structure and set of operating methods. The analysis in this report should be helpful to the legal advisers of a potential data trust, but is unlikely to be easily accessible for those who are thinking of setting up a data trust to follow before they engage legal advisers. Simplified guidance on governance, for use at the initial stage of data trust planning, could be very helpful here. And if that guidance were produced or endorsed by government and regulators, it would provide much needed reassurance that embarking on a data trust project will not present insurmountable difficulties for legal and regulatory compliance.

> The focus of guidance should thus be on how data trusts should develop data sharing rules which preserve the core rights of data subjects and on how they should balance the societal benefits from data sharing against the interests of the data subjects when deciding whether to allow such sharing.

Pinsent Masons

ANNEX A
Competition law and State aid

1. Competition law considerations

Competition law in the UK is principally concerned with two main prohibitions:[194]

- 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[195]), 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 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 publically available (for example through benchmarking to increase standards, or shared research and development to create new products or services which would otherwise not exist).

Therefore, in light of the Chapter I Prohibition, any data trust will need to 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. For example, the sharing of certain particularly sensitive information types, such as future pricing and volume information, is almost always prohibited. Beyond this, it is important to minimise the exchange of commercially sensitive information so that it goes no further than necessary to achieve the legitimate objective of the data trust.

In order to assess whether information should be shared it is necessary to look at both the type and scope of the information being shared (for example age, content and frequency). To the extent that more sensitive information needs to be shared, it may be necessary to consider aggregation and anonymisation of the information, and who within an organisation has access to the information.

More generally competition authorities are focusing heavily on the use of big data and its potential to be used for anti-competitive means. For example, the use of self-learning pricing algorithms, which have access to large quantities of information, could result in anti-competitive results even without the knowledge of the parties. Such theories are on the forefront of competition law enforcement policy[196]; so any data trust should be mindful of changes to this dynamic area of law[197], and remain aware of how its data is being used by participants.

The Chapter 2 Prohibition

The Chapter 2 Prohibition prohibits abuses of a dominant position. It should be noted accumulation of data is not, by itself, problematic from a competition law perspective. For a data trust to breach this prohibition the data trust would firstly need to be in a dominant position (for example if the data trust become dominant in the provision of certain data or access to the data trust has become essential for competitors in order to compete effectively); and secondly that the data trust was in some way abusing this position. Abuses can consist of either exploitative practices such as excessive access fees or unnecessary terms and conditions[198], or exclusionary practices such as granting discriminatory access or refusing access to certain companies (for example through the use of exclusive licences).

The House of Commons Select Committee[199] has already 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.[200]

We have already seen examples of where competition law authorities have forced the sharing of data due to concerns regarding a lack of competition. For example, in 2012, 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 194 above)) 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 their customer lists and other customer information to other operators to allow them to target new customers.

2. State aid considerations

Introduction to State aid

In determining the structure of the data trust and any financial model that apply to receipt of data, it will be important to consider if any State aid issues arise.

Under the European Union rules it is unlawful for State bodies to provide assistance to entities carrying out economic activity where this would distort fair competition. This assistance is called State aid, and the rules barring it are enforced by the European Commission and national courts.

How to identify if the measure is State aid

(all parts of the test below must be met for State aid to be present)

01 **Is there a transfer of State resources?**
'State resources' includes funding and other types of assistance (or provision of data at less than market price) from central government, State-controlled public agencies, regional and local government and State resourced research grants.

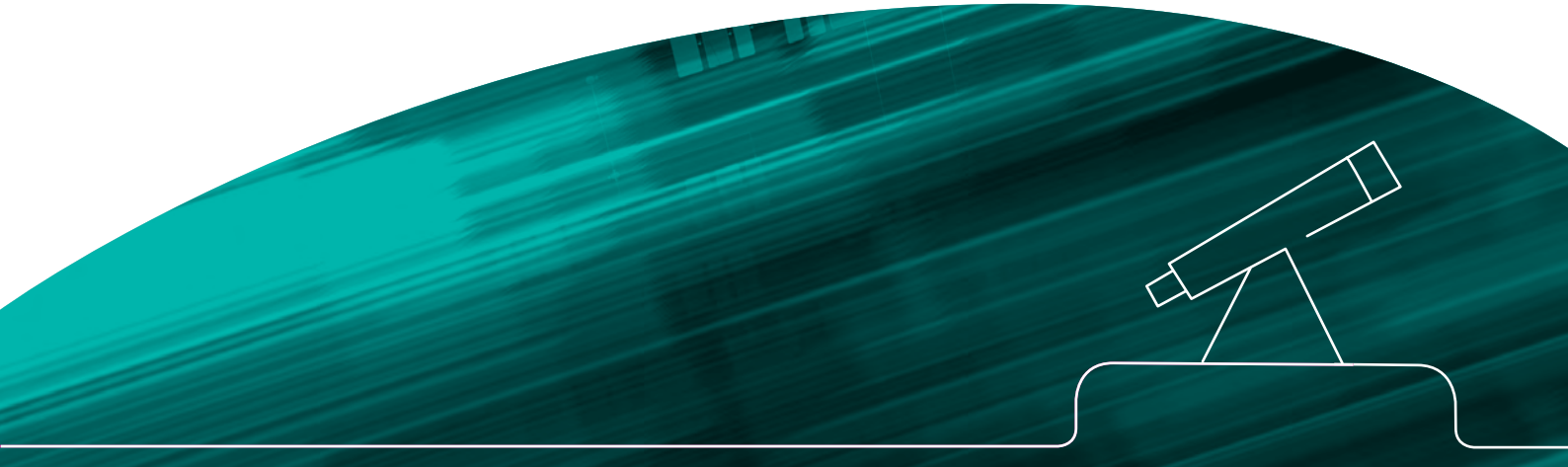
02 **Is the recipient of State resources carrying out an economic activity?**
For example processing of data for a fee.

03 **Does the aid provide the recipient with an advantage over its competitors?**

04 **Does the aid potentially distort competition between EU Member States?**

The measure is likely to be State aid

[194] 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).
[195] 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).
[196] In 2018, the UK competition authority invested in its own specialist data analytics team to ensure it stays ahead in the fields of data engineering, machine learning and artificial intelligence techniques.
[197] On 25 February 2019, Andrew Tyrie (CMA Chair) wrote to the Secretary of State for Business, Energy and Industrial Strategy outlining a number of key changes which should be implemented to the UK competition law regime. This letter discusses the potential for amending the Chapter 1 Prohibition to better regulate the use of pricing algorithms.
[198] 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.
[199] House of Lords Select Committee Report, Artificial Intelligence Committee, 'AI in the UK: ready, willing and able?' Published 16 April 2017 - HL Paper 10
[200] Report, 'Big Data: Bringing Competition Policy to the Digital Era', by the OECD, November 2016,



Pinsent Masons

State aid and data trusts

There is a risk of State aid arising in a variety of ways as a result of the establishment of a data trust. There is potential risk in the following sample scenarios:

- where public bodies provide funding or other forms of assistance towards the establishment of the data trust;
- where public bodies pay a fee to the data steward or other participant in order to gain direct access to the data which forms part of the data trust;
- where public bodies act in the capacity of data providers by passing data that they have obtained to intermediary private undertakings who are acting as data stewards;
- where public bodies sell data to a data dissemination platform;
- where public bodies act in the capacity of data steward by obtaining data from data providers and then disseminating this data to private undertakings; and
- where a public body invests funding (for example by way of equity) in an entity carrying out economic activity of any kind (for example processing and disseminating data for a fee).

In order to determine whether the establishment of the data trust, and its activities, creates a risk of unlawful State aid, it will be necessary to apply each limb of the four part test (outlined in the flow chart). Where State aid is deemed to be present, there are a number of exemptions and solutions which may be applicable. Specific legal advice would need to be sought on the details of each arrangement. Some potential solutions for exploration are set out below. The list is non-exhaustive; there are a number of other State aid solutions available beyond these that could be considered.

Where a public body is deemed to have provided unlawful State aid, this could result in the organisation being awarded aid suffering severe financial consequences as they may be ordered to repay the aid with interest. There is a ten year limitation period for bringing such a challenge. Furthermore, there is likely to be reputational damage for the authority that granted the unlawful State aid.

Potential solutions to State aid

If a measure amounts to State aid and it is not notified to, or approved by, the European Commission before it is put into effect it will be unlawful. Some exemptions and exclusions apply and these are subject to detailed guidance from the European Commission.

Market Economy Investor/Operator Principle ("MEIP/MEOP")

Economic transactions carried out by Member States do not confer an advantage in favour of an undertaking, and therefore do not constitute State aid under EU law, if they are carried out in line with normal market conditions. An example of this would be where a public body purchasing data ensured it paid market price by carrying out a competitive, transparent, non-discriminatory and unconditional tender procedure in the context of the sale and purchase of assets, goods and services. It may also be possible for the public body to engage independent consultants to carry out a benchmarking exercise of equivalent transactions carried out by comparable private operators in similar situations (when purchasing data or commercially investing in a data trust). It is important that in carrying out such an exercise, the public body ensures that the commercial opinion meets the requirements of European guidance and case law on MEIP/MEOP.

General Block Exemption Regulations ("GBER")

The GBER provides an exemption from the requirement to notify and obtain prior approval from the European Commission in respect of certain typical State aid measures. The GBER sets out detailed provisions for the treatment of specific categories of aid. The provisions explain in relation to each category the eligible costs that may be taken into account and the level of aid intensity. Examples of GBER exemptions include aid for research, development and innovation, aid for SMEs, training aid and aid for culture and heritage conservation etc.

Aid is covered by the GBER only insofar as the costs fall within certain specified categories (eligible costs) and only up to certain specified thresholds of all such costs (aid intensity). The GBER contains rules for determining the eligible costs and aid intensity.

De Minimis aid

The De Minimis Regulation allows small amounts of aid – less than €200,000 over 3 rolling years – to be given to an undertaking for a wide range of purposes. If this mechanism is used records of aid granted must be kept and all the rules of the de minimis regulation must be followed.

State aid and the impact of Brexit

It is worth noting what impact Brexit will have on State aid laws.

Permutation 1 – State aid under the Withdrawal Agreement

During the transition period EU law will continue to apply in the UK as it does today – including in relation to State aid. In effect, there would be no change to the law regarding State aid during the transition period.

Article 92 of the Withdrawal Agreement describes the situation where procedures are ongoing at the end of the transition. The European Commission will remain competent to resolve any State aid investigation that has been allocated a case number by the end of the transition period. The European Commission will then proceed as normal either to raise no objections, find no aid, or start a formal investigation.

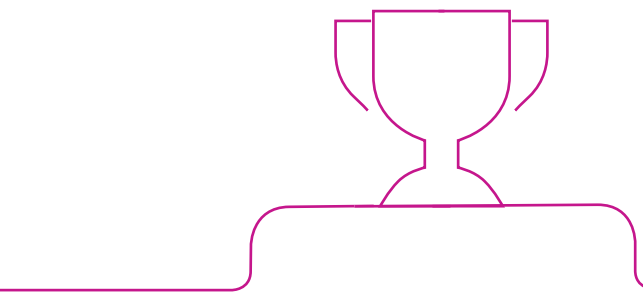
Following the transition period, it is expected that a State aid regime will be introduced in the UK that closely reflects the draft secondary legislation that has been prepared in the event of a no-deal Brexit (outlined below).

Permutation 2 – State aid in the event of a 'no-deal' Brexit

Draft secondary legislation has been prepared which will introduce a new State aid regime in the UK in the event of a 'no-deal' Brexit. The draft legislation proposes that the regime will be based on the current EU State aid regime, with the current EU regime essentially transposed into UK law, with the Competition and Markets Authority ("CMA") appointed as the regulator of such a regime. Alongside the draft secondary legislation, the CMA has also published guidance on how it would operate.

The State Aid Regulations give the CMA supervisory and, notably, enforcement powers in place of the European Commission. In some places the rules go further than the EU State aid regime. They give the CMA new enforcement powers such as 'dawn raid' powers which allow the CMA to enter and search aid beneficiaries' premises in the event that misuse of aid is suspected. Following an investigation, the CMA has the power to grant four different types of orders in relation to an aid measure: interim suspension; interim recovery; termination; recovery.

The limitation period for reviewing the aid remains the same as the current scheme of 10 years, so there is no change here in terms of how long aid grantors and recipients should hold onto the relevant documentation relating to the granting of the aid.



Queen Mary University of London

ANNEX B
Liability arising from data stewardship

This report has included very little discussion of the liability of those individuals who undertake a data stewardship role[201], which some readers might find surprising[202]. There is, though, a very good reason for this omission.

Throughout the report we have emphasised that each data trust will require a bespoke legal structure, governance system and set of rules for data sharing. These will need to meet the collective needs of the stakeholders in the data trust, and will thus be different for each data trust. We think it inevitable that the documentation which defines those matters, and imposes legally binding compliance obligations on participants in the data trust, will also deal expressly with the liability of those individuals in a data stewardship role. The liability regime will therefore also be bespoke to each data trust.

That said, we recognise that readers who are considering setting up a data trust may wish to know what the liability of those in the data stewardship role would be if there were no express liability provisions. An understanding of these matters may be helpful in devising an express liability scheme.

1. Liability and legal structures for data trusts

As we explained in Section 2, there are three main legal structures which a data trust might adopt.

- A purely contractual structure, in which all the rights and obligations of participants in the data trust are defined in legally binding agreements. There is no default system of liability under such a structure; liabilities arise from, either: (i) the contractual agreements; or (ii) otherwise at law including under relevant regulation and legislation, such as liabilities arising under the GDPR or liabilities, which are established under legislation and which cannot be excluded or varied by contract. The contractual documents need to set out the respective rights and obligations of the participants in the data trust and how risk and liability is to be allocated among those participants. This will include to whom the duties are owed, which can extend to third parties to the contract (such as individuals whose data is stewarded by the data trust) if the contract appears intended to confer the benefit of those duties on them or if legislation or regulation so dictates.
- A legal trust structure. We think that adopting such a structure is highly unlikely because trust law is conceptually a bad fit for a data trust (see Section 2). However, we also suggest that the duties imposed upon legal trustees are a useful starting point for deciding the duties which those who undertake a data stewardship role should be subject to. It will therefore be useful to explain those duties and other liabilities which can arise for their breach.
- A corporate structure. The directors of the data trust company will be the individuals undertaking data stewardship through the person of the data trust, and so it is also worth examining the duties of company directors.

Readers should note that only a contractual structure will impose liabilities which are specifically about data stewardship. For the legal trust and corporate structures, data stewardship liability is a side-effect of the general liability of those in charge, and this is another reason why we think that express provision about the duties and liabilities of those who undertake data stewardship will be essential, whatever legal structure is adopted by the data trust.

Legal trusts

In a legal trust the trustees own the trust property, and they owe *fiduciary* duties to the beneficiaries which are all based around dealings with the trust property. Adopting legal trusts as an analogy would require data stewardship duties to focus on dealings with the data.

The fundamental duty of trustees is to avoid any conflict between the trustee's own interests and those of the beneficiaries:

"… no person having duties of a fiduciary nature to discharge should be allowed to place himself in a situation where he has, or can have, a personal interest conflicting, or which may possibly conflict, with the interest of those whom he is bound to protect."[203]

[201] The Synthesis report (http://theodi.org/article/odi-data-trusts-report/) defines these people as "trustees". But in this Report we need to use that term specifically to mean the trustees of a legal trust, and so have adopted a wider description of such individuals.
[202] Although see further (i) Section 6.1.5 for general observations on the allocation of liability between a data trust's stakeholders; and (ii) commentary in Sections 3 and 4 on the liability of data providers and data users and the allocation of risk in contractual documents.

This is a duty of strict liability, and so it is no defence for the trustee to argue that there was no intention to create a conflict of interest.

Case law has identified different elements of this fundamental duty:

- the trustee must account for (i.e. hand over to the legal trust) any profit he makes from his position as trustee;[204]
- the trustee must execute any powers given to him by the trust documents only in accordance with the scope of the power granted.[205] In its analogical application to a data trust, this duty might be breached by licensing as a data user some category of person outside the categories specified in the data trust's aims and objectives;
- in deciding whether to exercise a power, the trustee must give proper consideration to relevant matters and not consider irrelevant matters;[206] and
- any power must be exercised in good faith. This means that the trustee must not exercise a power outside the scope of the trust documents, even if the trustee honestly believes that doing so would be "a more beneficial mode of disposition of the property and more consonant with that which he believes to be the real wish of the donor of the power".[207] To analogise to data trusts again, licensing a data user in a category to which data is expressly forbidden to be licensed would be a breach of this duty, even if the trustee believes doing so would advance the aims of the data trust (and even if that belief is shared by everybody else).

Breach of these duties gives rise to two kinds of potential liability.[208] The trustee is liable to compensate the legal trust for any losses which it suffers by reason of the trustee's breach, and also to account for any gains which the trustee has made from their position. However, it is possible for the legal trust documents to exclude the trustee's personal liability for breaches of trust, and such exclusions are common. Otherwise it would be difficult to find trustees who are willing to act, because of the liability risks. It is possible for the exclusion to cover negligence, and even gross negligence on the part of the trustee, and even to extend to deliberate breaches of trust which the trustee reasonably believes are in the best interest of the beneficiaries. It is not, though, possible to exclude the trustee's liability for breaches of trust which occur as a result of fraud or reckless conduct.

Corporate data trusts

A director of a company owes the duties which are set out in the applicable company law, which in the case of the UK is the Companies Act 2006. Sections 171-177 of the Act set out those duties as follows:

171. duty to act within powers;
172. duty to promote the success of the company;
173. duty to exercise independent judgment;
174. duty to exercise reasonable care, skill and diligence;
175. duty to avoid conflicts of interest;
176. duty not to accept benefits from third parties; and
177. duty to declare interest in proposed transaction or arrangement.

These duties[209] are owed to the company itself and not to the shareholders (even though the shareholders are the owners of the company). Thus a decision to enforce any claim against a director for breach of duty must be made by the board of directors, and the shareholders only have indirect power here through their ability to refuse to reappoint directors and instead appoint new directors. It should be apparent that Sections 175-177 of the Companies Act 2006 impose fiduciary duties which are very similar to those imposed on legal trustees, and the discussion of those duties will be applicable here too. The remedies available to the company are the same as those available to the beneficiaries of a legal trust: compensation for losses suffered by the company and an account of any benefits the director has received as a consequence of breach of the fiduciary duties.

2. Liability under the general law

In addition to their duties under contract or as company director or trustee, a person in a data stewardship role also has potential exposure to liability claims under the general law. The full range of possible liabilities is far too extensive to be analysed here, and in any event depends entirely on the particular context of a data trust.[210] However, there are two possible sources of liability which are worth explaining briefly.

[203] 46 Halsbury's Laws of England (2014) 233. See also 98 Halsbury's Laws of England (2019) 366.
[204] 98 Halsbury 367.
[205] Ibid 593.
[206] Ibid 594
[207] Ibid 605.
[208] Ibid 639.
[209] For a more detailed explanation of each duty see 14 Halsbury's Laws of England (2016) 573-590.
[210] As an example, if the data trust were stewarding patient medical data and one of those with a stewardship role was a doctor, in some circumstances the doctor might have a liability under the rules regulating the medical professions (though we have not investigated how far those circumstances are likely to arise in practice). To make the contextual point clearer, medical profession regulation would apply differently, perhaps not at all, to a non-doctor undertaking the same stewardship role.

Under data protection laws, the primary data protection obligations are placed on data controllers. These are defined as any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[211] Making such decisions is an obvious element of stewardship which relates to personal data. However, the fact that a person is involved in making such decisions will not necessarily mean they face potential liability under data protection laws. As one example, if the data trust is structured as a corporation then it will be the company which is the data controller; the directors who actually make those decisions are making them on behalf of the company, rather than in their personal capacity, and so in most cases it is the company which will face liability under data protection laws rather than the directors.[212] In a contractual data trust it would be possible to denote one individual as the data controller, acting on the advice of others but not bound by their decisions, in which case that person would be the sole controller. However, this kind of contractual arrangement creates a risk that the courts would look behind the legal form, so that if in practice the named data controller never made independent decisions then those who did in fact decide how personal data would be shared would be treated as joint controllers.

Liability for breach of data protection laws varies from liability to comply with enforcement orders made by the data protection regulator through to fines to a maximum of €20m (or, if the controller is an undertaking, 4 per cent of worldwide turnover if that is greater).[213] For breach of some data protection obligations, or for breaches that cause them distress, data subjects also have the right to claim compensation.

The general law of negligence might also impose liability on a person in a stewardship role if that person owes a duty of care to that other who suffers loss. The requirements for negligence liability are the existence of a duty of care, a breach of that duty, and the causation of foreseeable loss.[214]

Where the loss suffered is not physical injury or property damage, English law is reluctant to impose a duty of care. The main justification used by the courts for doing so is that the defendant gave an undertaking of responsibility to the claimant, and that undertaking covered the acts which gave rise to the loss.[215] In the case of a data trust, the most likely source from which the courts might find such an undertaking is the documents which establish the data trust, define its aims and objectives and set out its rules.

If a duty of care exists, the defendant's obligation is to take reasonable care to avoid foreseeable harms to the person to who the duty is owed. The required level of care depends on the defendant's expertise – thus lawyers are compared to reasonably competent lawyers, IT security professional to other similar professionals, and so on.[216] If a defendant has been negligent, liability only extends to those losses which out to have been foreseen as a possible consequence of the breach of duty.[217]

Liability for negligence is to compensate the claimant financially for the losses they have suffered. In the context of a data trust, this in practice limits the liability risk. Data providers and owners of IP rights in data might suffer losses which are large enough to make a legal claim worthwhile, but an individual whose data has been shared or otherwise dealt with negligently will in most cases suffer little if any financial loss, and thus a claim will not be worthwhile.

3. Liability in practice

From the discussion above it should be clear that the data stewardship duties which arise out of the legal structure of the data trust are potentially very broad, and thus the liability risk is hard to assess in advance of any claim. For this reason we would expect the foundational documents of any data trust to make clear provision about data stewardship liabilities; indeed, this is where the courts will look to understand the duties imposed by law even if there is no clear provision. We think it unlikely that any person would undertake a data stewardship role if their duties were not spelt out clearly. The potential duties owed under the general law cannot be defined by the data trust's foundational documents, and so there is a level of uncertainty here which cannot be managed in advance.

To avoid the deterrent effect of these liabilities, we would expect a data trust to have insurance in place which covers most of the potential liabilities of those engaged in data stewardship. It is quite normal for legal trustees and company directors to have insurance against liability, though fraud and other intentional breaches are not usually covered by such insurance.

The argument that liability, particularly personal liability for breach of fiduciary duties, is what protects stakeholders and keeps a data trust "honest"[218] is at first sight a compelling one. But we suggest that on further examination it does not hold water – data stewardship is fundamental to the successful operation of a data trust, but it will not be achievable if no-one is prepared to take on the role because of the liability risks.

[211] GDPR art 4(7).
[212] However, it should be noted that the Data Protection Act 2018 contains a number of criminal offences and it is possible, depending on the facts and circumstances, that a director could be found to be personally liable for the commission of such offences.
[213] GDPR art 83(4).
[214] Donoghue v Stevenson [1932] AC 562; Caparo Industries v Dickman and others [1990] 2 AC 605.
[215] Caparo Industries v Dickman and others [1990] 2 AC 605.
[216] Bolam v Friern Hospital Management Company [1957] 1 WLR 582.
[217] The Wagon Mound (No 1) [1967] 1 AC 617, Privy Council (Australia).
[218] See e.g. Lillian Edwards, "The problem with privacy: A modest proposal", (2004) 18 International Review of Law, Computer, and Technology 309; Sylvie Delacroix and Neil D. Lawrence, "Disturbing the 'one size fits all' approach to data governance: bottom-up data Trusts" (2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265315.

Pinsent Masons

Queen Mary University of London

bpe SOLICITORS

Notes

The words in this document are copyright the Open Data Institute 2019 and are licensed under a Creative Commons Attribution-Sharealike 4.0 International Licence. Design and images are copyright Pinsent Masons 2019. The trade marks of Pinsent Masons, BPE and Queen Mary University of London are not to be used without their respective permission.

BPE Solicitors LLP is a limited liability partnership registered in England and Wales with number OC349012 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office is St. James House, St. James Square, Cheltenham GL50 3PR. A list of the members of the LLP is displayed at the registered address, together with a list of those non-members who are designated as partners. © BPE Solicitors LLP 2019

This note does not constitute legal advice. Specific legal advice should be taken before acting on any of the topics covered.

Pinsent Masons LLP is a limited liability partnership, registered in England and Wales (registered number: OC333653) authorised and regulated by the Solicitors Regulation Authority and the appropriate jurisdictions in which it operates. Reference to 'Pinsent Masons' is to Pinsent Masons LLP and/or one or more of the affiliated entities that practise under the name 'Pinsent Masons' as the context requires. The word "partner", used in relation to the LLP, refers to a member or an employee or consultant of the LLP or any affiliated firm, with equivalent standing. A list of members of Pinsent Masons, those non-members who are designated as partners, and non-member partners in affiliated entities, is available for inspection at our offices or at www.pinsentmasons.com. © Pinsent Masons.

For a full list of the jurisdictions where we operate, see **www.pinsentmasons.com**

18148