bpe SOLICITORS

Extended ODI Data Trust report: 5

Further use cases to consider

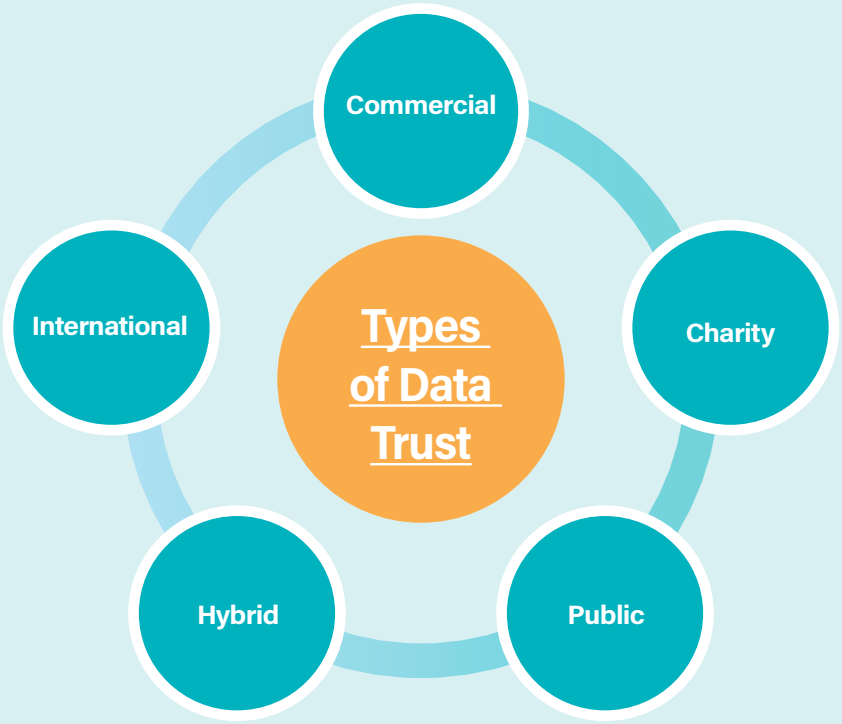
open data institute

Executive Summary

This report refers to the current thinking on the recommended form of a data trust that will best apply to the pilot project specific to the Royal Borough of Greenwich ("RBG") and the Greater London Authority ("GLA"). It should be noted that this model is the correct recommended approach as of 21 February 2019; any reader of this report should be aware that the model could be tweaked slightly as further feedback is received from the GLA and RBG following user interviews and stakeholder engagement workshops.

The form of data trust that would work best from a legal standpoint, and is thus recommended, is to have a separate corporate body set up to act as a data trust and hold data that is licensed to it. This would take the form of a Community Interest Company ("CIC"), as a body that must work towards prosocial aims. It will thus have built into it provisions requiring the promotion of the ethical sharing of data for a broadly public benefit; otherwise the Office of the Regulator of Community Interest Companies can enforce this entitlement.

Data would be licensed to the trust, as data is not a physical asset capable of being donated[1], and the licence can contain terms of how the data should be used. The license could also provide the means by which data providers are paid (if appropriate) for the use of their data. Governance would be conducted by a board managing the day-to-day operation of the data trust, with key shareholding stakeholders meeting less frequently to vote on more significant matters. Any disputes would be resolved by a dispute resolution board and termination of the data trust would be carried out by cancelling the licenses and liquidating the company in the normal manner for a CIC. For a further, more detailed overview of the recommended model, please refer to the legal synthesis report specific to the GLA and RBG pilot.



1 Oxford v Moss [1978] 68 Cr App Rep 183

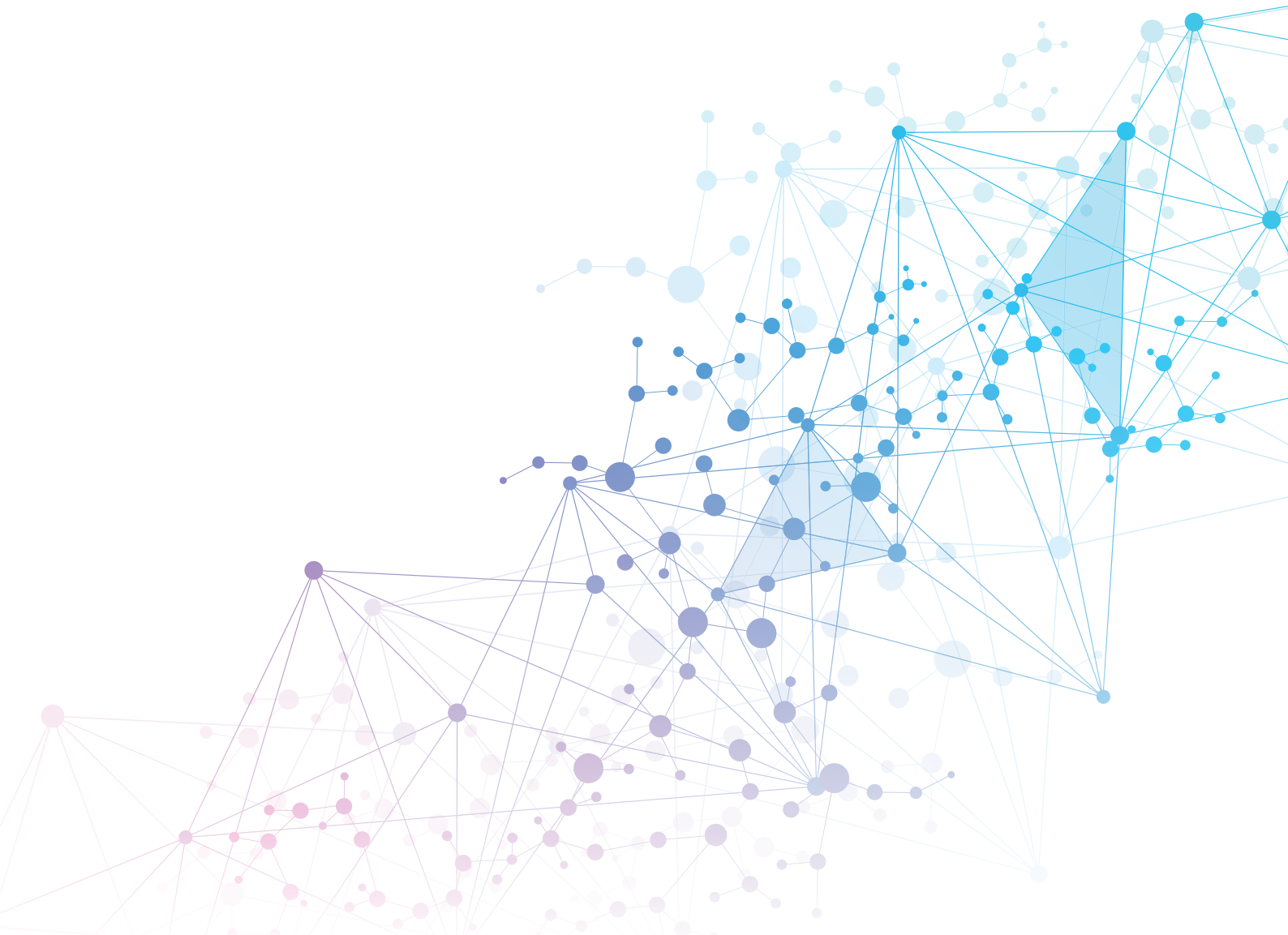
Introduction

The general legal report covers the general legal principles surrounding a data trust whilst the pilot specific legal reports provide more specific designs of a data trust tailored to suit a range of identified contexts.

The pilot specific reports act as a proof of concept for specific structures of data trust, the GLA and RBG pilot being a hybrid form (see below) mixing public bodies and commercial actors, the Wildlife pilot being a form of international data trust sharing between global border forces, and the Food Waste pilot being a commercial form of data trust working towards specific project.

These pilot specific reports focus on the needs of stakeholders in those specific cases. However, they do not posit how other scenarios might affect the data sharing. For example in the international context, how would it differ if it were a more commercial arrangement or if the jurisdictions were different?

If the idea of a data trust is to be adopted more widely to handle issues around data sharing, then all conceivable scenarios where a data trust could help will need to be considered. Below is an analysis on the five different suggested types of data trust, where they could be of use and the legal challenges that each one faces.



Commercial Data Trust

A purely commercial data trust will be one where there are either only commercial institutions sharing data between one another or one where there are primarily commercial organisations as the main stakeholders with some private individuals as well. Regardless of which stakeholders are involved however, a commercial data trust will be distinguished by the fact that it is used for a predominantly commercial purpose. This aligns with a company director's duty, as the company is itself a profit seeking institution, to maximise profit for the benefit of its shareholders and promote the success of the company.[2]

This could either be a data trust that exists for the duration of a specific project similar to a Special Purpose Vehicle company,[3] for a particular sector such as for sharing, for example, analytics data that could be mutually beneficial to all parties, or a purely commercial entity that is looking to profit from the sharing of data.[4]

This does beg the question of how commercial organisations could benefit from a data trust model of sharing data compared with, for example, data sharing agreements specific to a project or a multi-party contract club such as TeX,[5] an arrangement where there is a body providing standard sets of data sharing arrangements for multi-party data sharing.[6]

The clear benefit of these data sharing arrangements are that they are a pre-established format by which data can be shared on a one-to-one basis between organisations. Where a data trust differs is as a way to place data into a central repository and to potentially share data without the need to have specific agreements that have to be signed before accessing data and, ideally, without the necessity of negotiating contracts.

Bolero, a system of transferring records of receipt for shipping cargo,[7] and SWIFT, a group of organisations that share secure financial messages and transaction information,[8] are both so widely adopted due to the standardised form in which they operate. It would therefore seem that in order to have data sharing arrangements adopted more widely, they will need to be both in a standardised form and also in a way that ensures each actor can trust that the information is not going to be misused by anyone accessing the data. The potential benefit of having a data trust over another type of data sharing arrangement, is sharing data, that otherwise might not be in a standard form, but in a standard way that is not liable to misuse.

2 S.172 of the Companies Act 2006

3 Titan Europe 2006-3 Plc Colliers International Uk Plc [2014] EWHC 3106 (Comm) (30 September 2014)

4 [Are there any examples of commercial entities that use these type of arrangements?]

5 http://www.tisaexchange.co.uk/about_tex.html

6 http://www.tisaexchange.co.uk/releases.html?release_id=5

7 https://www.itic-insure.com/our-publications/intermediary/bolero-the-electronic-transfer-of-commercial-trade-information-2878/

8 https://www.swift.com/about-us

9 S.21 of the Companies Act 2006

Legal Issues relating to a purely commercial data sharing arrangement

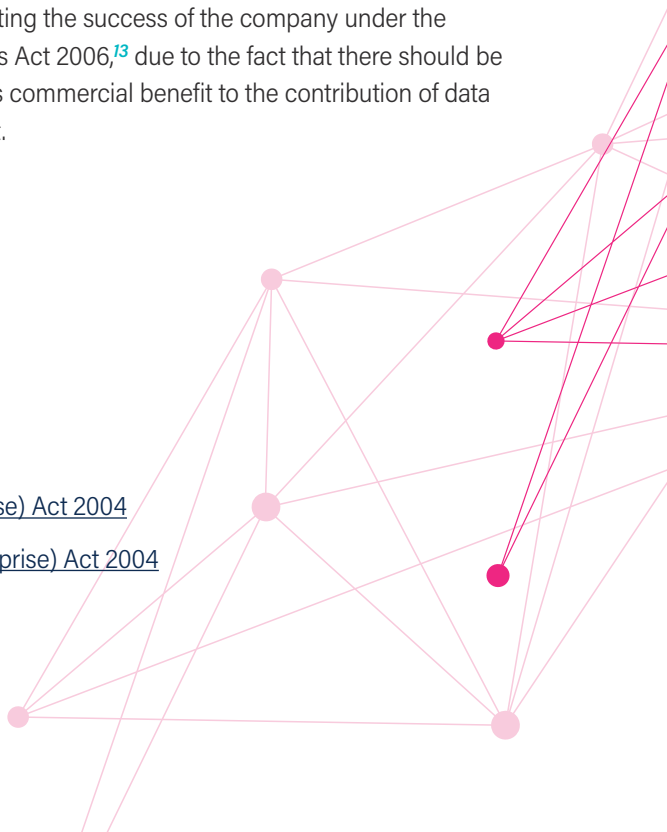
For all of the above commercial data sharing arrangements, they all rely on the premise that, if an organisation is not part of the data sharing arrangement then they will not receive the benefit of it. This is one way of ensuring compliance with a mutually agreed set of data trust rules, without having a specific prosocial purpose of way of working either baked into the data trust's articles of association[9] or in the form of a CIC,[10] if the corporate form of a data trust is followed.

As a commercial body, the CIC model would be wholly inappropriate for a structure owned by primarily profit-making institutions as the CIC would require the data trust to prove to the Office of the Regulator of Community Interest Companies the CIC is pursuing a community minded prosocial purpose,[11] which a commercial data trust is unlikely to have. A purpose such as the free-sharing of data would unlikely to be sufficient if it were for a purely commercial end or where it would have to be caveated with restrictions on who could access data, in the interests of commercial sensitivities. More suitable, would either be a model such as a Limited Company (LC) with contributors to the data trust either holding shares or a key representative group of stakeholders being shareholders, or as a Company Limited by Guarantee (CLG), with stakeholders contributing to the data trust being members. Either form could be relevant as any recompense that might be given to data providers for contribution of their data to the trust, could be returned to the providers through provisions in the agreement licensing their data to the trust. An organisational method would still be best in this instance due to the expediency of having a central body that can be made up of various stakeholders, and the balance of decision making between organisations of potentially differing levels of authority.

Commercial organisations looking to share data would benefit generally from having a data trust model over any other type of data sharing arrangement. By centralising the data sharing decision making process and concentrating it into a small number of individuals, this means that decisions can be made much more simply and quickly on behalf of all the corporate actors, improving efficiencies and transparency and thereby decreasing distrust. It is the reason why a company is a more efficient vehicle for many individuals working towards a common purpose, than to let all the individuals try to make decisions themselves without guidance. It would also be possible for individuals to be able to contribute their data to the data trust so that their data could be used by the commercial actors but with some return to individual data providers, should that be a possible model that the commercial organisations would wish to implement.

It might be possible that commercial organisations would wish to benefit from the information shared by the data trust without contributing data. A commercial data trust could either address this in the way that Swift does,[12] in that if you are not part of the data trust you do not receive the benefit of it, or by allowing access but actors will have to pay for the privilege.

If the organisational form is followed, there should not be issues around questioning whether its directors are promoting the success of the company under the Companies Act 2006,[13] due to the fact that there should be an obvious commercial benefit to the contribution of data to the trust.



9 S.21 of the Companies Act 2006

10 S.36A of the Companies (Audit, Investigations and Community Enterprise) Act 2004

11 S.45 – 48 of the Companies (Audit, Investigations and Community Enterprise) Act 2004

12 https://www.swift.com/about-us/community/swift-shareholding

13 S.172 of the Companies Act 2006

Commercial Organisations Compliance with Trust Rules

One potential legal issue would be ensuring compliance with the agreed upon trust rules. Whereas with the GLA and RBG pilots, if the adopted structure took the form of the CIC there is both the regulator who could ensure some measure of compliance with ethical data trust sharing but also the general reputational pressure to comply for the GLA and RBG, as public organisations. Commercial organisations running a data trust through an LC or CLG would not have such pressures. There would likely be a modicum of pressure from the public to comply with ethical data sharing as there is always public interest whenever there is a scandal involving big business, but businesses are less affected by the sway of public opinion as negative press can be the norm for some commercial organisations. Additionally, commercial organisations, as both perpetrators or victims of abuses of the data trust rules, would be reticent about making such failings public, due to a combination of embarrassment and the potential to shake shareholder and creditor faith in the organisation. External organisations such as the Chartered Trading Standards Institute[14] are too broad in scope to ensure compliance with specific data trust rules and the ICO has a focus that is more oriented towards data protection than any standard of data sharing.[15] There is therefore no real regulator currently that could subsume the position of ensuring compliance with data trust rules. This is a role that an NGO with expertise in this area could fulfil. Additionally, as the corporate organisational structure of a data trust will likely be followed, provisions in the articles of association for the trust can be put in place to ensure that the directors, who will manage the day-to-day operation of the trust, must act in a certain way that promotes the sharing of data fairly for the benefit of its commercial data providers.

Most likely, compliance and enforcement of data trust rules will have to come primarily internally and through self-regulation, due to the likely general opaqueness of a commercial data trust to any outside organisation. Certainly, a commercial data trust could benefit from having good data sharing rules certified, and the threat of having the certification removed should the rules not be enforced would motivate the data trust to enforce any breaches. Rather, the carrot-stick method by which the data trust can ensure compliance with the trust rules is that if a commercial organisation is found to be in breach then its access to the data trust could be suspended either while the breach is being investigated or as a form of punishment for breach of the trust rules. If being part of the data trust constitutes the provision of a commercial benefit to the commercial organisation, such a threat should ensure that good data sharing practices are followed. As mentioned above with the example of Swift, if the commercial organisation is not going to follow good practices and therefore be part of the data trust it will not reap the benefits.

Also, having a fair dispute resolution process that provides a resolution to a dispute without being overly confrontational and therefore which supports a continued data sharing arrangement after the dispute has been resolved, is important. A dispute resolution board, as discussed in the general legal report could facilitate this, at least in the initial stage. Given the rising cost of litigation and arbitration, these would be expensive and time-consuming processes to resolve a dispute, and whilst any dispute is ongoing, the parties to it would likely be suspended from the data trust to protect themselves and the other data providers. It would therefore be in both organisations' interest to resolve the matter swiftly and in a cost effective manner. If the matter is completely intransigent though, there is the option for the matter to be taken to court to have the issue resolved in a binding manner. Provided that the dispute resolution board is seen to make fair decisions, by ensuring that the board is made up of independent third parties with no stake in the data trust, this could be an effective method to ensure that commercial organisations align themselves with the agreed upon rules on data sharing.

14 https://www.tradingstandards.uk/

15 https://ico.org.uk/your-data-matters/

Competition Law Issues

A data trust that solely involves commercial actors and for a commercial purpose will have to ensure that it does not fall foul of competition law issues, for example the prohibition on conducting themselves in such a manner that amounts to a cartel.[16] If, for example, there are information exchanges between commercial organisations in the same sector that improve efficiencies between organisations then this is a positive outcome if the consumer or end-user will ultimately derive a benefit. If, however such information exchanges facilitate a structure where price fixing, market sharing or limiting outputs or sales occurs, amongst other forms of cartel activity, this amounts to an offence under competition law.[17] Additionally, if large key commercial organisations from the same sector control who can join the data trust and prevent smaller competitors from joining and thereby obtaining the possible competitive benefits that are there by being part of a data trust, then this could be seen as a practice limiting competition and the commercial organisations could be guilty of a cartel offence.[18]

To avoid falling foul of this offence, commercial organisations that form part of the data trust will need to ensure that they do not accidently indulge in any price-fixing through the sharing of commercially sensitive information,[19] that could affect the market sector and influence decisions by the large actors that form part of the data trust but that small competitors not part of the data trust would not have access to and therefore which could put them at a competitive disadvantage. The nature of the data trust arrangement and who is party to it will affect whether it is viewed as anticompetitive by the Competition and Markets Authority.[20]

Other Issues to consider

The applicable GDPR considerations will be the same for a commercial data trust as they will be for all other forms of data trust. For example, particular care will have to be taken if any employee or customer data is shared, as this will be classified under the definition of personal data within the GDPR[21] and therefore will likely need consent to be shared.[22]

Although entities such as TeX, Swift and Bolero (all referenced above) exist, that allow for dating sharing of specific standardised forms of data within certain circumstances, the aim of the data trust will be to allow for sharing of non-standardised data in a way that ensures security in the minds of the data providers and which can be adapted to any data sharing scenario. By having the storage of data centralised this would facilitate greater levels of data sharing. However, should the commercial actors so chose, there could also be a situation where the data trust itself does not store data, but acts as a register of what data is available and interested parties will seek data from each other on an as-needed basis. This scenario, whilst not the ideal of a data trust, reflects a potential commercial reality where organisations would wish to have some control over who can access data (yet being careful not to fall foul of competition law).

There could, for example, be a situation where a data trust is established as something similar to a special purpose vehicle company[23] and data is shared between specific partners for the life of a particular project and where each instance of data sharing between the parties is compartmentalised for the particular requirement for which the data is needed.

16 https://www.tradingstandards.uk/

17 https://ico.org.uk/your-data-matters/

18 https://www.tradingstandards.uk/

19 https://ico.org.uk/your-data-matters/

20 https://www.tradingstandards.uk/

21 https://ico.org.uk/your-data-matters/

22 https://www.tradingstandards.uk/

23 https://ico.org.uk/your-data-matters/

Charity Data Trust

At the opposite end of the spectrum to a commercial data trust, lies a charity data trust. This would encompass a situation where either the data trust is in itself a charity with, exclusively, charitable objectives, or it acts as a data trust that shares data between charities who make up the data providers and data users.

In all likelihood, such a data trust will be one and the same; however the distinction should be made as one could very much exist without the other. A data trust which is a charity itself, in purpose and not necessarily organisationally, would be able to receive data licensed to it from a variety of sources, be they individuals or commercial organisations, and put that data towards its charitable purpose. The organisational structure could be in the form of an LC, CIC, CLG, LLP or Charitable Incorporated Organisation (CIO). In terms of the LC and LLP, these forms would seem ill-suited to an organisation whose primary objectives are charitable for the same reasons they were not felt appropriate in the general and pilot specific reports; namely, that they do not have an inherently charitable or prosocial purpose built into the organisational governance so do not engender the level of trust or oversight that would be needed to provide public assurance that its intentions are pure. This is why registered charities have a regulator in the form of the Charity Commission[24] and a CIC has as its regulator the Office of the Regulator of Community Interest Companies.[25]

A CLG is also an option, with key stakeholders being members of the CLG and its Articles specifying the charitable purpose which should be pursued. The great advantage of a CLG is that, as it does not have share capital,[26] there is no way to return revenue generated to shareholders through the structure of the company and therefore it is not seen as a profit making institution; it is for this reason that it is the preferred form of legal entity for think tanks, societies and clubs.

The Articles could be amended to state that a prosocial pursuit should be followed; however, there is always the possibility that the Articles can be amended if a 75% majority of the members of the CLG[27] so wish. If a data provider has gifted its data (probably by giving an indefinite and possibly irrevocable licence to the data trust), it would not want the members of the CLG to vote to revoke the prosocial purpose contained within the Articles and then suddenly start using its donated store of data for purely commercial ends, such as targeted advertising, with no method of recourse from the data providers. Thus, it may be prudent for a key data provider to be given the right to become a member of the CLG, to mitigate this risk.

A charity must, of course, be completely transparent to ensure trust by all of those interacting with it. Thus, a legal form that has an external regulator to ensure that the data trust abides by its inherent prosocial purpose will be important to prevent the Trust from changing direction from its charitable purpose towards being a commercial organisation or one that wishes to exploit the data for a purpose other than that which was understood by its donors.

A CLG can be registered as a charity or a separate Charitable Incorporated Organisation ('CIO') can be set up, both of which are regulated by the Charity Commission. A CIC also has a separate regulator and needs to abide by the prosocial purpose stated upon its incorporation; otherwise the regulator can enforce compliance with the objects for which it has been established.

24 https://www.gov.uk/government/organisations/charity-commission

25 https://www.gov.uk/government/organisations/office-of-the-regulator-of-community-interest-companies

26 S.5 of the Companies Act 2006

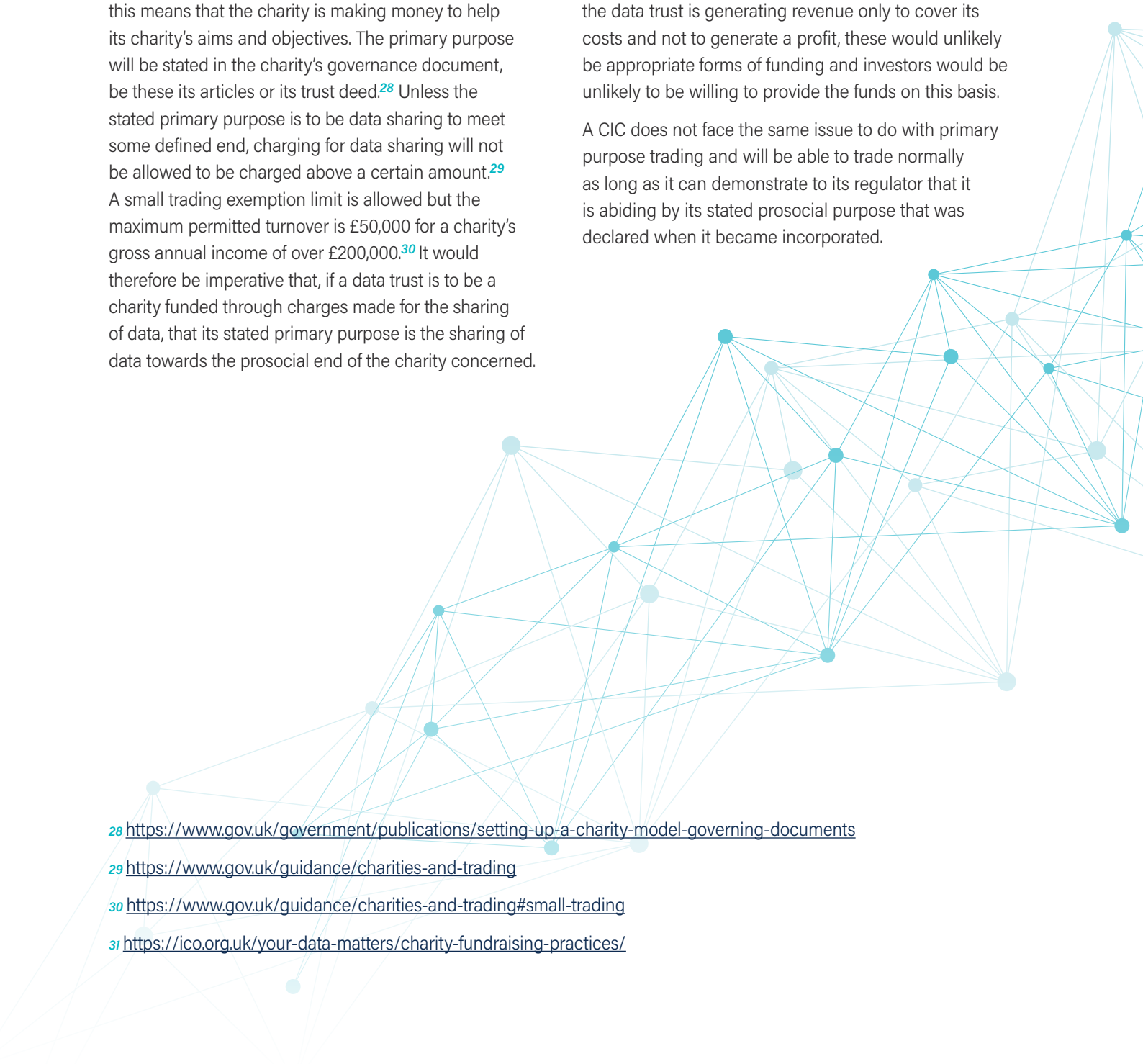
27 S.21 of the Companies Act 2006

Funding

In the general legal report, and the pilot specific report for RBG and the GLA, there was a suggestion that the data trust sustain its infrastructure. This could come in the form of data storage (which might not be relevant depending on the trust structure), the dispute resolution board and the board managing the data trust's everyday decision making, through charging for access to data, either as a flat rate or on a per-access basis. Organisations regulated by the Charity Commission (i.e. registered charities and CIOs), can generate revenue as long as it is classed as "primary purpose trading"; this means that the charity is making money to help its charity's aims and objectives. The primary purpose will be stated in the charity's governance document, be these its articles or its trust deed.[28] Unless the stated primary purpose is to be data sharing to meet some defined end, charging for data sharing will not be allowed to be charged above a certain amount.[29] A small trading exemption limit is allowed but the maximum permitted turnover is £50,000 for a charity's gross annual income of over £200,000.[30] It would therefore be imperative that, if a data trust is to be a charity funded through charges made for the sharing of data, that its stated primary purpose is the sharing of data towards the prosocial end of the charity concerned.

Any charitable data trust would otherwise have to be funded through more traditional charity funding methods such as donations and grants, which in itself can raise data protection issues around marketing to donors. A data trust raising funding via donations would have to be particularly sure of how it handles such data that is used for marketing, and that there is a clear divide between data that is provided to the trust for charitable data trust purposes and data that is permissible to be used for marketing.[31] Equity and debt funding would technically be available but given that the data trust is generating revenue only to cover its costs and not to generate a profit, these would unlikely be appropriate forms of funding and investors would be unlikely to be willing to provide the funds on this basis.

A CIC does not face the same issue to do with primary purpose trading and will be able to trade normally as long as it can demonstrate to its regulator that it is abiding by its stated prosocial purpose that was declared when it became incorporated.



28 https://www.gov.uk/government/publications/setting-up-a-charity-model-governing-documents

29 https://www.gov.uk/guidance/charities-and-trading

30 https://www.gov.uk/guidance/charities-and-trading#small-trading

31 https://ico.org.uk/your-data-matters/charity-fundraising-practices/

Data that is donated to the trust

In the context of a charity, assets are usually donated to be used for the charity's intended purpose. As previously mentioned, data is not an asset that is capable of being donated.[32] It would therefore be impossible for a data provider just to give over their information to the data trust. Additionally, unlike with money that has no sentimental or personal value beyond its monetary worth, data is more personal; it is thus possible that a data provider may be identified by the data which they have contributed to the data trust. Consequently, a data provider will also likely want to retain some measure of control over the data even once it has been "donated" to the trust, to ensure that it is not misused or to prevent any negative effect from rebounding onto the data provider.

Within other data trust contexts, it has been concluded that data will be licensed for the use by the data trust, with terms being contained within the license that will dictate how the data is used. A similar approach could be used for data being provided to a charitable data trust with a slight tweak. The license providing data to the trust would likely be much broader than a license in any other context because people wish to contribute towards prosocial goals but would still be limited as the public are generally more reluctant to donate their data to charities compared to companies following various high profile abuses of data use by charitable bodies.[33]

Again, the licensing model assists with this as the data provider will still be able to maintain a measure of control over how the data is used, thereby ensuring that they are more broadly protected from any misuse by the data trust. It is unlikely that an open-ended license to a charity of data would attract any kind of tax relief for charitable giving,[34] as such relief relates to gifts of money, land, property or shares or plant and machinery.[35] These are all physical assets where it is easy to ascribe a monetary value. Specialist tax advice would be required to see if a gift of the benefit of a license of data could qualify for charitable giving tax relief, but it would seem unlikely.

It is likely that data providers would wish to have provisions in the relevant license, stating that they can revoke the license, either at will or on certain conditions being met. As data providers would be contributing their data for free, the former is more likely. A charitable data trust will thus need clear provisions to prevent misuse of data. As data providers will not receive a pecuniary benefit a willingness to revoke the license of their data is much more likely, if they are in any doubt about the way it is being utilised. Such controls within the data license will also restrict with whom the data is shared whether it be other data trusts looking to share data for a common goal or third parties who can contribute to the goals of a data trust.

32 Oxford v Moss [1978] 68 Cr App Rep 183

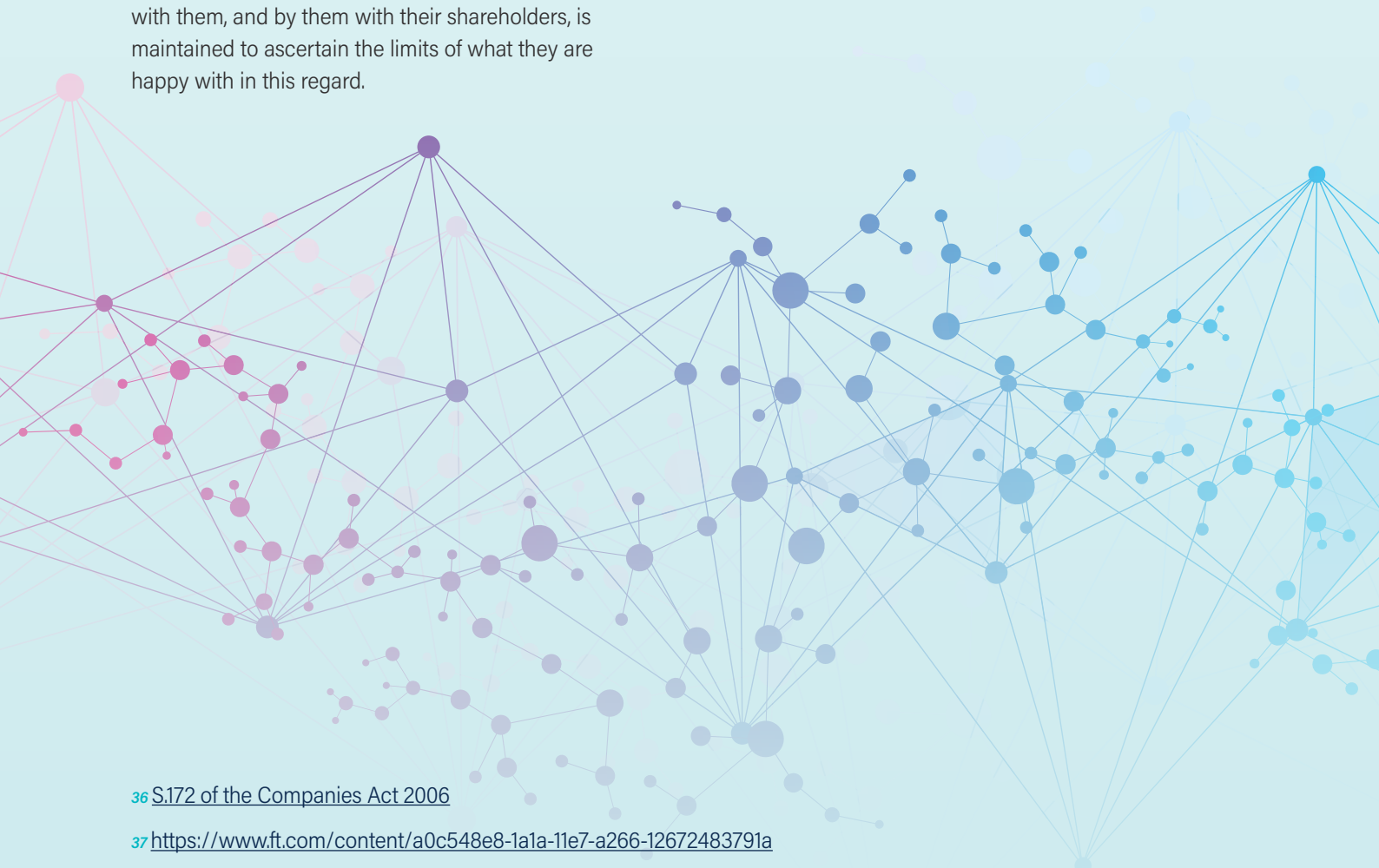
33 https://www.thirdsector.co.uk/tenth-public-would-share-data-charity/fundraising/article/1492206

34 https://www.gov.uk/donating-to-charity

35 S.63(2) Capital Allowances Act 2001

If a corporate or profit making institution is licensing its data for free to the data trust, if the funding model is not being followed where the data provider is paid for providing its data, it would have to justify that it is acting in a way that is promoting the success of the company when it contributes the data.[36] In addition, as there is likely to be no tax relief for "gifting" data to the trust, a company data provider will not be able to justify providing data by reference to any tax relief. Rather, providing data to the Trust would be an activity that is justified as being in accordance with a company's Corporate Social Responsibility policy. However, if shareholders do not support this, perhaps because the data being provided is inhibiting the ability of the company to function, it would be difficult for the directors to justify this activity to the shareholders, thus limiting a company's willingness to contribute data to the trust. Largely this will depend on the appetite of Company directors and ensuring that engagement with them, and by them with their shareholders, is maintained to ascertain the limits of what they are happy with in this regard.

Although this section has focused primarily on how a data trust acting as a charity would operate, there is also the possibility of charities having a data trust and sharing information between themselves, perhaps towards a common goal given the large number of charities that have overlapping purposes. Sharing of data in this context could help smaller charities flourish by sharing resources and could help to ensure that there is no duplication of effort if approaches are shared. Such a data trust will operate in the same way as it would in any other data trust context and there would not need to be any other special considerations for such a data trust. Charities will have to ensure however that their sharing of data in such a way remains legally compliant; there have been many fines for charities sharing donor lists with one another,[37] without consent, or using donor information to profile them to see if they could afford more donations.[38]



36 S.172 of the Companies Act 2006

37 https://www.ft.com/content/a0c548e8-1a1a-11e7-a266-12672483791a

38 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/04/ico-fines-eleven-more-charities/

Public Sector Data Trust

Whilst the above two data trust use cases reflect how some forms of data trust would operate within the private sector, the RBG/GLA specific pilot demonstrated that there is an appetite within the public sector for better data sharing arrangements. This is both to help improve services and operations by maximising already stretched resources, and also to assist in opening up new areas of activity within which the government can operate.

Such a data trust could cover the sharing of data across governmental bodies in addition to cross sector data sharing arrangements with the overall beneficiary being the government and, by extension, the public.

There would be no prohibition on having a public body set up its own data trust in the form of a CIC or other CLG, say through the allocation of some government funding. What is unique about a public data trust would be any issues around providing data to the trust.

Current data sharing and providing data to the Data Trust

There is already some guidance in place for data sharing between public bodies. Government bodies are already encouraged, in Labour policy documents,[39] to share resources through data sharing as a way of improving efficiencies and optimisations. Data sharing is permitted where there is an express statutory power allowing it, such as under the Crime and Disorder Act 1998,[40] the Anti-Terrorism, Crime and Security Act 2001[41] or the Immigration and Asylum Act 1999. Whether there is a statutory power permitting the sharing of data will entirely depend on the public body concerned; a specific review of each body that this power is available for would be needed together with a consideration of what data is looking to be shared. This analysis falls outside of the scope of this report, given the breadth and variety of public bodies in existence.[42]

If there is no express or implied power, where there is no express prohibition or permission and the data sharing is reasonably tangential to a legitimate activity, a government department may be able to rely on common law powers to share. These state a government department, headed by a Minister of the Crown, has the same powers as any legal person, regardless of statute. This "Ram Doctrine" has however had unfavourable treatment by Parliament, has not often been tested by the courts and would likely face difficulty should a government body try to rely on it.[43]

39 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272244/6683.pdf & https://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf

40 S.115 of the Crime and Disorder Act 1998

41 S.17 of the Anti-Terrorism, Crime and

42 https://www.gov.uk/government/publications/identity-document-validation-technology/supplementary-guidance-public-sector-data-sharing-for-prevention-and-detection-of-crime

43 https://publications.parliament.uk/pa/ld201213/ldselect/ldconst/165/16506.htm

Additionally, because individual data held by government bodies is sensitive and gathered by necessity due to the government body's role that it is fulfilling, there are often specific rules and legislation that govern the holding and sharing of data. Each department will have its own such regulations in relation to such data sharing unique to it. A particularly stringent example is HMRC, which has very specific rules in relation to data holding and sharing. HMRC has wide ranging powers to gather information from tax payers and third parties[44] and other bulk data gathering in general.[45] Requests are made in the form of notices for information, either formally or informally.[46] The gathering of such information is limited in scope though as information can only be requested so far as it is "reasonably required"[47] for checking a person's tax position and not if the document requested is over six years old from the date the request was made.[48]

Evidently, information gathered in this way can only be used for the reasons it was gathered under the primary legislation. To use this information for any additional purpose, such as sharing with a data trust, would be in breach of this legislation, so not possible. Similarly, holding the data beyond the time for which it was needed is not possible. If HMRC, and any government body that had gathered data involuntarily under primary legislation, wished to use such information they could request data from a data provider outside its powers under the Finance Acts, and therefore with the complete consent of the individual.

Currently, as gathered from interviews with RBG, any data sharing is carried out on an ad hoc basis and for a specific purpose, in part due to a fear that the body (in this case of RBG) would be in breach of the law by doing so. In the case of personal data, there is general reluctance to share this due to the public's heightened awareness of public bodies trying to share data in a way that could in any way be construed as being illicit. Thus, there is a heavy reputational risk but also impediments due to the Data Protection Act 1998 now updated by the Data Protection Act 2018 which implements GDPR. Under this, personal data garnered shall be adequate, relevant and limited to what is necessary.[49]

Additionally, personal data which identifies individuals can only be stored for no longer than is necessary for the purpose the data is processed.[50] In a private sector data trust this requirement could be met by the individual consenting during the gathering of the data.

Publicly gathered personal data is generally obtained without individuals having seen a consent form. It would be possible to integrate into the letters from the council or in forms from the NHS, provisions that would let data be shared if individuals give their consent, as long as the purpose for which it was being contributed to the data trust is carefully scoped. The other, far easier, way is to have the data anonymised effectively; it therefore falls outside the provisions of GDPR[51] and any provisions of the Human Rights Act 1998.[52] This could still be useful to the government in calculating statistical trends. Anonymising the data though would make it much more difficult to cross-refer different data points held by different departments to calculate population trends. In addition, given the number of data points held by public bodies about an individual, care would have to be taken so that, when these data points are cross-referred, an individual does not suddenly become personally identifiable and therefore subject again to the said legislation. This is particularly important if a form of double-blind anonymisation is used, where an individual's name is replaced by a reference number.

44 Schedule 36 Finance Act 2008

45 Schedule 23 Finance Act 2011

46 HMRC Compliance Handbook CH21150

47 Barty Party Co Ltd v HMRC [2017] UKFTT 697 (TC) (20 September 2017)

48 Paragraph 20 of Chapter 9 of Finance Act 2008

49 Article 5(1)(c) of GDPR

50 Article 5(1)(e) of GDPR

51 Article 4(1) of GDPR

52 Article 8 of the Human Rights Act 1998

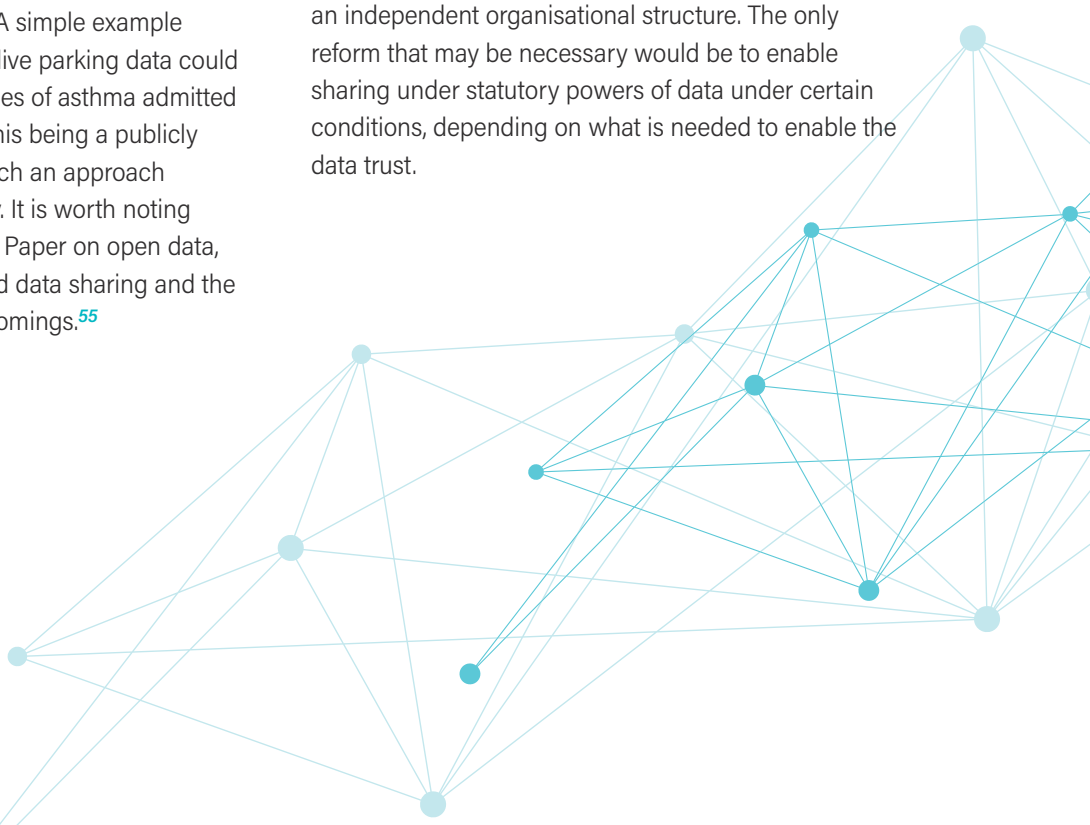
Data Trust potential

The appetite for such a government-wide data trust, would need to be determined through a government consultation process. As previously noted, sharing data between government bodies tends to be quite limited as each body tends to silo its own data for its own benefit.[53] The aim of having a data trust with centrally held information would be to facilitate easy sharing of data across government bodies for a given purpose. Probably more likely, both practically and to assuage people's fears that, for example, their public health data will not be provided to crime prevention agencies, would be sector or project specific data trusts; these can have a specific stated purpose that would be both something an individual could support but that would also more likely to satisfy GDPR requirements that data is held for a specific purpose,[54] which the data trust could scope when individual or organisations consent to the use of their data. A simple example would be one where a council's live parking data could be cross referred against instances of asthma admitted to a hospital. The advantage of this being a publicly driven initiative would be that such an approach could be implemented nationally. It is worth noting that the Government in its White Paper on open data, recognises the value of increased data sharing and the Government's associated shortcomings.[55]

The private sector driven Consumer Data Research Centre is a platform where private institutions contribute to the organisation data that is public, that is private but not sensitive or that is private and sensitive. This data is then shared with approved research partners, sometimes through an app only to ensure there are no data breaches of private sensitive data.[56] Such an approach could be similarly attractive to boost innovation within the UK if the wealth of public data was provided to researchers and innovative businesses.

It should be highlighted that, as a public body, there is no need to justify its actions to shareholders or other stakeholders beyond the public and the need to abide by legislation.

There should also be no need to enact any law reform in order for there to be a publicly run data trust as an independent organisational structure. The only reform that may be necessary would be to enable sharing under statutory powers of data under certain conditions, depending on what is needed to enable the data trust.



53 https://webarchive.nationalarchives.gov.uk/20150603223548/https://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf

54 Article 5(1)(c) of GDPR

55 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf

56 https://www.cdrc.ac.uk/partners/

Hybrid Data Trust

A hybrid data trust has already been considered in some depth with regard to the use cases specified within the pilot specific report for Pilot 1. The recommendation and analysis are, however, specific to those use cases, while the concept of a hybrid data trust has the potential to bring together prosocial purpose of the public sector with some of the streamlined approach of the private sector.

One particular instance referred to by the Smart Cities Strategist for Digital Greenwich, was to use the sharing of data to tackle the resource limitations and inefficiencies of the social care sector. Beyond just the care sector though there are several quasi-public sector areas where a hybrid data trust could provide value, for example healthcare or the prison system.

Generally implementable other forms of Hybrid Data Trust

There is no reason why the model of a data trust that is implementable within RBG, could not be implemented in the other 32 London boroughs as there is nothing unique about what RBG offers. Other councils outside London could operate their own data trusts and would not have to share across multiple administrative areas, as with London and its borough system. The same legal structure as recommended in the Pilot 1 legal report would also be appropriate within these contexts because the governance structure of a council, the potential commercial actors and the views of individual constituents are likely to be the same.

The potential for hybrid data trusts is thus numerous. Dependent on the sector and purpose they could face different challenges. Below are three key sectors that are data rich and have perceived large levels of inefficiencies; these have been focused on as they might benefit from a data trust.

Care Sector

As discussed, the Smart Cities Strategist sees the transport and energy use cases although, in themselves, important, as limited in scope and not a priority in terms of where councils should be focusing their attention. He suggests that potential benefits within the care sector include sharing information to support the 11,000 volunteers who operate in RBG or by providing a job board equivalent to help place elderly care patients in facilities appropriate to their needs and interests. The first suggestion, depending on the arrangement, could be dealt with without the need for a data trust; however, with the second it could potentially be useful. It could be overlaid with the Care Quality Commission's own website of information that tracks care ratings for residents' homes.[57] It is worth noting that data sharing within the care sector already occurs, specifically between the healthcare and social care sectors.[58] This however is covered by simple data sharing agreements; a data trust will seek to assure individual data providers that their data will be used in an ethical manner, as enforced, in the case of a CIC, by its regulator.

Given the blend of council and local social care private organisations, a CIC form of data trust would still likely to be optimal so that some value can be returned to individual data providers, but also so that the CIC is bound to abide by its stated prosocial purpose. This is of particular relevance given the general prosocial aims of the care sector and why a LC form would be less appropriate. For example, it seems unlikely that any distributions would be made in the form of dividends, either within the CIC or LC, or through the license, as the goal of a data trust within the care sector would be to improve inefficiencies for the benefit of all data providers. Thus, rather than any private business having to receiving payment for access to its data, it would be seeking to receive a benefit in kind or even provide a contribution to the continued running of the data trust.

Any data trust within the care sector will have to deal with individuals' personal and sensitive data, with those individuals being particularly vulnerable. In this context too, anonymised data is likely not to be as useful as specific individuals will need to be identified in order for recommendations for their care to be made to them. This is different to the GLA and RBG pilot where trend data can be cross referenced and great control exists over what data commercial organisations give to the Trust. This means that individual's data will be subject to GDPR and almost certainly include information that falls under the definition of a special category of personal data (e.g. racial or ethnic origin, health data or potentially biometric data) which have more strict controls on their handling.[59] There are various provisions under which processing of such sensitive data can occur; however; it is recommended that explicit consent is used[60] to ensure maximum engagement. Consent from the elderly whom no longer have capacity, or from foster children who have no relative to give consent on their behalf, can have consent provided by a third party who has authority to give consent on their behalf. This advice is from the ICO as the GDPR is silent on this point.[61]

57 https://www.cqc.org.uk/help-advice/help-choosing-care-services/map-service-ratings-across-england

58 https://ico.org.uk/media/for-organisations/documents/1625861/data-sharing-code-of-practice-additional-case-studies-201701.pdf

59 Article 9(1) of GDPR

60 Article 2(a) of GDPR

61 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

Prison Sector

Sharing prisoner data is another controversial and sensitive area where a data trust could potentially benefit the ecosystem. There has been a suggestion by the think tank, "Reform" that data from prisoner records, cross referenced with healthcare data and social care data, could be used to prove a more comprehensive picture of the needs and history of the homeless and make any intervention more effective.[62] Whilst it is outside the scope of this report to comment on whether sharing such data so broadly is ethical or effective, this section addresses any issues specific to the prison sector. Other possible uses for a prison specific data trust would be to share approaches around how prisons solve mental health issues and which are successful or prisons could share real-time information between one another of crimes committed within the prison as an indicator of how drugs or other contraband are being brought into the prison. Whilst overcrowding is likely not something a data trust could directly help tackle, if prisoner data is made available to researchers who could review for factors that contribute to recidivism or that show a propensity for offending in the first place, approaches could be collaboratively developed to tackle these problems. The latter does not necessarily have to involve creating a new data trust but could involve contributing data to another trust.

The National Offender Management Service already has a data sharing policy that applies to all prisons and to the National Probation Service, in addition to their own operation.[63] The policy covers the different types of data sharing arrangement available. If a data trust were to be included within the prison sector, this policy would need to be amended to include allowing data to be licensed to the data trust. The processing, collection and retention of prisoner data is permitted in the opinion of the Ministry of Justice under GDPR for electronic monitoring[64] and, by extension, prisons meet all the same requirements of the principles under GDPR, i.e. the retaining of such data is needed to meet a prison's requirement under law.[65]

The most significant issue to face a data trust where prisoner data is shared is that any kind of consent from the prisoners themselves to data being shared is highly unlikely. Consent has been suggested as the primary way by which both compliance with GDPR provisions can be secured and to enable greater levels of engagement with the data providers, here being prisoners, to ensure there is no resentment to data being shared without their consent. Whilst the resentment of prisoners is something the public are likely to have little sympathy for and they cannot prevent the prison from collecting their data in the first place, the real stumbling block would be GDPR and human rights provisions.

62 https://reform.uk/sites/default/files/2018-11/Data in the Public Sector_WEB.pdf

63 https://www.justice.gov.uk/downloads/offenders/psipso/psi-2016/psi-16-2016-pi-15-2016-information-sharing-policy.pdf

64 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/756230/code-of-practice-electronic-monitoring.pdf

65 Article 6 and Article 10 of GDPR

The GDPR issue is that, if there is no consent to the data processing and therefore sharing, the prison would have to rely one of the other conditions under which data can be processed. There is no contract being processed[66] therefore data cannot be collected under this provision; the "vital interest" condition[67] is construed by the ICO as the data processing being necessary to protect someone's life,[68] which would unlikely to be relevant here. The legal obligation provision[69] would cover the collection of data but not its sharing as there is no statutory provision that would require the sharing of data in the contexts suggested above where a data trust might be useful. The public interest condition[70] to the processing of data may be relevant as the administration of justice[71] is one suggested category that falls under this condition; however, the public interest condition is construed very narrowly. Most likely to be relevant would be the "legitimate interest" condition.[72] Whilst, because a data trust is a new thing, so it has not been tested whether such suggested data sharing would be captured by this condition, if the data sharing was to improve prison services and address misconduct, it is likely that such data sharing would be permitted. In addition, as referred to above, the National Offender Management Service already has a policy related to data sharing that seems to meet the provisions implemented under GDPR (despite being drafted prior to this legislation coming into effect).

Equally, whilst a prison should be aware of having respect for the privacy of its prisoners' personal life,[73] this is a qualified right. Thus, the legitimate sharing of prisoner data in a careful and secure way in order to improve the conditions and services of the prison would be unlikely to breach this right. It is important that personal data can be shared in this way as anonymised data will be less useful if correlations between individuals' personal details and their actions cannot be calculated; interventions will then be much more difficult. Additionally, whilst researchers could use statistical, aggregated or meta-data for analysis, raw data that can be cross-referred with other sources will likely yield the most useful insights.

66 Article 6(1)(b) of GDPR

67 Article 6(1)(d) of GDPR

68 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

69 Article 6(1)(c) of GDPR

70 Article 6(1)(e) of GDPR

71 S.8 of the Data Protection Act 2018

72 Article 6(1)(f) of GDPR

73 Article 8 of the Human Rights Act 1998

Healthcare Sector

The NHS has already invested money to support increased data sharing arrangements[74] and has a code of conduct for the use of data for the benefit of the NHS.[75] This not only helps within a clinical context but meets the general push that the NHS is making to boost entrepreneurship[76] and capitalise on the unique IP generated within the NHS. A system is in place that allows the sharing of patient records between GPs and other NHS bodies such as hospital trusts, but this is not yet live. The NHS recognises the issues with this and are currently trialling a pilot project[77] where GPs, social care and hospitals will all work from the same patient record.[78] A data trust, supported by a suitable technical sharing arrangement could support such an arrangement in a form similar to that suggested in the public data trust section above. This would build on NHS current policies[79] and toolkits[80] relating to data sharing within the NHS. The NHS should nevertheless be careful as to whom they share data with, even within the public sector, as there was a public backlash when the NHS was found to be sharing patient data with the Home Office for the purpose of tracking immigration offenders and vulnerable people, a practice that they have now discontinued.[81]

A hybrid data trust form could benefit this ecosystem by allowing researchers access to this data to improve innovation. If researches were not from the NHS but from third-party commercial organisations or private research institutions such as universities, a data trust model would be beneficial because the in-built structures would ensure a level of confidence with the data sharing. People are generally happy to share their personal information with commercial organisations if there is a clear patient benefit to doing so and there are suitable safeguards in place.[82] A data trust, in the form recommended in the above contexts and in the RBG and GLA pilot model would likely be most appropriate here too, providing the necessary safeguards and assurances that patients would need to permit their data to be shared with commercial organisations.

74 https://publictechnology.net/articles/news/nhs-digital-commits-C2 A315m-help-data-sharing-between-health-and-social-care

75 https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

76 https://www.england.nhs.uk/ourwork/innovation/clinical-entrepreneur/

77 https://www.england.nhs.uk/wp-content/uploads/2018/05/local-health-and-care-record-exemplars-summary.pdf

78 https://www.gponline.com/gps-share-patient-records-social-care-hospitals-nhs-england-pilot/article/1465658

79 https://www.england.nhs.uk/ourwork/tsd/data-info/data-sharing-and-privacy/

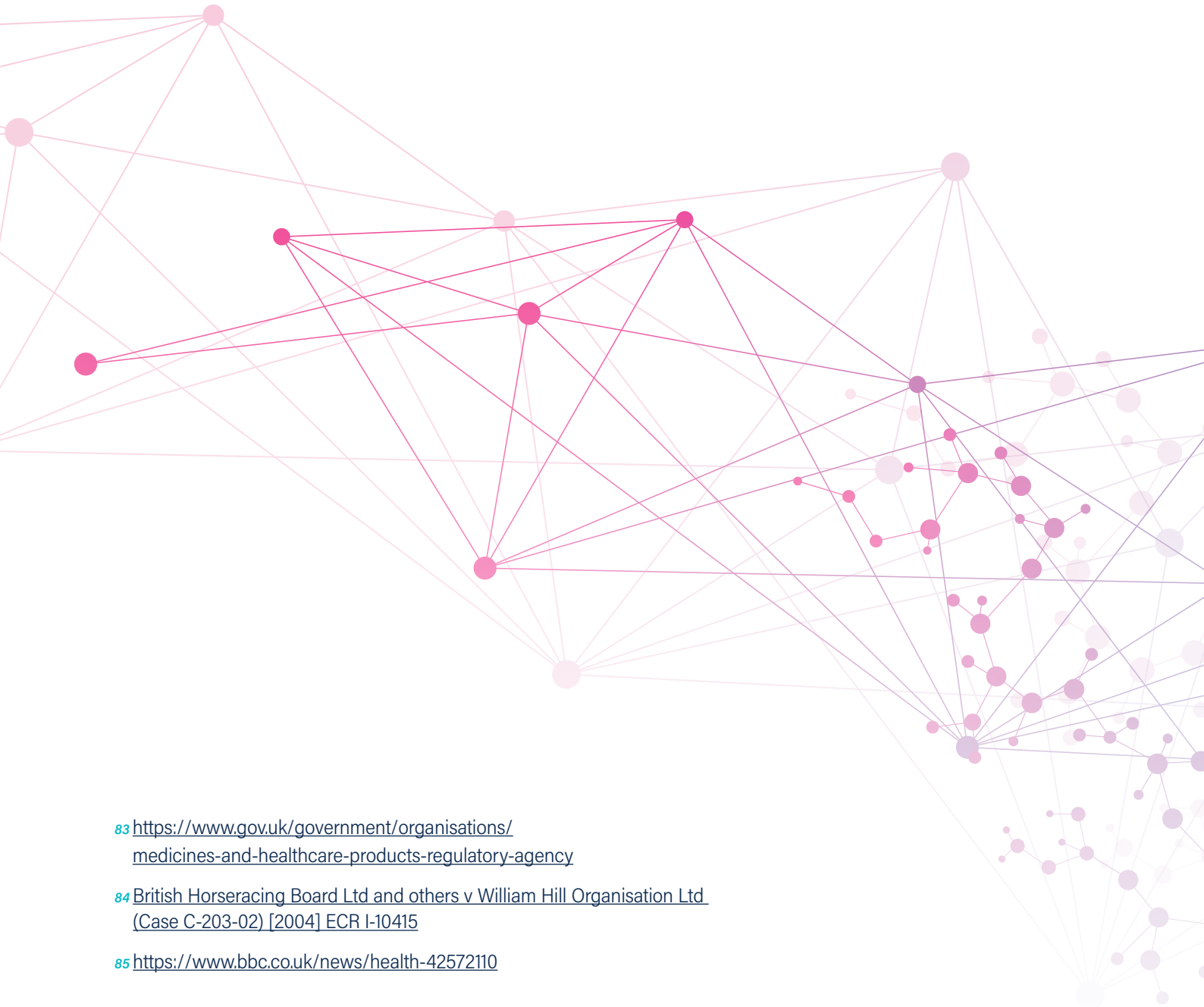
80 https://www.dsptoolkit.nhs.uk/

81 https://www.digitalhealth.net/2018/11/nhs-digital-patient-data-sharing-home-office-end

82 https://www.ipsos.com/ipsos-mori/en-uk/commercial-access-health-data

The potential issue that could, while not necessarily unique to healthcare data trusts, be potentially more relevant is Intellectual Property . Any commercial organisation that builds a product on the back of any healthcare data would potentially wish to have ongoing access to this data for the purpose of calibrating the product or as part of the approval process when submitting a drug to the Medicines and Healthcare Products Regulatory Agency.[83] Key provisions will have to be included in the terms under which researchers have access to the data to ensure that no new database rights are created in the data that might vest in the researchers.

As a significant investment[84] in creating a new database would be required, this is probably unlikely. Researchers must have continued access to the data. If the NHS feel that suitable measures are not being taken to ensure that the data is being handled in a fair way, they could remove the data from the data trust (as long as a provision in the data providing license allowed them to do so). As commercial organisations would potentially be paying for access to the data, the NHS could therefore receive a return on the vast amount of patient data that it holds, thereby helping with the financial issues the NHS has been facing.[85]



83 https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency

84 British Horseracing Board Ltd and others v William Hill Organisation Ltd (Case C-203-02) [2004] ECR I-10415

85 https://www.bbc.co.uk/news/health-42572110

International Data Trust

Whilst a data trust has the potential to be highly effective on a national level to promote data sharing, for it to be a truly transformative concept, it would have to, and be able to, operate internationally. This means not only having international providers but also international data users. Other countries such as Canada are seeking to promote data sharing arrangements;[86] the Canadian population are generally happy for their data to be shared as they are pragmatic about the benefits that can be achieved.[87] Canada has though faced some criticism about its arrangement to share data between itself and EU by the EU's legal advisors.[88] In America, a company is trying to commercialise the concept of a data trust by providing the technological structure to have one in place.[89]

Copenhagen has tried to set up its own form akin to a data trust in the form of its Copenhagen Data Exchange,[90] something akin to a hybrid data trust model that allows sharing of data between private and public sectors. This sought to provide a platform for the commercial selling of data but had a limited uptake due to a combination of an immature market, issues bundling up the data to be sold in the correct format and reluctance to share data with an open data platform due to ethical concerns.[91] These issues provide an example of the issues UK data trusts might face and could be addressed through establishing a use case as an exemplar, having an appropriate technical response and the data trust adopting suitable governance procedures, perhaps supported by certification of the data trust.

86 https://www.genomecanada.ca/en/canadian-international-data-sharing-initiative-accelerate-health-care-innovation

87 https://www.the-cma.org/resource/newsroom/2018/majority-of-canadians-are-ok-with-sharing-their-personal-data

88 https://www.immigration.ca/fr/canada-eu-passenger-data-sharing-deal-infringes-privacy

89 https://brighthive.io/#data-trust-description

90 https://cphsolutionslab.dk/en/news/city-data-exchange

91 https://cphsolutionslab.dk/content/2-what-we-do/3-data-platforms/3-city-data-exchange/1-learnings-from-the-city-data-exchange-project/city-data-exchange-cde-lessons-learned-from-a-public-private-data-collaboration.pdf?1527149474

International Data Providers and Data Users

If a data trust is established within another jurisdiction, local laws would apply so recommendations made with the collective data trust reports would not be relevant. If a contractual data trust model was adopted it could specify that the laws of England and Wales be applicable, therefore the recommendations would be relevant. Equally, for the reasons established in the general legal report, traditional equitable trust law would be just as inappropriate in an international context as it would be nationally. The general recommendation within the pilot report though is that a separate organisational structure is established to which data could be licensed. In order for the recommendations within the collective reports to be relevant this would have to be established within England or Wales; an organisation established in another jurisdiction would, ordinarily, be subject to local laws. Thus, the recommendation as to legal structure, governance, termination of the data trust or any of the other provisions recommended in the general report, pilot specific report and above would remain the same dependent of course on the purpose of the trust and whether there are public or commercial data providers and users involved.

The key difference for an international data trust will be the transferring of the data across borders. Due to GDPR being EU legislation, the restrictions placed on transferring data under this are the same within the UK as they are within any other EU member country. Therefore, the provisions relating to compliance with transferring of data will likely, without commenting on other countries local rules, be the same between EU member countries due to GDPR taking precedent over local laws. It should be noted that the withdrawal agreement[92] with the EU has the purpose of incorporating GDPR into UK law to allow such a process to continue even when the UK leaves the EU. The UK will however become a "third country" (i.e. third-party country) for the purposes of other countries within the EU transferring data to the data trust.[93] The same rules will apply when a data trust is transferring data outside of the UK to a data user outside of the EU.

A data trust would have to ensure that any country within which data is to be transferred, has a suitable measure of protection to be able to handle that data.[94] Some countries with secure provisions in place are referred to as secure under GDPR but, even if the country is not preapproved, data can still be transferred if the agreement permitting the transfer, the data trust rules, has provisions in place to ensure protection.[95] These can include matters like standard data protection clauses in the form adopted by the EU Commission.[96] It will therefore be important before drafting the data

92 The European Union (Withdrawal) Act 2018

93 https://gdpr-info.eu/issues/third-countries/

94 Article 45(1) of GDPR

95 Article 44 of GDPR

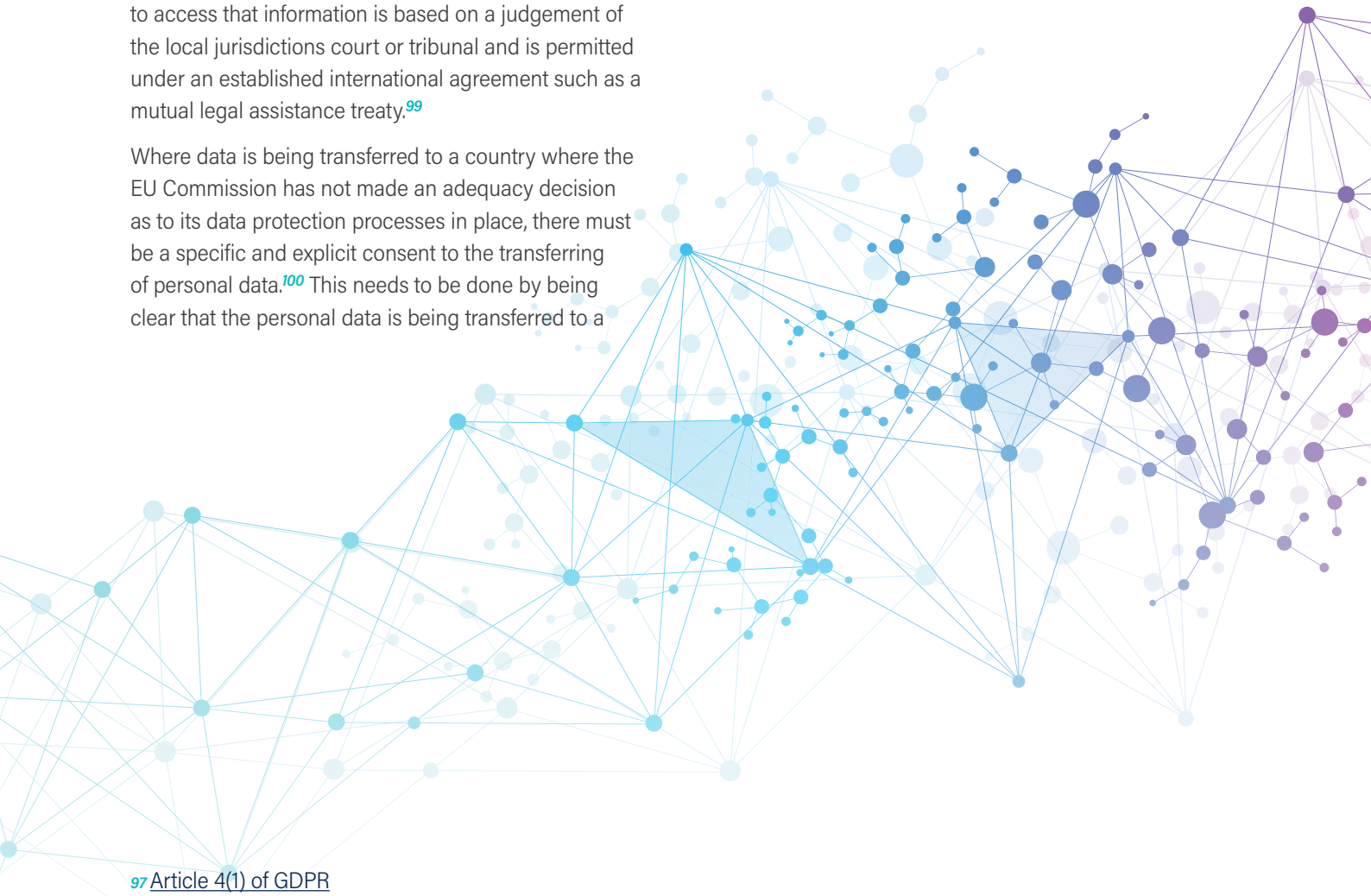
96 Article 46(2) of GDPR

trust rules to think whether there will be potentially any international data users as approved clauses may need to be included in the data trust user terms. It should be noted that the regulations relating to GDPR are relevant only if the data is qualified as personal.[97] This means that aggregated, meta or anonymised data transferred to and from the UK can happen freely and without the special protections that are required if the data identifies an individual personally.

It is unlawful for public authorities in these third countries to access data that is transferred from an EU member to the third country[98] unless the request to access that information is based on a judgement of the local jurisdictions court or tribunal and is permitted under an established international agreement such as a mutual legal assistance treaty.[99]

Where data is being transferred to a country where the EU Commission has not made an adequacy decision as to its data protection processes in place, there must be a specific and explicit consent to the transferring of personal data.[100] This needs to be done by being clear that the personal data is being transferred to a third country where there may not be an adequate level of protection for the personal data in place and this consent must be given positively, either through a signature or by ticking a box.[101]

International data trusts as discussed here are not in and of themselves a new form of data trust. Rather, they are a data trust established in the UK (specifically England and Wales) with an international component by virtue of data being transferred across jurisdictions. For example, water aid charities coordinating between national and transnational partners would be both an international data trust and a national data trust.



97 Article 4(1) of GDPR

98 Maximillian Schrems v Data Protection Commissioner (Case C-362/14) [2015] EUECJ

99 Article 48 of GDPR

100 Article 49(1)(a) of GDPR

101 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

Conclusion

As is explained above, the proposed legal form of a data trust is sufficiently adaptable, with some minor tweaking or extra consideration, to work in a variety of contexts or organisational structures. This is positive, as all sectors can benefit from the sharing of data. In an increasingly competitive, resource-stretched and complex world, all areas can benefit from the operational efficiencies and, ideally, prosocial purpose that is the driving force behind a data trust.

In all cases, with the exception of a purely commercial data trust, a CIC with the stated purpose of the ethical sharing of data would be ideally the best model, subject to the Office of the Regulator of Community Interest companies permitting this as a valid purpose. Failing this, the best structure is a CLG with good data sharing principles built into the trust rules, and the same provisions relating to governance of the organisational body and the dispute resolution board to deal, in the first instance with any disputes. Thus, everything that would apply to the recommended CIC model, but with a CLG used instead of a CIC.

Let's talk

In these pages, we hope we've given you a flavour of how we can help you and your business, regardless of company size or life-stage. To find out how we can support you, please get in touch and let's discuss what would work best to help you achieve your goals.

Rob Bryan
Partner & Head of Science & Technology

01242 248228
rob.bryan@bpe.co.uk

Emily Barwell
Solicitor

01242 248487
emily.barwell@bpe.co.uk

Rupert Parker
Trainee

01242 248222
rupert.parker@bpe.co.uk

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.

BPE Solicitors LLP

St James House,
St James Square,
Cheltenham,
GL50 3PR

Tel: +44 (0)1242 224433
Fax: +44 (0)1452 358138

89 Judd Street
London
WC1H 9NE

bpe@bpe.co.uk
@BPE_Solicitors
bpe.co.uk