ADR UK response to NDS Data: a new direction November 2021

About ADR UK

ADR UK (Administrative Data Research UK) is an Economic and Social Research Council (ESRC) programme funded until September 2026. The partnership is supported by £90 million reinvestment from the ESRC, part of UK Research and Innovation (UKRI).

Its objective is to transform the way researchers access the UK's wealth of public sector data to enable better informed policy decisions that improve people's lives. By linking together administrative data held by different parts of government and making it available to approved researchers in a safe and secure way, we are enabling vital research that has the potential to lead to more effective public services. Our work involves a wide range of themes, from improving education and healthcare to tackling crime.

ADR UK is made up of four national partnerships – ADR England, ADR Scotland, ADR Wales, and ADR Northern Ireland, and the Office for National Statistics (ONS)– coordinated by a UK-wide Strategic Hub. Each partnership is made up of academic and government partners, as well as dedicated secure services through which approved researchers can access de-identified administrative data.

To find out more, visit the ADR UK website.

The below forms our response to the NDS Data: a new direction (November 2021). This accounts for the interests of all ADR UK partners, including those within each of the devolved nations – ADR England, ADR Northern Ireland, ADR Scotland, and ADR Wales – and on a UK-wide level.

General thoughts

Introduction

The proposed changes to the data protection regime are wide ranging and reflect an emphasis on making the most of data opportunities and clarifying areas that have caused uncertainty. There is a focus on driving growth, supporting competition, global operation and unleashing the economic value of data, reducing burdens on business, removing barriers to data flows, and supporting innovation. This approach is encapsulated in many of the proposed changes outlined in the consultation.

Whilst we welcome efforts to provide clarity and reduce uncertainty in a complex area, we endorse the ICO's response to the consultation (*Response to DCMS consultation "Data: a new direction" (ico.org.uk) that the data protection regime needs to work for people as well as for business, economic growth and innovation:

> *Given the importance of data protection to all of us, it is critical that the Government clearly and unambiguously sets out how its proposals would deliver for people, not just for businesses and society as a whole (ICO consultation response 6 October 2021 p10).*

It is also worth highlighting that while the proposals are geared towards providing clarity in a rapidly evolving area, they do amount to very significant changes at a time where organisations are consolidating and embedding their data protection compliance measures following the Data Protection Act 2018 and UK GDPR.

Public trust

In order to effectively unpack how the new proposals can effectively work for people, as well as for business, it is suggested that the UK government effectively and authentically engages with the public about data use, technological changes, and the proposed changes to the data protection regime. This is a complex area and may require a number of different initiatives to ensure there is an effective and open public dialogue about these issues to ensure participation from a broad section of society. This consultation document is of a highly technical and specialist nature that is not geared for a wide public audience. It is important that the public are engaged in this new direction for data in a meaningful way. Good communication as well as a willingness to initiate a public dialogue on these issues is an important element of public trust in a climate where there is controversy about data use.

In the field of administrative data research, ADR UK have carried out a literature review on public attitudes towards the sharing and linking of administrative data for research. It outlines that public engagement is based on three concepts: public communication, public consultation, and public participation. In terms of existing public knowledge, it found that knowledge 'of the sharing and use of administrative data for research is low, and that this can have an impact on levels of support for the practice' (p8). The executive summary outlined that the public is broadly supportive of administrative data research, as long as three conditions are met: 1) public interest, 2) privacy and security and 3) trust and transparency. Further, that these conditions are not enough in isolation, but that there must be a minimum standard of all three (p1).

Page 11 of the NDS consultation states that the public are 'generally in favour of their personal data being used for scientific research that can deliver real benefits to society.' It is suggested that this support is conditional on the three aspects above being met. Furthermore, the overall approach would be strengthened by a wider public engagement, participation, and communication

campaign to explore and clarify the benefits to society, as well as how privacy and security is secured in a new era of data protection.

Given that public trust is such a significant element of this work and is repeatedly referred to throughout the document, it is suggested that some further analysis is done to clarify and detail what is meant by key concepts, such as 'public trust' and 'public interest'. There is significant analysis in the proposals about the concept of 'fairness' (pp26-30). A similar level of analysis on public trust and public interest would provide further clarity. It would also demonstrate a commitment on the UK government's part to understanding and developing the different dynamics of public trust.

We note in paragraph 289 that the concept of public trust revolves around the duties imposed on public authorities: *The UK's current data protection framework already recognises the importance of public trust by imposing specific requirements on public authorities.* We suggest a more sophisticated concept of public trust would be helpful in this context.

Public good

Overall, we would also like to emphasise the importance of public good arising from research using personal data and data linkage. If DCMS wants to broaden the definition of which types of organisations are allowed to access and process health data then it needs to be based on evidence that the public agree with the changes, by testing it with the public through proper debate (as suggested above).

The Government would need to demonstrate they are having a public debate about this and that ministers are listening to the public. It would be acceptable if a system, separate but similar to ADR UK, was set up to grant private organisations secure access to public sector data, which the government is overseeing in a controlled way. However, there are risks to public perception if the government are sharing public sector data without proper controls on how private organisations are using or sharing the data.

In addition, the spirit of the General Data Protection Regulation (GDPR) is about effective use of people's data in a safe and transparent manner. Broadly speaking, people don't complain about lawful basis for processing or about what is research or not. They complain about lack of transparency about what decisions are made around access to and sharing of data, and how. The consultation rarely mentions transparency and the proposed changes make scant reference to people. The focus seems to be largely around fixing things which aren't broken (e.g., legal basis). Having a legal basis doesn't equate with lawfulness. It gives the impression they are focusing on the law, not the reason why the law is necessary. We think the legal underpinning of data sharing for research or statistics is relatively clear, it is the social contract with the public that has to be earned irrespective of what we can do legally.

Anonymisation

The one area that would help us legally, however, is supporting functional anonymisation. This is that data stored and used for research and statistics according to the '5 Safes' (e.g., pseudonymised in trusted research environments by qualified researchers) can be done so without consent and would not be classed as "personal data".

This has particular relevance for administrative data research. In our response to the ICO consultation on their draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies, we noted that this is a complex and evolving area both legally and technically. A

review by Bristows Introduction to Anonymisation (July 2021) gives a comprehensive review of the legal landscape in this area.

At present and as reflected in the proposals, there have been different approaches to determining anonymisation and this is likely to continue to evolve. We welcome the distinction between "truly anonymous", "effectively anonymised" and "pseudonymised" information in the ICO guidance. This recognises that 'even where you use anonymisation techniques, a level of inherent identification risk may still exist. However, this residual risk does not mean that particular technique is ineffective' (ICO Draft Guidance on Anonymisation p10).

A clear test to be adopted in the data protection legislation may be helpful but would still raise many questions about its application. Organisations would still need to be sufficiently equipped and skilled to carry out this test, as well as carry out an assessment of all the relevant factors (to determine for example the risk of identification) and this can be a complex process. Further detail from the ICO about the factors organisations need to take into account to make these kinds of judgements would be helpful.

Digital Economy Act 2017

While the section referring to the Digital Economy Act (DEA) 2017 of the Consultation relates to public service delivery powers, it would be worth flagging a current limitation of the DEA: section 65 (4) which precludes disclosure of information connected to functions relating to the provision of health services or adult social care.

Whilst there is other complementary legislation that can be used in conjunction with the DEA to link health and administrative data within Scotland, England, and Wales, this is not the case for Northern Ireland. This has been a significant limitation in terms of research with either a health focus or a health component. Addressing this aspect within the DEA, which already carries many safeguards for utilisation of data for research for public good, may address some of the points raised in the wider consultation.

Research purposes

The Covid pandemic has highlighted the importance of administrative data research and other statistical health and social research on complex policy and societal challenges. There is a need to ensure that there is an effective, transparent, and workable regulatory framework in place to facilitate data use for research purposes where there is a genuine public interest. We welcome the intention to make improvements in this area. However, there are specific issues to raise about the detail of the proposed changes and the potential consequences, as outlined further below.

Research purposes

Q1.2.1. To what extent do you agree that consolidating and bringing together research-specific provisions will allow researchers to navigate the relevant law more easily?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

We do not think that this will add value. Those interpreting UK GDPR for research are familiar with all relevant provisions and have interpreted requirements so that UK research is enabled by GDPR. It isn't advisable for researchers themselves to interpret primary legislation, as data protection is an organisational or corporate responsibility, and so it isn't necessary to make it simpler for this audience. The complexity of the legislation in how parts relate to each other means that consolidating research provisions may also have unintended consequences and create issues.

We recommend leaving these provisions as they are. Consolidation is not necessary and could instead add confusion and complexity if organisations feel compelled to review their approach and understanding in light of changes.

Q1.2.2. To what extent do you agree that creating a statutory definition of 'scientific research' would result in greater certainty for researchers?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

The research provisions of GDPR were written to enable research and innovation. We have not encountered any issues related to organisations being unclear about when these apply. It is obvious that the research enablers in GDPR apply to research that ADR UK funds, which is supported by recital 159. Not defining scientific research in law is the best approach for flexible interpretation to support activities that are in the public or legitimate interest and meet the recital definition. Any legal definition could end up being too prescriptive and/or not comprehensive enough and could therefore disadvantage UK research. Instead, adding a statutory definition of scientific research could instead add confusion and complexity if organisations feel compelled to review their approach and understanding in light of this change.

In health research, the main issue around defining research comes, not from GDPR, but from health department policy and whether the UK Policy Framework for Health and Social Care Research applies.

As above, in the eyes of data protection law there are no 'researchers'. There are organisations that undertake research. Organisations should be encouraged to do more to assist the people that they employ to understand the current legal regime, rather than a new regime be put in place.

Q1.2.3. Is the definition of scientific research currently provided by Recital 159 of the UK GDPR ('technological development and demonstration, fundamental research, applied research and privately funded research') a suitable basis for a statutory definition?

- Yes
- **No**
- Don't know

As explained in our response to Q1.2.2 there is a risk that defining this in law does not facilitate research and innovation but hinders it. There is merit in leaving this undefined so innovators can interpret this in a flexible way if needed.

Placing the recital 159 definition in law may also increase the reliance on individual interpretation and guidance would need to be developed to address this. This seems an unnecessary burden on ICO because there isn't an issue in the UK research sector with knowing when to apply the research provisions of GDPR.

Any statutory definition of 'research' would have to align with other law, policy, and guidance around what constitutes 'research'. Data protection law providing a definition of something that extends widely beyond data use doesn't seem appropriate, especially as there are other organisations better placed to do this. This is analogous to our concerns in Q1.5.4.

Recital 159 to the UK GDPR provides a definition of scientific research purposes which includes, for example, technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health. This definition could be broadened to cover more bases. Reducing uncertainty around what constitutes research would reduce the perceived level of risk to organisations and also improve transparency for individuals.

Q1.2.4. To what extent do you agree that identifying a lawful ground for personal data processing for research processes creates barriers for researchers?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

The administrative data research community (including Whitehall departments, the UK Statistics Authority and Devolved Administrations) is moving ever closer to a shared understanding, interpretation, and implementation of GDPR. All parts of the research approvals system support and are aligned to this approach.

The confusion in the health research community is more likely to do with ethical research practice and managing disclosures of confidential information, where consent plays a pivotal role. Changing GDPR does not solve this.

Using public task and legitimate interest lawful bases builds public trust in research, it is good to be able to say that UK research organisations meet the high bars for using these lawful bases,

research is conducted in bona fide research establishments, and data subjects (research participants) can trust that their personal data will be processed in a safe and robust way.

Research collaborations may encounter difficulties in identifying a GDPR lawful basis where there is more than one Controller. Our experience of this is that further guidance on identifying Controllers or Processors in research collaborations would be more useful. Changing the legislation would not get to the heart of the issue. Instead, this could instead add confusion and complexity if organisations feel compelled to review their approach and understanding in light of this change.

In some circumstances establishing a lawful ground for personal data to be used in research can creates barriers in that it makes it a lot more difficult to bring data together in anticipation of a range of research questions (and justifying why we're keeping this data beyond the scope of an individual research project. Moving to the basis that data could be shared into trusted research environments (defined as those accredited as a secure data processing environment by the UK Statistics Authority) and then held securely as "non-personal" data would help with this, as well as giving a legal basis around production of research and statistics in the public good for that initial data transfer.

In summary, the lawful ground should be clear and not open to interpretation so that the boundaries are clear. The lawful ground should be carefully defined so as it allows for the research that society requires.

Q1.2.5. To what extent do you agree that clarifying that university research projects can rely on tasks in the public interest (Article 6(1)(e) of the UK GDPR) as a lawful ground would support researchers to select the best lawful ground for processing personal data?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- **Strongly disagree**

We don't think that this clarification is necessary in law. Identifying the most appropriate lawful basis for research is a key difference in GDPR implementation between EU member states, and the UK has an agreed and specific approach. Changing the law to support the UK interpretation is not needed. Instead, this could instead add confusion and complexity if organisations feel compelled to review their approach and understanding in light of this change.

Q1.2.6. To what extent do you agree that creating a new, separate lawful ground for research (subject to suitable safeguards) would support researchers to select the best lawful ground for processing personal data?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

Having a new lawful basis specifically for research could significantly compromise public trust in research. GDPR recognises that research is different to other processing activities, that it is important and so provides for it in specific and enabling ways. This is appropriate because there are some GDPR fundamentals that need to be fulfilled before these research provisions can be applied. Choosing from a list of appropriate lawful bases that are equally available to all personal data processing is important, research is not seen as so special that the rules do not apply. To engender public trust, research should not be given more allowances than is absolutely necessary. In addition, changing to a new legal basis, away from 'task in the public interest' will give the inadvertent impression that the research in the UK is not in the public interest. We do not feel that creating a new lawful basis is necessary as the current Article 6 list works for research.

Since it is a GDPR transparency requirement that data subjects (research participants) are informed of the lawful basis for processing, to change this would have significant resource impact on the sector.

Although a new lawful ground could help reduce the complexity for organisations undertaking research in identifying a legal ground it would require safeguards on top of those already present in Article 89(1) of the UK GDPR in order to prevent a data subject's personal data from being used in unexpected ways. Depending on what these safeguards were, new challenges could present.

Q1.2.7. What safeguards should be built into a legal ground for research

We do not support the need for additional safeguards for research as we do not support the need for a new research lawful basis in Article 6.

Q1.2.8. To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

It is difficult to understand the motivation for this proposal when research does not generally use consent as the GDPR lawful basis. In the very few circumstances where consent is the lawful basis in research this might be superficially beneficial, however it might also serve to undermine the GDPR consent. Consent is the only lawful basis that fully relies on the data subject's understanding of, and agreement to processing. To allow expansion of processing purposes to such an extent that they cannot be defined, could undermine the nature of GDPR consent. Since research doesn't tend to use this lawful basis, it seems an unnecessary change. It could also potentially be open to exploitation and interpreted as a "carte blanche" for research.

Q1.2.9. To what extent do you agree that researchers would benefit from clarity that further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

GDPR enables research. Research is never an incompatible purpose, which translates into practice that data collected for any original purpose can be used for research by the same or another Controller, as long as the broader requirements of GDPR are met; principally that processing is lawful, fair, and transparent, and the research safeguards are met. This seems like a reasonable and pragmatic interpretation and is not difficult to implement in administrative data or health research, so does not warrant a change to the law.

Selecting a lawful basis for research is not difficult as described in Q1.2.4, therefore there is no need to articulate in law that research processing is both compatible and lawful. And stating in law that research processing is lawful may be detrimental to public trust in research, having to demonstrate this is important for public trust. This is especially true where consent was the lawful basis for the original processing and consent was not described during the consent discussions, it could breach the fairness principle. For health research this is probably a theoretical issue as re-use of care data is the primary example, and processing for care does not rely on consent so this is not a practical problem. In addition, data collected under the 1998 data protection regime for purposes that did rely on consent would no longer do so, as when GDPR came in a new Article 6 lawful basis was required for continued processing, and this was very unlikely to be consent.

Q1.2.10. To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and it where it would require a disproportionate effort to do so?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

Research data is very valuable and may need to be reused for other purposes that were not considered at the outset. In practice it is very difficult, if not impossible, to be transparent with participants where there is no longer contact, and/or there is a risk of disclosure of research data to others. Data is likely to have been provided directly by participants, so the Article 14 5(b) exemption is not available. To have a similar exemption for this would be beneficial.

We agree that a change is needed here, however only somewhat agree with the proposals as it is not needed for all research where data was collected directly form participants, but in specific circumstances as described in Q1.2.11.

That said, although we see the benefits in this by reducing burden, it could lead to ambiguity and a default position of "would require a disproportionate effort to do." Who would decide what a "disproportionate effort" is? Could lead to inconsistency and challenges as indicated in the consultation document.

Q1.2.11. What, if any, additional safeguards should be considered as part of this exemption

Applying a new exemption would need to be limited to a particular subset of research where there is no longer contact with participants, and/or where transparency measures have the potential to breach of other laws, such as common law of confidentiality, e.g., if contact is initiated after a period of time. We do not believe that the exemption would need to be applied to all research that uses data collected directly from participants, where there is disproportionate effort required to apply transparency measures, and it may lead to perverse incentives and compromise public trust in research if it was.

Further processing

Q1.3.1. To what extent do you agree that the provisions in Article 6(4) of the UK GDPR on further processing can cause confusion when determining what is lawful, including on the application of the elements in the compatibility test?

- Strongly agree
- Somewhat agree
- **Neither agree nor disagree**
- Somewhat disagree
- Strongly disagree

Since research is never an incompatible purpose, it is difficult to understand in the research processing of personal data when the provisions in Article 6(4) need to be applied and therefore do not have any comment on questions in this section (Q1.3.1 – Q1.3.4). Our response to Q1.2.9 may be relevant.

Legitimate interests

Q1.4.1. To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?

- Strongly agree
- Somewhat agree
- **Neither agree nor disagree**
- Somewhat disagree
- Strongly disagree

Creating exhaustive lists in legislation does not, at face value, appear to be a good idea. It is very difficult to anticipate all scenarios, and it isn't an agile solution to a potential problem to have to

wait for legislative change in order to amend. Better signposting of guidance may be more appropriate and enhancing this with more research focused examples.

Q1.4.2. To what extent do you agree with the suggested list of activities where the legitimate interests balancing test would not be required? Please explain your answer, indicating whether and why you would remove any activities listed above or add further activities to this list.

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- **Strongly disagree**

Creating exhaustive lists in legislation does not, at face value, appear to be a good idea. It is very difficult to anticipate all scenarios, and it isn't an agile solution to a potential problem to have to wait for legislative change in order to amend. Better signposting of guidance may be more appropriate and enhancing this with more research focused examples.

Q1.4.4. To what extent do you agree that the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- **Strongly disagree**

Having different approaches for demonstrating legitimate interests in research involving children as compared to adults will make things more confusing for the research sector. We recommend that processing data from all individuals is held to the same legitimate interest standards. It seems more relevant to focus resource on how best to produce and provide child-appropriate transparency, than tinker with lawful bases.

AI and machine learning

Q1.5.1. To what extent do you agree that the current legal obligations with regards to fairness are clear when developing or deploying an AI system?

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

Fairness can be a difficult concept to articulate, understand and apply. For AI it is necessarily regulated by a complex interplay of legislation and regulatory agency, and it is important that

these work together to form a cohesive framework. In this consultation document, DCMS provide a good guide to the factors and the complexity at play. Specific guidance for AI development (research) and deployment (use) needs to consider all these factors, and regulators need to work with each other and the community to do this justice.

Q1.5.2. To what extent do you agree that the application of the concept of fairness within the data protection regime in relation to AI systems is currently unclear?

- Strongly agree
- **Somewhat agree**
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

Good guidance coordinated well between bodies is the best way to tackle this.

Q1.5.4. To what extent do you agree that the development of a substantive concept of outcome fairness in the data protection regime - that is independent of or supplementary to the operation of other legislation regulating areas within the ambit of fairness - poses risks?

- Strongly agree
- **Somewhat agree**
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

GDPR has fairness as one of the core principles, but, unlike all the other principles, contains limited information about what constitutes fairness, probably because it is so hard to define in law. It could be interpreted that for AI technologies that process personal data, outcome fairness is already included under the fairness principle, it isn't excluded.

Explicit, prescriptive clauses in GDPR governing outcome fairness may not allow for technologies currently in use that do not serve the whole of society, but which add value to discreet groups within populations.

Instead of legislating for outcome fairness, it would be better discussed in coordinated guidance involving all relevant regulars and departments. GDPR and ICO would not adequately cover this alone. This would also provide a more agile solution for rapidly evolving technology, uses and associated governance.

Q1.5.5. To what extent do you agree that the government should permit organisations to use personal data more freely, subject to appropriate safeguards, for the purpose of training and testing AI responsibly?

- Strongly agree
- Somewhat agree
- **Neither agree nor disagree**
- Somewhat disagree

- Strongly disagree

Better guidance around anonymisation and environmental controls to make it not reasonably likely that identification would occur, would support much AI development and place development outside of data protection regime.

Where use of personal data in AI development is necessary, prior to deployment human intervention in the form of results assessment, testing and validation is likely, so the automated decision-making and profiling requirements of data protection do not tend to apply.

Data minimisation and anonymisation

Q1.6.3 To what extent do you agree with the proposal to confirm that the re-identification test under the general anonymisation test is a relative one (as described in the proposal)? Strongly agree

- Somewhat agree
- Neither agree nor disagree
- **Somewhat disagree**
- Strongly disagree

We agree re-identification test is a relative one, but this should not be in legislation. It is complex and it doesn't seem appropriate to include more detail in legislation, rather to have more practical guidance from government or the regulator.

Re-identification depends on intent, availability of data, knowledge, skills, and technical ability to link data, appetite to breach legal agreements, the existence and severity of professional and employment sanctions, to name a few. These depend on the data, the viewer, the controller, policy, and other players specific to the sector.

It isn't just the means available to the controller to reidentify, it's the means available to the viewer of the data. If classed an anonymised, the viewer's processing may not need a controller. It's complicated and not good territory for any more detail in legislation, much better to develop good guidance and signpost current ICO messaging.

Innovative data sharing solutions

Q1.7.1. Do you think the government should have a role enabling the activity of responsible data intermediaries?

- **Yes**
- No
- Don't know

In the health research sector, a government role e.g., issuing ministerial mandate or statutory vehicle, has been essential for some intermediaries like NHS D to operate. However, universities have been able to act as intermediaries (e.g., SAIL databank at Swansea University) without these.

Q.1.7.2. What lawful grounds other than consent might be applicable to data intermediary activities, as well as the conferring of data processing rights and responsibilities to those data intermediaries, whereby organisations share personal data without it being requested by the data subject?

It depends on whether they are public authorities or commercial or charitable organisations as to which lawful basis are available to them. If commercial or charitable and legitimate interest is their approach, the same tests as for all use of legitimate interest would be recommended. In addition, increased government or regulatory oversight and monitoring of activities would engender public trust. This could include accreditation, and new schemes may need to be developed to ensure that they are fit for purpose.