Scottish Government
Riaghaltas na h-Alba

Final Report of the Independent Expert Group for the Unlocking the Value of Data Programme

August 2023

Final Report of the Independent Expert Group to the Scottish Government on Unlocking the Value of Data

The Independent Expert Group

Chaired by:

- Angela Daly - University of Dundee

Members:

- Annie Sorbie - University of Edinburgh
- Ruchir Shah - Open Government and Civil Society Activist
- Esperanza Miyake - University of Strathclyde
- Colin Birchenall - Digital Office for Scottish Local Government
- Charlie Mayor - NHS Greater Glasgow and Clyde
- Carol Young - Coalition for Racial Equality and Rights
- Alexander Weir - Canon Medical Research Europe Ltd.
- Ronnie Kelly - Fujitsu UK

Former members:

- Mahlet Zimeta ('Milly') - The Open Data Institute
- James Stevenson - Duo Verre Partnership LLP

The writing of this report was coordinated and overseen by Angela Daly with contributions from IEG members.

Acknowledgements

We would like to thank the Scottish Government Secretariat who supported this work. We would also like to thank all those who have provided feedback on earlier iterations of the principles, recommendations and other aspects of this report. In particular we thank: members of the Practitioner Forum; the Democratic Society and all those members of the public and experts who participated in workshops; all those who attended the September 2022 webinar; and the authors of the three literature reviews. We thank Charalampia (Xaroula) Kerasidou (University of Oxford Ethox Centre in Population Health) for peer reviewing this report.

Angela Daly would like to thank the Leverhulme Research Centre for Forensic Science and the Law School at the University of Dundee for supporting her role as IEG chair. She would also like to thank Magdalen College, University of Oxford which hosted her for a research visit from October to December 2022.

Table of contents

Ministerial Foreword

I welcome this report by the Independent Expert Group for the Unlocking the Value of Scotland's Data Programme.

The Scottish Government commissioned this work in order to explore how we can unlock the value of Scotland's public sector personal data in ethical, transparent ways, to realise social, economic and environmental benefits.

Data is central to our aspiration to create an ethical digital nation, where digital services embody the highest ethical standards, personal privacy is robustly protected, people have agency to control their personal information, and no-one is left behind.

While they may seem like abstract concepts, data and ethics play a vital role in enabling better outcomes: from improving public services, to reducing inequalities, to creating sustainable and inclusive growth. The global pandemic, and our response to it, illustrated how the public sector can collaborate at pace, to bring public data together in dynamic, transparent and innovative ways.

While we have legal safeguards in place to ensure the safe, secure processing of personal data in Scotland, we need to address current cultural barriers that impede greater value being created from this data.

Public sector partners have identified the need for guidance when managing data access requests by the private sector. This report provides a foundation on which we can create a framework that will support data controllers to safely, ethically and confidently share data with the private sector.

Public trust and engagement is paramount. Empowering the public to shape the development of ethical practices and approaches is fundamental to securing this trust. In parallel with this, the Scottish Government recently engaged a public engagement panel, whose insights will inform our thinking and strengthen public scrutiny of data-led decisions.

We also require greater collaboration with the private sector in Scotland, to create conditions that enable businesses to innovate with public data, for the benefit of wider society. At all times, value and risk must be carefully balanced. In Scotland, protecting privacy rights and data-driven innovation will go hand-in-hand.

I am determined that we embrace these opportunities to realise our ambition for Scotland to be a global leader in data innovation, based on a solid foundation of public trust and participation.

This report and the supporting evidence – as well as the review of current operational practice by Research Data Scotland – strengthens our evidence base. It underlines our commitment to using data responsibly and innovatively to improve outcomes as envisioned in Scotland's Digital and AI strategies. Furthermore, it complements our data strategy for health and social care, which seeks to empower people to manage their own health and social care data, in safe, appropriate and effective ways.

The Scottish Government will consider this report by the Independent Expert Group, and respond to its recommendations in due course. In the meantime, I would like to thank Professor Angela Daly and the members of the group, both for their report, and for their broader, valuable contribution to this programme of work.

Mr Richard Lochhead
Minister for Small Business, Innovation, Tourism and Trade

Chair’s Foreword

This report adopts a holistic, engaged and multistakeholder approach to unlocking the value of public sector personal data in Scotland for use by the private sector. We have developed a Policy Statement, a set of seven Guiding Principles and 19 Recommendations to steer the implementation of this work by the Scottish Government and other bodies in the Scottish public sector.

The report is the main output of the work the Independent Expert Group on Unlocking the Value of Data has conducted over the last 15 months. I am very grateful to the IEG members for their time, expertise and input. I am also very grateful to the academics who conducted the three literature reviews which fed into this report, the Democratic Society who conducted public engagement activities and the Scottish Government Secretariat who supported our work.

It has been an honour to serve as the Chair of the IEG. I hope that our findings, especially the Policy Statement, Principles and Recommendations, will position Scotland as an internationally leading Ethical Digital Nation. In doing so, Scotland will implement excellence and equity in enabling engagement, and sharing the benefits of private sector use of public sector personal data. Furthermore, Scotland can provide an important example of doing data better for other countries and nations.

Professor Angela Daly
Professor of Law & Technology, Leverhulme Research Centre for Forensic Science and Law School, University of Dundee

August 2023

Acronyms

ADR	Administrative Data Research
AI	Artificial Intelligence
CEDAW	Convention on the Elimination of All Forms of Discrimination against Women
CERD	Convention on the Elimination of All Forms of Racial Discrimination
CRPD	Convention on the Rights of Persons with Disability
COSLA	Convention of Scottish Local Authorities
D&IN	Data and Intelligence Network
DARE UK	Data and Analytics Research Environments UK
DEA	Digital Economy Act
DemSoc	The Democratic Society
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPDI	Data Protection and Digital Information Bill
DSIT	UK Department for Science, Innovation and Technology
ECHR	European Convention on Human Rights
eDRIS	electronic Data Research and Innovation Service
EQIA	Equality Impact Assessment
G2B	Government to Business
GDPR	General Data Protection Regulation
EU	European Union
HDR-UK	Health Data Research UK
HSC-PBPP	Public Benefit and Privacy Panel for Health and Social Care
iCAIRD	Industrial Centre for Artificial Intelligence Research in Digital Diagnostics
ICO	Information Commissioner’s Office
IDS	Indigenous Data Sovereignty
IEG	Independent Expert Group
IP	Intellectual Property
LGBTi	Lesbian, Gay, Bisexual, Transgender and Intersex
MRC	Medical Research Council
NDG	National Data Guardian
NHS	National Health Service

NHSS	NHS Scotland
NPF	National Performance Framework
ONS-ADR	Office for National Statistics Administrative Data Research
PBPP	Public Benefit and Privacy Panel
PSED	Public Sector Equality Duty
PSO	Public Sector Organisation
RDS	Research Data Scotland
SHAIP	Safe Haven AI Platform
S-PBPP	Statistics Public Benefit and Privacy Panel
ToR	Terms of Reference
TRE	Trusted Research Environment (also known as Safe Havens)
UK	United Kingdom
UN	United Nations
UVOD	Unlocking the Value of Data

Glossary

Data

Information about people, things and systems.
According to the UK Government Data Strategy:

> "Data about people can include personal data, such as basic contact details, records generated through interaction with services or the web, or information about their physical characteristics (biometrics) – and it can also extend to population-level data, such as demographics. Data can also be about systems and infrastructure, such as administrative records about businesses and public services. Data is increasingly used to describe location, such as geospatial reference details, and the environment we live in, such as data about biodiversity or the weather. It can also refer to the information generated by the burgeoning web of sensors that make up the Internet of Things."

Data Access

Authorised permission and ability to collect, inspect, adjust, copy, and transfer data. This includes how users get access to the data, where it is located, and who owns or is in possession of the data.

Data Controllers

Defined in the UK GDPR Art 4(7) as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

According to the ICO:

> "Controllers are the main data use decision-makers – they exercise overall control over the purposes and means of the processing of personal data. [...] If you exercise overall control of the purpose and means of the processing of personal data – i.e., you decide what data to process and why – you are a controller."

Data Processors

Defined in the UK GDPR Art 4(8) as: 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

According to the ICO:

> "Processors act on behalf of, and only on the instructions of, the relevant controller. [...] If you don't have any purpose of your own for processing the data and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the data."

Data Sharing

Enabling actions to make the same data available to one or many consumers or users.

Personal Data	Defined in the UK GDPR (Article 4(1)) as: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”
Private Sector	The segment of the economy owned, managed and controlled by individuals and organisations seeking to generate profit. Companies in the private sector are usually free from public or state ownership or control.
Public Sector	The organisations run by the government that exist to provide services for the population and communities. (see also ‘Public Bodies’).
Public sector personal data	Personal data (see above) that is controlled or processed by the Public Sector.
Value	Viewed in the broadest terms covering economic, social and/or environmental factors, in a holistic way. Neither solely or predominantly financial or economic in character, and should also be social and environmental.

Executive Summary

This report is the final output of the Independent Expert Group (IEG) on Unlocking the Value of Data (UVOD), to the Scottish Government. This report is a ministerial commission, and was originally commissioned by Mr Ivan McKee, former Minister for Business, Trade, Tourism and Enterprise. Chaired by Professor Angela Daly from the University of Dundee, the IEG was set up to provide 'strategic guidance and oversight' to the UVOD programme on private sector use of public sector personal data in Scotland.

According to the UVOD IEG terms of reference (ToR):

> **The purpose of this programme is to aid decision-making by data controllers regarding the release of, or provision of access to, public sector personal data by the private sector, for public benefit.**

The IEG has produced three main outputs over its 15 month lifetime: a recommended Policy Statement, a set of seven Guiding Principles and 19 Recommendations. Altogether, these aim to guide the Scottish Government and Scottish public sector in adopting an appropriate, ethical and engaged approach to Unlocking the Value of Scotland's public sector personal data for private sector use in ways which promote public benefit.

The recommended Policy Statement is:

> We consider that when public sector personal data is used by the private sector, this should be done in a way which delivers public benefit and is in the public interest.
>
> This requires consideration of matters including:
>
> - the potential benefits and consequences of data use for the public;
> - people's rights (in particular the right to privacy); and
> - any value (and also any costs and harm) that is expected to be generated by the data use (viewing value in the broadest economic, social and/or environmental terms), including how these benefits and value will be shared with the public.

The Guiding Principles are:

Public engagement and involvement

Public interest and public benefit

Do no harm

Transparency

Law, ethics and best practice

Enabling conditions

Regular review

The 19 Recommendations, addressed to the Scottish Government, are grouped under three key themes: Engage, Enable and Ensure. Their headings are:

Engage	Enable	Ensure

1. Engage in ongoing meaningful public and practitioner involvement and review throughout the data lifecycle
2. Engage with expert stakeholder groups
3. Engage the general public
4. Enable early adoption of Guiding Principles in targeted policy areas
5. Enable awareness of the data held
6. Enable a streamlined approach to data access
7. Enable shared standards and protocols and enable high standards and best practices
8. Enable existing intermediaries and join up
9. Enable collaborative research in this area including the collation of further evidence on blockages and proof of concept research
10. Enable user-centred approaches
11. Enable further investigation into technological opportunities
12. Ensure action plans, resources and conditions are in place
13. Ensure reasonable public benefit rationale provided by those seeking data access, informed by publics and reviewed and verified over time
14. Ensure Data Protection (DPIAs) and Equality Impact Assessments (EQIAs)
15. Ensure red lines on access for certain purposes
16. Ensure transparency from public sector in data access provisions and from private sector about their access to this data
17. Ensure oversight is appropriately resourced
18. Ensure collaboration and further input around benefit-sharing
19. Ensure public can trust the companies accessing the data

This report commences with an Introduction containing background and contextual information about the IEG and UVOD and our approach towards compiling this report. The following section contains the IEG's Policy Statement, Guiding Principles and Recommendations, with associated description and context. This is followed by a Context section comprising: a discussion of data categories and types; relevant laws, policies, organisations and initiatives in Scotland; summaries of the Scottish Government-commissioned literature reviews and public engagement activities; a discussion of public benefit, public interest and value; and an overview of data critique.

1. Introduction

1.1 Background

This report is a ministerial commission, originally by Mr Ivan McKee, former Minister for Business, Trade, Tourism and Enterprise and written by the assembled Independent Expert Group (IEG) on Unlocking the Value of Data (UVOD), chaired by Angela Daly and comprised of experts from different stakeholder groups and backgrounds. The IEG was set up to provide 'strategic guidance and oversight' to the UVOD programme on private sector use of public sector personal data in Scotland.

During 2022 and early 2023 we, the IEG, had been tasked with considering the issue of access to public sector personal data by the private sector, in response to stakeholder feedback that data controllers were unsure about decision making in this domain.

The Scottish Government considers in the terms of reference (ToR) that there is 'significant potential to create public benefit from the use of public sector personal data by, or with, the private sector', and set up the UVOD programme on the basis of 'substantive feedback from stakeholders' (mainly public sector data controllers) 'who identified a case for action'.

We have considered the issue of access to personal data held by the public sector in Scotland for use by private sector organisations over the last 15 months, drawing on our own multidomain and multistakeholder expertise, and engaging with various other stakeholders and the general public to inform our views. To that end, we have formulated a Policy Statement, set of Guiding Principles and a series of Recommendations for the Scottish Government. We found it necessary to explore foundational issues and the landscape in Scotland for public sector data use and were unable to produce a framework that is easily put into operation by public sector data controllers in Scotland during the relatively short (15 month) lifetime of the IEG. We trust that our Policy Statement, Principles and Recommendations can inform the creation of such a framework in the near future.

1.2 About the Unlocking the Value of Data (UVOD) programme

The purpose of the UVOD programme is to aid decision-making by data controllers regarding the release of, or provision of access to, public sector personal data by the private sector, for public benefit. The programme reports to the Scottish Government Minister for Small Business, Innovation, Tourism and Trade, Richard Lochhead.

The Scottish Government commenced the UVOD programme in 2022 in response to feedback from data controllers in the Scottish public sector who were unsure of how to respond to requests by private sector organisations for access to personal data held by the data controllers. While such access in certain circumstances may be permitted under UK data protection legislation, an ethical and best practice approach to providing access has not been clear to public sector organisations making these decisions. According to Stevens and Laurie (2017), this has produced a 'culture of caution' due to, among other reasons, 'misperceptions of the law', 'lack of resources and expertise' to manage data requests, fear of reprisals and 'public backlash' if something goes wrong.

The Scottish Government has considered in the IEG's ToR that there is the 'significant potential to create public benefit from the use of public sector personal data by, or with, the private sector'; although there are also significant risks inherent in this that need to be managed. To examine this issue in more detail, the Scottish Government has commissioned three literature reviews, on (i) public engagement, (ii) frameworks, and (iii) benefit realisation, and formed this Independent Expert Group (henceforth 'IEG') on which we sit. Some preliminary public engagement and consultation has accompanied the IEG's activities.

1.3 The Independent Expert Group (IEG)

The IEG was set up in early 2022, with the appointment of the IEG chair, Angela Daly, supported by a Scottish Government Secretariat. IEG members from a diverse range of backgrounds, stakeholder groups and disciplines were appointed, comprising expertise and experience across a range of areas including law, civil society, health, open data, digital media and industry.

The first IEG meeting took place in March 2022, followed by the second in April, the third in May, the fourth in June, the fifth in August, the sixth in September, the seventh in October, the eighth in December 2022, with the ninth and final IEG in February 2023. In August 2022, the IEG published draft Principles in a blogpost, for presentation, discussion and awareness-raising at a public webinar in September 2022. In September 2022 the Scottish Government commissioned The Democratic Society (DemSoc) to lead engagement with experts and members of the general public to discuss the themes underpinning the IEG and the draft Principles, principally in the form of two focus groups with members of the public in Scotland (one online in November 2022, the other in-person in Inverness in January 2023) to discuss and shape the IEG's Principles.

The Scottish Government Secretariat also established a Practitioner Forum Short-Life Working Group in November 2022 comprising representatives of different public sector stakeholders including data controllers. The Practitioner Forum was set up to work alongside the IEG, and to provide advice on the content and priorities for the IEG report and recommendations.

The IEG has also engaged with academics, especially through the organisation of a special track at the Data for Policy conference in December 2022. Feedback from all of these sources has been taken into account in this document and our Policy Statement, Guiding Principles and Recommendations.

1.4 IEG objectives

The IEG has been set up to provide ‘strategic guidance and oversight’ to the UVOD programme on private sector use of public sector personal data in Scotland. The Scottish Government considers that the UVOD programme:

> **supports the Scottish Government’s commitment to improving outcomes through the ethical and innovative use of data, as enshrined in our National Digital and AI strategies.**

Intended outputs and activities of the IEG have been to produce a policy statement and framework/guidance for Scottish public sector data controllers, and in doing so engage with different stakeholders including the public and practitioners. We have produced a Policy Statement and Principles to guide decision-making and governance by Scottish public sector data controllers. We have engaged with stakeholders mainly through the aforementioned webinar in September 2022, the Practitioner Forum (which is made up of representatives from the Scottish public sector) and the general public, via The Democratic Society.

The IEG has worked as best as it can within the challenges and limitations outlined below. We have spent much of our time understanding the complex landscape in Scotland as regards private sector access to public sector personal data. While a desirable outcome for our work, we have not been able to produce an easily operationalisable framework for implementation by Scottish public sector data controllers. We considered that scoping the landscape and understanding the problems were key first steps that we needed to take, before a framework could be formulated. We hope that such a framework could be produced, with further input especially from public and private sector stakeholders. Technical considerations to support such a framework would also need to be taken into account.

We did not issue a formal call for evidence as part of the IEG mainly given time constraints and the need for us, as IEG members, to clarify the issues on which we have been working. The Scottish Government may wish to build on the foundational work done by the IEG, and address these gaps in the IEG activities and outreach, by issuing a call for evidence to support the next stages of the UVOD programme after the end of the IEG’s lifetime.

1.5 Approach and scope

The IEG conducted our work via a series of IEG meetings, complemented by insights from the engagement sessions and Practitioners' Forum. We also drew on our own multistakeholder experience and interdisciplinary expertise to inform our work. The IEG adopted a consensus-based approach to our work, aiming to find common ground across IEG members especially in terms of our outputs. We note below in Section 2.2 some topics on which consensus was not found but which are still important topics to consider for the UVOD programme after the IEG's lifetime.

In Scope	Not in Scope
Private sector access to public sector personal data via agreements, contracts, etc for the purposes of commercial research, development and innovation.	Private sector provision of data infrastructure for Scottish public sector personal data.
	Non-personal data held by the Scottish public sector.
	Personal data held about people in Scotland by UK Government bodies.
	Public or third sector access to public sector personal data in Scotland.
	Private sector organisations which provide public services and corresponding personal data e.g. GP practices providing personal data to the NHS.

1.6 Preliminary considerations

The IEG was instructed to consider private sector access to public sector personal data in Scotland. In the Glossary above, we offer a definition of 'private sector' as 'the segment of the economy owned, managed and controlled by individuals and organisations seeking to generate profit'. However, 'private sector' is not a well-defined and neat term in practice. Many if not all of the considerations in our Principles and Recommendations could apply to other actors, from other parts of the public sector, or the third sector, requesting access to public sector personal data in Scotland. Our analysis and outputs are confined to private sector use in line with our ToR. However, in implementing the findings from our work, the Scottish Government should ensure that a situation does not result in which the private sector can access public sector personal data more easily or swiftly than other public sector, third sector or other actors.

We know from stakeholders in the Scottish public sector that they are unsure and lack confidence in addressing private sector requests for access to personal data which they hold, which the terms of reference of the IEG are intended to guide/remedy. However, another premise of the IEG/UVOD work is that there is personal data held by the Scottish public sector that the private sector cannot access or cannot access easily enough, and that this is potentially impeding value creation in the public interest for public benefit.

There are some insights from the Scottish Science Advisory Council that earlier in the COVID-19 pandemic 'there was a 10 month delay due to the lack of agreed approaches to proportionate information governance in the context of pertinent emergencies', with the implication that private sector organisations such as pharmaceutical companies were unable to access health data in a timely fashion.

In the Appendix to the Scottish Standing Committee on Pandemic Preparedness Interim Report (August 2022), some challenges were identified:

> **Data accessibility and in particular project delays due to existing information governance arrangements has been identified as a priority issue. Among the challenges noted, delays in existing information governance arrangements such as the Public Benefit and Privacy Panel (PBPP) for Health and Social Care have led to delays to projects such as linking vaccine effectiveness data with viral genomics – data which has been essential to the Scottish and UK governments' responses to the COVID-19 pandemic. There have also been challenges where ethical and information governance approval processes do not include representatives with expertise in a subject, for example in genomic technologies, which can lead to delays and challenges stemming from a lack of understanding of the desired application of data in genomics. Current processes should be reviewed to consider addressing these challenges, which can delay vital research during pandemics.**

It is unclear whether any of these delays and blockages involved requests for data access by the private sector.

Pandemics such as COVID-19 can be, and are, viewed as exceptional events. Personal data, especially health data, held by the public sector should be accessible in order to address emergency health situations, in line with data protection law.

However, further evidence is needed that existing decision-making mechanisms regarding private sector access to public sector personal data, especially outside of a pandemic situation, require revision and amendment, vis-a-vis 'locking up' public benefit and value and being detrimental to the public interest. All relevant societal interests and human rights must be taken into account in such an assessment. More engagement with the private sector, as well as other stakeholder groups, should happen on this point. A future work stream might helpfully be centred on the private sector and their views in order to fully identify and evidence these access concerns. However, it is important to ensure wider views on this point are also sought, not just from the private sector, to ensure a balanced picture of what is in the public interest. Building on the work of the Data and Intelligence Network, including its Ethics Framework, the Scottish Government should consider implementing fast-tracked data access processes for truly emergency situations such as future pandemics.

The UVOD programme originally purported to be ‘citizen led’ but we have in fact had limited engagement with the public (mainly through the DemSoc initiative and the public webinar run in September 2022) and in practice the programme has been led by the Scottish Government Secretariat and the IEG, which comprise civil servants and independent multistakeholder experts, respectively. Far more engagement and co-creation with the public, including citizens but also taking account of other residents of Scotland who may not be UK citizens, is required. We use the term ‘publics’ to capture the diversity and different experiences and viewpoints of people, as the ‘public’ is not a homogenised single entity. For this to happen, it also would need adequate budget and resources, a plan and leadership which the IEG has not been able to provide due to our own resource and time constraints. For such technical and complex policy matters as considered in the UVOD programme, we consider that publics in Scotland should be actively engaged and involved. Nevertheless, it is the government’s role to be the decision-making body, and in so doing balance interests and protect the public from undesirable consequences of both action or inaction on this topic.

1.7 Challenges and Limitations

There have been various challenges and limitations to the IEG and our work. IEG members have contributed to this on a non-remunerated basis which limits the time and resources we have been able to contribute - including in light of industrial action in some sectors such as higher education which has also limited the time some IEG members have been able to contribute. We have conducted this work during the ongoing COVID-19 pandemic which has impacted on our own health and entailed that our work has been carried out mostly online.

We are constrained by the resources and expertise available to us as IEG members and vis-a-vis the Scottish Government Secretariat. In conducting our work, we mainly drew on our own multistakeholder and multidisciplinary expertise. We were not able to commission research on economic analyses of potential public sector personal data use by the private sector, which was beyond the expertise of the IEG members ourselves and which was a research gap we identified at a late stage of the IEG’s lifetime.

We also had limited input from the private sector, despite our attempts to reach out to them. For instance, the Practitioner Forum only contains public sector practitioners and not private sector practitioners. There has been some engagement with industry as part of DemSoc’s engagement activities. For the future stages of the UVOD work, such research and engagement is key. Better formats for engaging with the private sector are needed, which involve a smaller commitment of time and resources than conventional consultations and expert groups request. The Scottish Government should consider what would be more effective ways to engage with industry and at what point in the policy and consultation cycle.

We have had input from third sector organisations, but recognise the pressure under which such organisations operate, especially those which are smaller and have even more constrained resources. The Scottish Government should consider whether some kind of resource support could be provided to facilitate the involvement of these groups and individuals in the policy and consultation cycle.

Our analysis is relevant and reflects the state of affairs as of April 2023 including vis-a-vis legislation in force. This means that we do not include a detailed analysis of the Data Protection and Digital Information Bill (DPDI Bill) proposed by the UK Government.

2 Policy Statement, Principles & Recommendations

We recommend the following policy statement for adoption by the Scottish Government, to guide the use of public sector personal data by the private sector.

2.1 Recommended Policy Statement

We consider that when public sector personal data is used by the private sector, this should be done in a way which delivers public benefit and is in the public interest.

This requires consideration of matters including:

- **the potential benefits and consequences of data use for the public;**
- **people's rights (in particular the right to privacy); and**
- **any value (and also any costs and harm) that is expected to be generated by the data use (viewing value in the broadest economic, social and/or environmental terms), including how these benefits and value will be shared with the public.**

In order to achieve the vision comprised by the Statement, we have formulated the following Guiding Principles and Recommendations to steer and underpin the decision-making and governance by relevant stakeholders in the Scottish public sector on permitting access to the personal data they hold by private sector organisations.

2.2 Guiding Principles

We have devised seven high-level Guiding Principles which we present here with some context and explanation.

An initial and early version of these Principles was made public in August 2022 for comment. We have refined these principles based on feedback from a number of sources in the intervening months, including from attendees of the September 2022 public webinar, the Practitioner Forum in late 2022-23, the engagement workshops with expert stakeholders and the general public run by DemSoc, also in late 2022-23, and elsewhere.

Practitioner Forum input has been particularly important in understanding how viable these principles would be in terms of implementation in current systems. We acknowledge that the Principles have not been further 'tested' or 'validated' at this point, and given the current status of systems, some may be more aspirational than practical for the time being. Other Principles do, however, reflect and reinforce existing practices and approaches to data access and governance in the Scottish public sector. In any case, while the Principles can be viewed as a guide rather than as 'set in stone', their spirit should not be compromised in any future implementation.

In finalising the set of Principles, we removed two principles which were among the original set. One of the two, 'Precaution' was considered to be covered already in other Principles, notably #2 Public interest and public benefit and #3 Do no harm. The other removed principle, ‘Right to opt out’, was discussed at length among the IEG and Practitioner Forum stakeholders. Concerns were raised about the lack of feasibility of a right to opt out - who would enforce and regulate this right? Existing technical data systems in Scotland and data sharing practices have not been designed around such opt out. Concerns were also raised about the possibility of datasets being biased or unrepresentative if people were able to opt out, which may have detrimental impacts on research and subsequent development based on those data. Some members of the IEG remained in favour of retaining the right to opt out as a principle (based on their and others’ research among other topics e.g. Kuntsman & Miyake, 2022; Daly, Devitt & Mann, 2019; see also Hartman et al., 2020). However, as there was no longer a consensus or agreement on this point among the IEG, the Principle was removed. Nevertheless, we do consider that facilitating people’s control and autonomy over their own personal data is a key issue for further exploration beyond the lifetime of the IEG.

Another point on which there was no consensus was as regards intellectual property (IP) and benefit-sharing, with some IEG members advocating for the Scottish public sector to co-own IP rights over the outputs created by the private sector using public sector personal data, while other IEG members considered that this would be unworkable in practice and detrimental to economic value being produced. Accordingly, we have advocated for appropriate benefit-sharing models to be adopted, without specifying further what these should be in terms of IP ownership.

The final set of Guiding Principles are as follows:

1. Public engagement and involvement

Public confidence and trustworthy data use are of paramount importance. All decision-making about and governance of private sector use of public sector personal data should actively seek to support the dual aims of public confidence and trust.

Decision-making and governance by public sector data controllers need to support this principle by incorporating forms of evidence and expertise such as:

- **Findings from high quality, diverse and proportionate public engagement and public involvement in developing the process of how decisions are made about use of personal data, including those who are seldom heard, and bodies representing communities of interest;**
- **External expertise in, for example, data science, law, ethics, public administration and business, equality, diversity and inclusion;**
- **Established Scottish, UK and international evidence on what is considered to constitute public benefit, public interest and public value.**

The public and experts need to be involved and consulted throughout the data lifecycle (from data creation to data destruction) as data creation, access and use is a dynamic process.

The use of evidence, expertise and public engagement should therefore be ongoing and reviewed throughout the data lifecycle.

Consultation with publics can also ensure and demonstrate that use of personal data is fair (see ICO guidance) and allow potential risks and harms to be identified and managed. Such consultation should be ongoing.

In seeking to animate this principle, we view the Data and Intelligence Network Pilot Public Engagement Panel as a promising initiative which may facilitate meaningful public engagement and involvement in decision-making and governance about public sector data use and access in Scotland. The pilot is scheduled to deliver a final report later this year. Furthermore, this work has built on the Scottish Government's Digital Ethics Group, which published their report Building Trust in the Digital Era: Achieving Scotland's Aspirations as an Ethical Digital Nation in 2022.

We acknowledge that public and expert engagement and involvement has resource implications for Scottish public sector bodies. In light of this, the Scottish Government should provide adequate resources to facilitate this engagement and involvement. If there is a limiting of such resources, then issues around the proportionality of public involvement will need to be addressed.

Less resource-intensive methods of achieving this for the Scottish public sector could include the involvement of lay representatives on decision-making panels, such as the Public Benefit and Privacy Panel (PBPP) model mentioned below; and adhering to best practice standards on engagement and participation by those in private sector organisations wishing to use public sector data.

In sum, ultimately, the precise approach will need to be considered on a case-by-case basis. However, taking into account our work over the last 15 months, alongside the evidence provided by publics and experts, there is an indication that meaningful public involvement and engagement is the cornerstone of acceptable data access and use.

2. Public interest and public benefit

> **All access to public sector personal data must be done in the public interest and must also (intend to) produce public benefit and public value.**

As is discussed at length later in this report, both concepts – public interest and public benefit – are deeply contextual, and indeed closely linked. What is 'good' as a benefit or is 'in the public interest' depends on the values or objectives of society. For example, the Scottish Government's Digital Strategy from 2021 sets out the aim that Scotland should be an Ethical Digital Nation.

In our work we have considered a wide variety of different ways that these somewhat elusive terms can be understood in order to provide a starting point for future discussions on private sector use of public sector personal data in Scotland.

We consider that recent work undertaken by the National Data Guardian (NDG) (2022, p. 3) to help define 'public benefit' as a '"net good" accruing to the public' could be drawn on in Scotland by public sector data controllers and panels assessing whether a proposed data use produces public benefit (see Section 3.7.1 on Public Benefit below for full details).

When seeking to define the public interest, it has further been proposed that: 'actions taken in the public interest can be broadly described as those that promote objectives valued by society' (Harvey & Laurie, 2021). We suggest that data access and use that is in the public interest should not only deliver demonstrable public benefit, but should also take place in such a way that takes account of:

- the need to engage and involve publics;
- the recognition that the public interest may change over time and therefore requires review; and
- transparency and accountability.

These are features that permeate our Guiding Principles.

Taken together, this suggests that a 'bottom-up' approach may be preferred, whereby the public interest and public benefit are terms that are co-constructed with publics, in specific contexts, rather than 'defined' by the IEG or a similar entity (i.e. a top-down approach). This is reflected in our Recommendations that invite greater involvement of the Scottish public in the UVOD Programme henceforth.

Value should be produced for the people of Scotland. This value should not solely be financial or economic in character, and should also be social and environmental: so economic value is not the only type of value. However if economic value is produced by the private sector using public sector personal data, this value must be shared with the people of Scotland, for instance through appropriate benefit-sharing mechanisms. Regard should also be taken of the social, environmental and economic costs as well as value which may be produced. In the case of the environment, we follow the Digital Ethics Expert Group Report (2022, p. 25) in advocating for a 'Green Digital Scotland' as part of Scotland's ambition to become an Ethical Digital Nation which 'addresses the environmental impacts of its digital usage', in particular the power consumption and carbon emissions produced by storing and processing digital data.

If the only benefit of a specific data use is the generation of profit by a commercial organisation, it is unlikely that use can be deemed to be in the public interest or to deliver public benefit, in line with the NDG guidance mentioned above. However, the NDG (2022, p. 9) does recognise that 'the generation of proportionate commercial profit may be acceptable to the public if the use also delivers a public benefit, such as improved services or improved NHS knowledge and insights'. It is important that such improvements/ benefits should not just be alluded to, but carefully outlined along with the pathways that will be used for such benefits to return to the public and e.g. the NHS. For example, will they be 'sold back' to the NHS? This knowledge may impact on whether a use of personal data would be in the public interest or not.

Data controllers and other decision-makers in the Scottish public sector are responsible for making decisions about whether and how to permit access to (personal) data held by the public sector. However, they need support in making these decisions in ethical, accountable and consistent ways. To do this, input from the public is necessary, especially in the form of ongoing consultation and engagement with publics on their views on public benefit, public interest and data use.

In addition, there should be some representation of the public in decision-making and governance, which might draw from the pre-existing PBPP model in Scottish health, as they include 'lay' members i.e. members of the general public, as well as subject-matter experts. Another option would be to have panels only made up of lay members of the public making or contributing to the making of decisions, as suggested in the ONS-ADR UK report considered below. In any case, members of the public involved in panels need to be compensated for their time and receive other support for their contributions and attendance.

To ensure decision-making and governance is consistent, certain tests and questions could guide panels assessing requests for personal data in order to establish whether public benefit and public interest is proven/shown.

We further recommend more detailed tests and guidance around public benefit and public interest be devised on the basis of these principles, insights from charity law and the NDG guidance from England, and further expert and public input in Scotland.

A reasonable rationale for public benefit, public interest and value must be demonstrated, made transparent and revisited over time including before access to data is granted and after data has been accessed and used. General and unsupported claims to public benefit, interest and value should not be accepted.

We also urge data controllers, panels and others involved in decision-making and governance to ensure that an open, transparent and accessible review is undertaken of instances where personal data has been used once the project or initiative is complete. Here, relevant decision-makers should discern whether the claimed public benefit was indeed created by the private sector organisation accessing the data. Learning gleaned from such reviews should be fed back into decision making and governance to drive improvement over time.

A common situation when a private sector organisation wishes to access public sector personal data will often involve the production of commercial benefit, overlapping with public benefit also being produced. When addressing such situations where commercial benefit as well as public benefit will be produced, this should be proportionate to the public benefit produced. The public benefit evaluation process should ask the applicant to provide a transparent assessment of how the commercial interests are proportionately balanced with the benefits to the public. This process should be as open, accessible and transparent as possible, in the spirit of open government and open data.

We do acknowledge situations in which the public benefit may be harmed if private sector organisations cannot use public sector personal data. In such situations, the public benefit may be better served by permitting this use. However, harm to public benefit from not allowing the use of personal data would need to be evidenced. If such harm includes companies being dissuaded from setting up in Scotland or from hiring more staff in Scotland, this would need to be demonstrated with evidence.

To ensure accountability, those making decisions about data access should give reasons for their decisions, and these should be made publicly available if possible. Private sector organisations accessing data must also be accountable to both the public sector data sources and to the public at large. One way of facilitating this is through transparency, one of our later principles.

3. Do no harm

Allowing access to personal data by companies should seek to produce no harm. If something harmful occurs, this should be addressed immediately.

Some uses of personal data may involve risks of harm being produced. These risks need to be acknowledged, addressed, mitigated and reduced to acceptable levels before private sector organisations can access (and can continue to access) public sector personal data, to the satisfaction of data controllers and others involved in decision-making and governance, such as panels.

Data protection law (Recital 4 of the UK GDPR) states that the processing of personal data should be designed to serve 'mankind' [sic] and recognises the need to consider it 'in relation to its function in society' and to balance the protection of personal data against other human rights, in accordance with the principle of proportionality.

This principle is also in line with good data protection implementation and compliance, especially as regards data security and personal data breach obligations.

Harm should be viewed in a broad sense. While it will include direct misuse and non-securing of personal data (which would also likely be infringements of data protection law) it may also include uses that are not illegal as such. Non-illegal conduct might include conduct that would cause reputational damage to the Scottish public sector. In the same way that we adopt a broad view of what 'value' is, we also adopt a broad view to what 'harm' is and can include physical, emotional, financial, economic harm, to people, the environment and the economy in Scotland and the world at large. Harm may also involve only private commercial benefit being produced from the use of public sector personal data, although in such a situation, the 'public benefit and public interest' principle (#2) will also not be fulfilled either.

As with public benefit and public interest, the concept of 'harm' should involve input from publics about what they consider to be harmful. This input and dialogue on harm must be ongoing. Feedback from DemSoc workshops with the public identified participants had quite expansive definitions of what constitutes 'harm'.

There may also be different risks associated with the kind of personal data for which access is being sought: is it fully identifiable personal data? Pseudonymised data? Aggregate data? Synthetic data? How is it being accessed? In a TRE? etc. These should also be taken into account on a case-by-case basis.

Private sector organisations could be required to carry out a data protection impact assessment (DPIA) and equality impact assessment (EQIA) before being able to access data. DPIAs are part of a risk-based approach to personal data use, and are required by law to be completed 'for processing that is likely to result in a high risk to individuals', but the ICO recommends that they are completed also 'for any other major project which requires the processing of personal data'. If not currently the practice, we recommend that DPIAs are completed for all requests by the private sector to access public sector personal data.

EQIAs facilitate the understanding of the potential impact of a policy or activity on equality by 'ensuring that the policy does not discriminate unlawfully; considering how the policy might better advance equality of opportunity; and considering whether the policy will affect good relations between different groups' (Equality and Human Rights Commission, 2016, p. 10). In Scotland, EQIAs are a specific legal requirement for public sector public bodies under the Scottish Specific Public Sector Equality Duties. Any public sector organisation in Scotland with a policy of sharing personal data with the private sector must conduct an EQIA of that policy (whether new, revised or existing policies).

There are already systems in place to manage risk, especially in the health sphere, such as the privacy and public benefit panels, public interest assessment, use of TREs, use of less risky data e.g. deidentified data, approved researcher processes, and contractual conditions on access, among others. These should continue to be used, and, where they provide examples of best practice, consideration should also be given to expanding these into areas where they are not currently used. This may be where such systems will help to balance the interests in data use (including with private sector organisations), and the need to protect privacy and other rights and avoid harm.

There may be certain uses and circumstances of public sector personal data by certain private sector organisations for certain purposes where the risk of harm is so high that the public sector data controller should not permit access. Such scenarios might be termed 'red lines' and include e.g. access by insurance, credit rating and marketing companies. Again, we also consider it unlikely that such uses would meet the public benefit principle.

Once data access has been granted, risks should be monitored on an ongoing basis by all relevant parties, including the data controller and the private sector organisation using the personal data. This tracking will have resource implications for public sector data controllers which need to be met by the Scottish Government.

4. Transparency

Transparency is linked to public benefit, public interest, and public engagement as the value of personal data access by private sector organisations needs to be open to scrutiny by society at large, throughout the data and project lifecycles.

There must be transparency about, for example:

I. Which public sector personal data is being accessed from which public body?

II. Which private sector organisation is accessing the data?

III. When?

IV. For what purpose?

V. What are the specific public benefits, public interest and value of the purpose/s?

VI. What does the private sector organisation do or make with that data?

VII. How are benefits of/value generated by those outputs shared with the Scottish public sector AND the people of Scotland?

VIII. How are decisions made by the public sector to grant access to personal data?

IX. How is access managed and what controls are in place (e.g. TREs, panel reviews, approved researchers etc)?

X. To what extent the use of data actually did produce the public benefits in practice and was value was shared back with the people of Scotland?

This Principle complements and augments various pre-existing transparency and data reporting requirements, including from data protection law, freedom of information law, Information Asset Registers, and Caldicott Requests (in the NHS). However, transparency is not just about providing information, but rather about ensuring that this is useful, easy to find, and intelligible to people.

The highest levels of transparency and public communication should be implemented by the Scottish public sector. This means that claims by private sector organisations about the need for commercial confidentiality over matters which would impede the measures of transparency listed above must be critically appraised by public sector organisations and accepted only where deemed necessary and in accordance with public benefit and public interest. Private sector organisations accessing public sector personal data should bear obligations to provide this information, especially at the end of a project, to the public sector, which should be made publicly available.

Appropriate resources and procedures need to be put in place within the Scottish public sector to facilitate this transparency. The aforementioned information must also be publicly communicated. This might involve different communications aimed at different groups e.g. for researchers, for regulators, for the general public. Some of this communication could take place via a publicly available data use register for the public sector in Scotland, which could be run by Research Data Scotland.

5. Law, ethics and best practice

Any access to personal data must be permitted only in line with the highest legal and ethical standards, including best practices internationally in areas including: privacy; data protection; equality and human rights; and data ethics.

It is clear that any access to personal data must only be permitted in line with the law, notably data protection law and equality and human rights law. However we have seen at times that this does not always happen so it is worth reiterating here. The law only goes so far, and public sector organisations and private sector organisations must also adhere to ethical approaches and best practices. Ethics and best practice are evolving, and should be informed by local, national and international expertise, and may also be informed by public engagement, especially on what publics consider to be ethical. What is ethical is likely to be linked to notions of public benefit, public interest, harm, and risk. This will ensure Scotland is an Ethical Digital Nation, in line with the Digital Strategy.

If best practice is not currently implemented in Scotland, this should be aimed for by public sector organisations in terms of how they govern and manage the personal data they hold. As mentioned earlier, our work relates to the legal standards as they are at the time of writing. If the UK Government is successful in implementing the Data Protection and Digital Information Bill into law, this will likely lower data protection standards in UK law compared to those implemented from the EU GDPR. Such a situation may entail a more important role for best practices. What constitutes best practices in this area should be part of the ongoing dialogue with, among others, experts in relevant areas in Scotland and internationally.

6. Enabling conditions

Enabling conditions need to be in place within Scotland's public sector if personal data is to be made available for access by the private sector. For example:

1. **Public sector organisations (PSOs) need to be aware of what personal datasets they hold and publish information about them publicly.**
2. **PSOs should identify and address inequalities in current public sector datasets, notably the extent to which data can be disaggregated by protected characteristics.**
3. **PSOs need to ensure the security and quality of the datasets they hold.**
4. **PSOs need to have staff with adequate skills and training in place on data, digital and information governance literacy.**
5. **PSOs need to have adequate resources to support the provision of access to personal data they hold to the private sector.**

Public sector bodies are funded to deliver public services and not necessarily to support private sector requests including for personal data access. This may involve additional effort and resources from the public sector organisation, for which the public sector organisation is not resourced, especially in times of fiscal restraint such as the current one.

Personal data is also primarily collected by the public sector in order to provide public services, so the data available can include administrative data collected as part of that service delivery. This may mean that not all potential datasets generated are easily usable by other actors, such as the private sector and other researchers, since these are not 'research ready'. The lessons learned to date across local government indicate many potential datasets would require considerable cleansing and additional methodological detail (e.g., robust metadata) to enable wider re-use, if such use was deemed appropriate (Tetley-Brown & Klein, 2021). If datasets are to be made more accessible this may require further resources for the public sector organisation. If the Scottish Government views this as desirable, it should ensure that it provides adequate resources to this end.

One concern raised by IEG and Practitioner Forum members is that there are inequalities present in Scottish public sector personal datasets. In particular, concerns were raised about the extent to which data can be disaggregated by the protected characteristics under the Equality Act 2010 (see section 3.2.2 below). Mitigating these inequalities is key to ensuring Scotland is leading with law, ethics and best practice in this area. Datasets should be checked for relevant inequalities, since otherwise permitting further access and use of that data could further embed and further reinforce those inequalities. The work carried out under the new Equality Evidence Strategy (see section 3.3.6 below) will help to achieve this.

We acknowledge that work is already being carried out at both the Scottish and UK Government levels in the context of, for instance, data maturity, transformation and standards (including cataloguing, 'findability' and consistent application of metadata for data sources). We include this principle to support and augment that work, which should be done in concert with other policy initiatives such as UVOD.

7. Regular review

These principles should be subject to routine review and ongoing monitoring through deliberation with the general public, public sector, private sector and third sector stakeholders, academic and other experts, in Scotland and elsewhere, to reflect developments in evidence, technology and practice.

In making regular review a principle, we aim to highlight the ways in which many policy initiatives, including involving expert groups, can be viewed as a 'one off' event to set policy at a particular point in time for the foreseeable future. In a topic as dynamic as data, that approach is not appropriate as many factors change, even over short periods of time. Therefore we seek to have regular review enshrined as a principle to raise its importance and its crucial role in this particular context. This needs to be supplemented too by ongoing monitoring, possibly by an independent oversight agency or independent commissioner such as that suggested in the D&IN Ethics Framework ('a Data Ethics Guardian or Commissioner for Scotland').

2.3 Recommendations

Drawing from the Principles and context, we have devised the following recommendations, grouped under the following themes of 'Engage', 'Enable'' and 'Ensure'.

Engage

	Heading	**Recommendation**	**Considerations**
1	Engage in ongoing meaningful public and practitioner involvement and review throughout the data lifecycle	The Scottish Government should provide adequate resources to facilitate the implementation of these Principles including supporting ongoing meaningful public and practitioner involvement and engagement.	The Research Data Scotland Public Engagement Fund is a step in the right direction to fulfil this recommendation.
		The Scottish Government should devise an ongoing programme of engagement with different stakeholders and the general public, including before these principles and guidance can be operationalised.	
		The Scottish Government should ensure that the use of evidence, expertise and public engagement is also ongoing and reviewed throughout the data lifecycle, through all the stages from data creation to data destruction.	
		The Scottish Government should regularly review the principles we have devised and their implementation through deliberation with different stakeholder groups and this should reflect developments in Scotland and internationally in evidence, technology and practice.	This review and monitoring may involve the Scottish Government setting up a new independent oversight agency or commissioner to perform these tasks and hear complaints about processes. This aligns with the suggestion in the D&IN Ethics Framework to appoint a 'Data Ethics Guardian or Commissioner for Scotland'.

Engage

	Heading	Recommendation	Considerations
2	Engage with expert stakeholder groups including: - The private sector - The third sector - Academics	The Scottish Government should ensure deeper engagement and consultation with private sector organisations to understand the challenges and benefits of public sector personal data access.	Some stakeholders pointed to the Scottish Government Data Strategy for Health and Social Care consultation process as receiving good engagement and feedback from the private sector, which may form a model for future private sector engagement. Better formats for engaging with the private sector are needed, which may involve a smaller commitment of time and resources than conventional consultations and expert groups request. The Scottish Government should consider what would be more effective ways to engage with industry and at what point in the policy and consultation cycle.
		The Scottish Government should ensure deeper engagement and consultation with third sector organisations.	The Scottish Government needs to recognise the pressure that such organisations operate under and consider whether some kind of resource support could be provided to facilities the involvement of these groups and individuals in the policy and consultation cycle.

Engage

	Heading	Recommendation	Considerations
2		The Scottish Government should also ensure deeper engagement with academics, from a wide range of disciplines (including data science, social sciences, humanities, law, ethics, public administration and business, health, equality, diversity and inclusion) and institutions in Scotland and elsewhere. The Scottish Government and Scottish public sector data controllers should engage in an ongoing dialogue about these issues with experts in relevant areas in Scotland and internationally.	This engagement with academics and institutions should facilitate the identification and use of established Scottish, UK and international evidence on what is considered to constitute public benefit, public interest and public value and other topics. The Scottish Government should consider implementing the Council for the Orientation of Development and Ethics (CODE) model as a way of engaging independent experts throughout a project lifecycle.

	Heading	Recommendation	Considerations
3	Engage the general public	The Scottish Government should ensure that the general public is involved in decision-making about aspects of private sector access to public sector personal data, including in the co-creation of notions of public benefit, public interest and harm.	The diversity of the public should be acknowledged and the views of those who are seldom heard and bodies representing communities of interest should be included. The National Standards for Community Engagement can help facilitate this. We also follow Erikainen and Cunningham-Burley's (2021, pp. 18-19) recommendations that this should: > 'involve the use of deliberative and dialogue based public engagement methods' > 'identify where, to what extent, and at what levels, publics wish to be involved in decision making about private sector use of public sector data' > 'identify the best and most acceptable oversight, governance, and safeguard mechanisms that should be implemented to govern private sector uses of public sector data in ways that ensure that data is protected, and that public benefit is realised'; and > 'ensure that all cases of private sector use of public sector data have stringent oversight, governance, and safeguard mechanisms that publics find acceptable and trustworthy'.

Engage

	Heading	Recommendation	Considerations
3		The Scottish Government should ensure (adopting Erikaninen and Cunningham-Burley's recommendation) that publics be involved in the development of effective benefit-sharing models for private sector partnerships, including profit sharing and reinvestment of profits into the public sector.	We further recommend adopting Berti Suman and Switzer's (2022, p. 39) recommendation: 'Be aware of how framings from government as well as other dominant actors (such as market actors) can erode or undermine 'true' public benefit and engage the public via processes of public engagement on the assessment of public benefit and in the co-creation of the notion of value.' In doing so, the Scottish Government should 'seek to build social licence as a fundamental resource to ensure that private data sharing with businesses operates as a trigger for public good' (Berti Suman & Switzer, 2022, p. 39).
		The Scottish Government should ensure (following Erikaninen and Cunningham-Burley's (2021, p. 19) recommendation) that 'all cases of private sector use of public sector data are transparent and clearly communicated to publics, and implement educational campaigns that inform publics about private sector use of public sector data more generally'.	We recommend that the Data and Intelligence Network and Research Data Scotland be the most appropriate facilities to take forward such public engagement activities including for the UVOD programme.

Enable

	Heading	Recommendation	Considerations
4	Enable early adoption of Guiding Principles in targeted policy areas	The Scottish Government, Public Health Scotland and other data controllers and decision-makers in the Scottish public sector should review their operations and implement the Guiding Principles.	This implementation should occur firstly through a series of use cases/pilot projects which could be targeted at high value datasets such as health, planning and transport personal data.
5	Enable awareness of the data held	The Scottish Government should provide a clear and publicly accessible overview of what personal data is held by the Scottish public sector and how it may be available for access by others (other public sector organisations, private sector organisations, third sector organisations, academic researchers etc).	Such an overview should also be provided in an accessible way to the general public, as well as to more expert audiences such as researchers. Research Data Scotland is developing a metadata catalogue for data in Scotland available for research which aims to help researchers discover data which is already available and give directions about how to access it, although this is still at an early stage of development. In doing this, the Scottish Government and Research Data Scotland should consider implementing Earl et al.'s (2021, p. 22) recommendation: 'From earliest phases, develop ways to market the value and utility of the data sharing infrastructure to immediate stakeholders and users (i.e., researchers, private sector innovators) and be transparent about the risk and opportunities. Ways of doing this include involving stakeholders in the designs of the infrastructure or creating a typology of data and datasets that may be of value.'

Enable

	Heading	Recommendation	Considerations
6	Enable a streamlined approach to data access	The Scottish Government should implement a clear and streamlined process for accessing public sector personal data in Scotland which enables parity of access. In implementing the findings from our work, the Scottish Government should ensure that a situation does not result in which the private sector can access public sector personal data more easily or swiftly than other public sector, third sector or other actors.	This should take account of the needs of different types of users, e.g. private sector organisations, public sector organisations, third sector and academia. This recommendation complements the recommendation of the Life Sciences in Scotland Industry Leadership Group Digital & Data Subgroup in 2021 to implement a 'Once for Scotland' national data architecture and governance system for health and social care data. This also complements the vision from the Review of the Information Governance Landscape across Health and Social Care in Scotland (2022) for 'Streamlined Information Governance in Scotland, to enable the realisation of benefits from digital and data-driven health and care innovation' and the recommendations to establish a National IG Direction for Health and Care and 'de-clutter the IG landscape'.

Enable

	Heading	Recommendation	Considerations
6			We recommend that the Scottish Government considers Earl et al.'s (2021, p. 22) recommendation to: 'Develop a central resource or agency, such as a data permit authority, that helps aggregate, combine, and link data and has the autonomy to decide which permissions to grant, as well as the resources needed to provide quality data. Make the process of this as transparent as possible.' Research Data Scotland's scope could be expanded to encompass such a role.
		The Scottish Government should consider implementing fast-tracked data access processes for truly emergency situations such as future pandemics.	Fast-tracked data access processes in emergencies should build upon the work of the Data & Intelligence Network including its Ethics Framework.

Enable

	Heading	Recommendation	Considerations
7	Enable shared standards and protocols and enable high standards and best practices	We support Earl et al.'s (2021, pp. 21-22) recommendation that: there should be a: '[f]ocus on creating shared data standards and protocols across agencies and local and national contexts - a public agency could be dedicated to this role. These data standards should create confidence in the quality of the data as well as the consistency of the data sets.'	Doing this could also ensure that Berti Suman and Switzer's (2022, p. 39) recommendation to '[i]mplement effective strategies that tackle the identified constraints for promoting Government to Business (G2B) data sharing, for example the absence of common principles on the matter' is fulfilled.
		The Scottish Government and Scottish public sector data controllers and others involved in decision-making should ensure that private sector access to public sector personal data is only permitted in line with the highest legal and ethical standards, including international best practice.	Ethics and best practice will be evolving, and should be informed by local, national and international expertise, and may also be informed by public engagement, especially on what publics consider to be ethical. We also support Earl et al.'s (2021, p. 22) recommendation to '[s]hare ethical standards and best practices internationally' via the development and maintenance of 'an international community of practice'.

	Heading	Recommendation	Considerations
7			Best practice can also be constituted by the 'creative and fruitful collaboration schemes and initiatives existing between research centres, civic organisations and private actors (at times also engaging the public sector) to share personal data, taking for example certain citizen science activities and the reality of data cooperatives and of creative common licensing schemes' (Berti Suman & Switzer, 2022).
		In line with the Scottish Minister's Duty within the Scottish Specific Equality Duties, the Scottish Government should ensure that Scottish public bodies understand their responsibility to Equality Impact Assess their approach to data sharing. This must include consideration of how to identify and mitigate data gaps for protected characteristic groups. Onward use of data which contains such gaps risks creating, maintaining or widening inequalities.	The Scottish Government should ensure any equalities data gaps are addressed as part of the implementation of the new Equality Evidence Strategy 2023-2025 and the Equality Data Improvement Programme.

Enable

	Heading	Recommendation	Considerations
8	Enable existing intermediaries and join up	The Scottish Government should build on pre-existing bodies including Research Data Scotland, the Safe Havens and Scottish universities to facilitate access to public sector personal data by private sector organisations.	These existing actors should be utilised, supported with sufficient and appropriate resources, and their expertise should be built upon and processes and procedures refined to take account of the principles and other recommendations. These are successful operating models and bodies for facilitating secure access by commercial entities to public data. Accordingly, we recommend they are built upon and resourced for other public sector organisations to learn from them.
		The Scottish Government should adopt more joined-up policy and initiatives in this area.	There is a lot of complementary activity underway within and across the Scottish Government itself, and that the UVOD Programme going forward would benefit from a clear linkage and demarcation to these initiatives.
		The Scottish Government should resource Research Data Scotland to provide a consultancy service for public sector data controllers to advise on access requests by the private sector, informed by these principles with an advisory board of multistakeholder experts and public representatives.	Informed by the advisory board, RDS should formulate draft standard contracts/templates which could be used by data controllers to facilitate these data access requests.

Enable

	Heading	Recommendation	Considerations
9	Enable collaborative research in this area including the collation of further evidence on blockages and proof of concept research	The Scottish Government should implement an ongoing programme of research in this area undertaken in partnership between public sector bodies, third sector, universities and research funders.	The Scottish Government should inquire with multiple stakeholder groups to establish whether such blockages exist, especially outside of health/pandemic situations, and whether the blockages are detrimental to public benefit being produced and the public interest. The Scottish Government should engage with a wide range of stakeholders, including but not limited to the private sector, on this point, to ensure a balanced picture of what is in the public interest.
		The Scottish Government should seek further evidence that existing decision-making mechanisms regarding private sector access to public sector personal data are causing negative outcomes or blockages before they ought to be altered.	This further evidence should include independent economic analyses of potential public sector personal data use by the private sector and what expected social, economic and environmental value would be created, and what expected social, economic and environmental costs might be. Theoretical assumptions underpinning such analyses must be made clear by the researchers and the likelihood of this value being created in current and near future political and economic circumstances in Scotland should be elucidated.

Enable

	Heading	Recommendation	Considerations
9		The Scottish Government should commission more research, and seek evidence and views about whether and how Scottish public sector bodies could facilitate access to personal data for proof of concept research and/or access to synthetic data taking account of barriers such as quality and standardisation.	This research and evidence activity may be best led by Research Data Scotland.

Enable

	Heading	Recommendation	Considerations
10	Enable user-centred approaches	The Scottish Government should consider other forms of data sharing design and infrastructure which centre individuals more, facilitating their control and autonomy over their personal data, and which will be context-specific.	These could include personal data stores that are controlled by the individuals whose data is stored there. Data cooperatives are another model which may combine control and consent of individuals with facilitating data use. Another potential model is that of data trusts. A further approach could be an opt out function, whereby individuals are able to opt out of their personal data which has already been collected by the public sector being used by the private sector. In considering these models and approaches, the Scottish Government must pay due regard to the diversity of the public in Scotland and the specific needs some people may have, e.g. who speak English as a second language, or who have disabilities. The Scottish Government should commission further research on these models, including feasibility for implementation, alongside current mechanisms such as Research Data Scotland. The Scottish Government should also support a meaningful dialogue and co-creation with the public from the early stages in the designs of the data sharing infrastructures, as recommended by Earl et al. (2021).

Enable

	Heading	Recommendation	Considerations
11	Enable further investigation into technological opportunities	The Scottish Government should seek and support more input at the technical architecture level to better understand the technology that could support the implementation of the principles, such as on overseen and traceable data access and usage	

Ensure

	Heading	Recommendation	Considerations
12	Ensure action plans, resources and conditions are in place	The Scottish Government should develop action plans for the next phases of the UVOD programme based on these principles and recommendations. The Scottish Government must ensure that the enabling conditions as outlined in Principle #6 are in place in Scotland's public sector and that the resources are provided to facilitate these conditions.	

	Heading	Recommendation	Considerations
13	Ensure reasonable public benefit rationale provided by those seeking data access, informed by publics and reviewed and verified over time	The Scottish Government should ensure that data controllers and others involved in decision-making over data access in the Scottish public sector require that private sector organisations provide a reasonable rationale for public benefit, public interest and value. This rationale should include information that assists decision makers to consider the impacts of data access including vis-a-vis data protection and equality.	This should be demonstrated, made transparent and revisited over time including before access to data is granted and after data has been accessed and used. We recommend the adoption of Erikaninen and Cunningham-Burley's (2021, pp. 19-20) recommendations: > 'Ensure that all cases of private sector use of public sector data are centrally motivated by and have a demonstrable potential to deliver public benefit, and provide convincing evidence and justifications for how public benefit will be realised.' > 'Ensure that all cases of private sector use of public sector data have an in-built benefit-sharing system based on these benefit-sharing models.' We also recommend the adoption of Berti Suman and Switzer's (2022, p. 4) recommendations: > 'Start with pilot sharing in those fields where studies demonstrate that ordinary people are supportive of health and social care data being used for public benefit but make sure that public benefit outweigh private profits and interests.'

Ensure

	Heading	Recommendation	Considerations
13			- 'Emphasise principles of commutative and distributive justice in considering benefit-sharing arising from the use of publicly held personal data.' - Respect key principles such as that of proportionality, transparency, accountability, and respect for ethical values and norms in designing frameworks for public sector personal data (benefit) sharing. Value co-creation should also be promoted in the construction of benefits.'
		In interpreting the definitions of public benefit and public interest, the Scottish Government should ensure that there should be appropriate mechanisms for publics to give input into what they consider these to be. The public should also co-create notions of value and harm. These should form the basis of tests for public benefit and public interest, on the basis of the Guiding Principles, insights from charity law and the NDG guidance, and further expert input.	The D&IN Pilot Public Engagement Panel and Research Data Scotland may be the appropriate organisations to implement this recommendation.

Ensure

	Heading	Recommendation	Considerations
13		The Scottish Government should ensure that data controllers and others involved in decision-making review instances where personal data has been used once the project or initiative is complete, to discern whether the claimed public benefit or public interest was indeed delivered by the private sector organisation accessing the data.	Learning gleaned from such reviews by data controllers and others of whether public benefit and interest were indeed delivered by the private sector should be fed back into decision making and governance to drive improvement over time.
14	Ensure Data Protection (DPIAs) and Equality Impact Assessments (EQIAs)	The Scottish Government should require private sector organisations seeking access to public sector personal data to carry out a data protection impact assessment (DPIA) and Equality Impact Assessment (EQIA) before being able to access the data.	
15	Ensure red lines on access for certain purposes	The Scottish Government should implement certain 'red lines' or prohibitions on private sector access to public sector personal data.	These should include no access by insurance, credit rating and marketing companies, and no use which is purely or mostly commercial compared to that which produces public benefit.

Ensure

	Heading	Recommendation	Considerations
16	Ensure transparency from public sector in data access provisions and from private sector about their access to this data	The Scottish Government should ensure that there is transparency and public communication about the access to public sector personal data by the private sector.	
		The Scottish Government should ensure that private sector organisations bear obligations to be transparent and provide information to the public and to the Scottish public sector data controllers about their access and use of public sector personal data.	Research Data Scotland should maintain a publicly available data use register for the public sector in Scotland where this material vis-a-vis transparency could be communicated.
17	Ensure oversight is appropriately resourced	The Scottish Government should ensure public sector data controllers and others involved in decision-making and governance are properly resourced to achieve the objectives in the previous principles.	
18	Ensure collaboration and further input around benefit-sharing	The Scottish Government should ensure that private sector access only happens in collaboration with the Scottish public sector and appropriate and convincing benefit-sharing built into the use of the data should take place with the Scottish public sector and people of Scotland.	

Ensure

	Heading	Recommendation	Considerations
18		The Scottish Government should seek more input on appropriate models of benefit-sharing for public sector personal data use by the private sector, building on the Berti Suman and Switzer (2022) literature review.	This additional input on benefit-sharing models should include a systematic search and request for case studies of good practice, successes and challenges. This should be informed by benefit-sharing arrangements in the biodiversity context 'where benefit-sharing is firmly embedded as both a principle and an outcome of access to certain forms of information' (Berti Suman & Switzer, 2022).
19	Ensure the public can trust the companies accessing the data	The Scottish Government should ensure that only private sector organisations which comply with agreed standards of corporate behaviour are permitted access to public sector personal data in order to maintain public trust.	Agreed standards of corporate behaviour would comprise private sector organisations complying with legislation and fulfilling financial and regulatory obligations such as tax.

2.4 Conclusion

Here we have set out our findings on private sector access to public sector personal data in Scotland, in the form of three specific outputs: a Policy Statement, Guiding Principles and Recommendations, accompanied by justifications, context and considerations. It is now up to the Scottish Government to consider these findings and, we hope, implement them in practice. Some Recommendations require further work, evidence gathering and research to be done, and some require ongoing programmes of engagement with different stakeholder groups and the emerging literature and practice in Scotland and internationally.

Achieving these outcomes will require a strong commitment from the Scottish Government, Scottish public sector, stakeholders in all sectors and the general public to ensure that the highest standards are followed and developed in an ongoing feedback process. This will require requisite resources to be allocated to support this along with political will. However, for Scotland to achieve its goal of being an Ethical Digital Nation, and ensuring personal data is used for public benefit purposes by the private sector, such a commitment and resources are necessary. In doing so, Scotland will also benefit by becoming a globally leading nation in ethical, appropriate and fruitful data practices.

In terms of practical and immediate next steps and future work, the Scottish Government now plans to undertake an iterative planning approach to the next stages of the UVOD programme. We, the IEG, consider that developing a decision-making and governance framework for public sector data controllers when considering access requests by private sector organisations is an important next step for the UVOD programme and we acknowledge that we have not provided one. Its development should also engage independent experts, the public and other stakeholders. The Scottish Government should make a commitment to continuing this work in the next stage of the UVOD programme.

In operationalising and implementing the Policy Statement, Guiding Principles and Recommendations, we consider that certain use cases or pilots should be identified by the Scottish Government, Research Data Scotland and other relevant stakeholders, as per Recommendation #4 above, to trial the Statement and Principles and see what might work for a broader implementation throughout the Scottish public sector.

3. Annex: Context

The Scottish Government's Unlocking the Value of Data programme, and the IEG which forms part of it, take place within a broader context in Scotland, in the UK, in Europe and internationally of personal data use and sharing, digital policymaking and ethical and political discussions on data. Here we provide an illustration of this context. These topics are vast and we cannot cover exhaustively all aspects of them. However, we give a taste of some of these themes and their relevance to the IEG.

There are vast debates and activity around data access, sharing and use, and how to value this. Some of these relate to non-personal data (which includes data about deceased individuals and anonymous data), which is not the topic of the IEG's work; instead we have been looking at personal data which is defined in the UK GDPR (Article 4(1)) as:

> **any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**

We have been considering personal data held by the public sector in Scotland. This includes personal data collected from interactions with the NHS, the Scottish Government and local authorities in Scotland (including local council services such as education, social care and council tax payments). UK public sector organisations also collect personal data about people in Scotland, such as through immigration and the benefits system. While we would like these agencies to follow our policy statement, principles and recommendations, they relate to reserved powers and are beyond the jurisdiction of the Scottish Government.

Here we are also specifically considering access to public sector personal data by the private sector. The private sector can broadly be defined as organisations that are usually profit-making companies, and include a wide range of sectors, from pharmaceutical companies to supermarkets to energy companies and farms. The boundaries between the public sector, private sector and other sectors like the third sector (which include charities, community organisations and universities) are not always clear. We restrict our analysis to private sector organisations' access to public sector personal data as this is the mandate the Scottish Government gave us, but we consider that many of the points we make could equally apply to public sector organisations accessing other public sector organisations' personal data.

3.1 Data categories and types

Personal data can be further divided into various categories, some of which appear in data protection law and some of which do not. Data protection law (UK GDPR Art 9) recognises 'special category personal data' as:

> **personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.**

The principles of data protection do not apply to processing data which is 'anonymous', including for statistical or research purposes, as defined in UK GDPR Recital 26 as:

> **information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.**

Pseudonymous data is considered to be personal data (and therefore comes under the definition and scope of personal data), and is also explained in UK GDPR Recital 26:

> **Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.**

Other terms are used with regards to personal data especially in research contexts such as aggregated, raw data, and synthetic data. These terms are not legally defined. Each of these terms may also constitute personal data if the requirements above from data protection law are met.

Raw data is data that has not been processed for use. Aggregated data according to IBM is the outcome of a process 'where raw data is gathered and expressed in a summary form for statistical analysis'.

Synthetic data, according to the ICO, is 'data which does not relate to real people, it has been generated artificially'. If this data cannot be 'related to identifiable living individuals' it will not be personal data. However, as synthetic data is likely to have as its basis 'real' data, and if that data is personal data then its processing must comply with data protection law. Furthermore, according to the ICO:

> **it may be possible to infer information about the real data which was used to estimate those realistic parameters, by analysing the synthetic data. For example, if the real data contains a single individual who is unusually tall, rich, and old, and your synthetic data contains a similar individual (in order to make the overall dataset statistically realistic), it may be possible to infer that the individual was in the real dataset by analysing the synthetic dataset. Avoiding such re-identification may require you to change your synthetic data to the extent that it would be too unrealistic to be useful for machine learning purposes.**

3.2 Relevant laws

Our work takes place in a complex and multi-layered legal and policy environment. In Scotland, we have three relevant levels of government: local authorities, the devolved administration (Scottish Government) and the UK Government. The competences of the UK and Scottish Governments are part of the devolution settlement and governed by the Scotland Act 1998. Until 2021, European Union (EU) law also applied in the UK including Scotland, but since the UK left the EU, this has ceased to be the case unless the specific law is 'retained'. There are certain key areas of legislation which relate to personal data and data sharing, namely data protection law, equality and human rights, and the Data Economy Act. There is also the common law of confidentiality in Scotland, and more recently a common law right to privacy was recognised by the Court of Session.

3.2.1 Data protection law

Data protection law, which governs the processing of personal data, originates in EU law and notably the General Data Protection Regulation (GDPR) which the UK implemented before it left the EU. Data protection law is highly significant for our work given the subject-matter of the IEG being 'personal data'. Currently, data protection is a 'reserved' matter to the UK Government, and the GDPR remains implemented in the UK post-Brexit via the UK GDPR and in conjunction with Data Protection Act 2018 (although this may be subject to change with the proposed DPDI Bill). Organisations, whether public, private or third sector, in Scotland must comply with UK data protection law, and the UVOD and IEG work takes place within the framework of UK data protection law.

Within the definition of 'personal data' there are subsets of personal data termed 'special category personal data' which are listed in Art 9 UK GDPR (in full above). Some personal data held by the Scottish public sector will constitute special category personal data, and is subject to further requirements and restrictions for its processing and use.

EU data protection standards, while not perfect, do represent a current global 'gold standard' or 'best practice' in the absence of substantive international law on this topic.

Data protection law allows the processing of personal data so long as certain conditions are met. Contrary to a commonly-held belief, data protection law does not always require the consent of individuals to process their data. There are six lawful bases for processing personal data, of which consent is one. Consent may not always be the appropriate lawful basis for processing.

Data protection law also does not prohibit per se the accessing of personal data by third parties. This is possible so long as its requirements are met. As current data protection law has been implemented since 2018, Scottish public sector organisations are experienced in complying with these rules and standards, and this remains fundamental to how personal data is handled. Data protection compliance in the UK is overseen by the regulator, the Information Commissioner's Office (ICO), which also issues guidance on data protection issues.

The ICO has issued guidance on the research provisions of data protection law. It states that:

> **These provisions recognise the importance of scientific and historical research and technological development to society. They ensure that data protection requirements enable technological innovation and the advancement of knowledge.**

'Scientific research' is elaborated on in Recital 159 UK GDPR:

> **the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.**

Private sector use of public sector personal data within the UVOD programme's scope is likely to fall within this definition of research. The ICO has an indicative list of criteria for scientific or historical research and an indicative list as to what would constitute 'statistical purposes'.

There are various exceptions to rights for data subjects in data protection law which relate to research such as within the right to be informed when data is collected from a source other than the individual (UK GDPR Art 14(5)(b)) and within the right to erasure (UK GDPR Art 17(3)(d)).

Within the data protection principles in UK GDPR Art 5, two of them (purpose limitation and storage limitation) contain research-related provisions: personal data can be further processed for research purposes which would not be considered incompatible with the original purposes; and can be stored indefinitely so long as there are appropriate measures in place to safeguard the rights and freedoms of data subjects.

For research, the usual lawful bases used are 'public task' or 'legitimate interests'. For special category personal data, a lawful basis for processing and a special category condition for processing in compliance with UK GDPR Art 9 is needed. This processing of special category data must also be 'in the public interest'. Public interest is not defined in the legislation but the ICO says: 'you should broadly interpret public interest in the research context to include any clear and positive public benefit likely to arise from that research'. The ICO provides some indicative examples of what may constitute public interest/public benefit processing and also mentions the avoidance of harm being 'a key factor in determining whether or not your research is in the public interest'.

Section 19(2) DPA 2018 stipulates that the research provisions cannot be used if the processing is likely to cause substantial harm or substantial distress to a data subject. This is one of a number of safeguards (in Art 89 UK GDPR and section 19 DPA 2018) which must be put in place in order to use the research provisions of data protection law. Other safeguards include:

- **technical and organisational measures to ensure respect for data minimisation;**
- **the use of anonymous information where possible;**
- **where not possible the use of pseudonymous information; and**
- **not carrying out research for the purposes of measures or decisions about particular people (unless the research is approved medical research).**

Among the technical and organisational measures, the ICO suggests, among others:

- **the carrying out of data protection impact assessments (DPIAs) where necessary;**
- **the use of privacy enhancing technologies such as trusted research environments
(TREs - see below for more detail); and**
- **accountability frameworks such as the Five Safes (see below for more detail).**

Data protection impact assessments, or DPIAs, are 'a process to help you identify and minimise the data protection risks of a project' and must be carried out if processing is 'likely to result in a high risk' to individuals. The ICO also considers it 'good practice' to carry out DPIAs 'for any other major project which requires the processing of personal data'.

The ICO has obligations under the Data Protection Act 2018 to produce various codes of practice, including one on Data Sharing, whose current version is from 2021. The Data Sharing Code aims:

> **to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way in this changing landscape. This code will guide practitioners through the practical steps they need to take to share data while protecting people's privacy.**

Among various proposed reforms, including changing the definition of 'personal data', the DPDI Bill also has provisions on research. According to the UK Government Department for Science, Innovation and Technology (DSIT), which has responsibility for data protection:

> **Unleashing more scientific research**
>
> **Current data laws are unclear on how scientists can process personal data for research purposes, which holds them back from completing vital research that can improve the lives of people across the country.**
>
> **The Bill has updated the definition of scientific research to clarify that commercial organisations will benefit from the same freedoms as academics to carry out innovative scientific research, such as making it easier to reuse data for research purposes. This will reduce paperwork and legal costs for researchers, and will encourage more scientific research in the commercial sector. The definition of scientific research in the new Bill is non-exhaustive, in that it remains any processing that 'could reasonably be described as scientific' and could include activities such as innovative research into technological development.**

These proposals have received differing receptions from different stakeholder groups. Some concerns have been raised by some (e.g. Dr Chris Pounder of Amberhawk) that this may lead to 'unethical' research taking place. Questions have also been raised about whether the UK will retain its adequacy decision with the EU if it implements the DPDI Bill reforms.

3.2.2 Human rights and equality law

The UK, and Scotland as a constituent part of it, remains a member of the European Convention on Human Rights (ECHR - which is a separate legal regime to EU law). ECHR rights are given some effect in the UK via the Human Rights Act 1998. Compliance with the Human Rights Act 1998 is a condition of the Scottish Parliament passing legislation as per the Scotland Act 1998. There are other pieces of legislation such as the Equality Act 2010 (which implements anti-discrimination rights and the Public Sector Equality Duty) and the aforementioned Data Protection Act (which implements the right to privacy from Article 8 ECHR).

The Scottish Parliament passed a bill to incorporate the UN Convention on the Rights of the Child into Scots law in 2021, but this is being challenged by the UK Government at the time of writing. The Scottish Government has also committed to introducing a Human Rights Bill for Scotland, incorporating four more UN treaties (the International Covenant on Economic, Social and Cultural Rights; the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW); the Convention on the Elimination of All Forms of Racial Discrimination (CERD); and the Convention on the Rights of Persons with Disability (CRPD)) and including the right to a healthy environment, and rights for older people and LGBTi people.

The human rights legislation in force is relevant to personal data, to ensure that personal data is handled in ways which do not cause discrimination or infringe other human rights. Public sector bodies making decisions about data access must also adhere to the positive legal obligations designed to advance equality placed on them by the Public Sector Equality Duties, both within the Equality Act 2010 and the associated Scotland specific legal regulations.

The Equality Act protects against discrimination, victimisation and harassment due to one or more of nine protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; and sexual orientation. The PSED requires public authorities to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different groups when they are carrying out their activities. In accordance with the Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012, Scottish public sector organisations must carry out Equality Impact Assessments (EQIAs) 'to assess the impact of applying a proposed new or revised policy or practice against the needs of the general equality duty'. The Equality and Human Rights Commission publishes guidance on the Equality Act 2010, including specific guidance on the relationship between PSED and data protection law.

3.2.3 Digital Economy Act

The UK-wide Digital Economy Act 2017 (henceforth DEA) includes provisions in Part 5 on data sharing in the public sector, in the context of five chapters: (i) public service delivery; (ii) civil registration; (iii) debts owed to the public sector; (iv) fraud against the public sector; and (v) data sharing for research purposes. Data protection law must also be complied with in these circumstances. The DEA provisions are supplemented by statutory codes of practice. The DEA does not cover the sharing of health and social care data.

In 2020, the Scottish Government consulted on a list of Scottish public authorities to be considered for inclusion in the debt and fraud schedules of the DEA. A further consultation was conducted later in 2020. These consultations fed into the development of the Digital Government (Scottish Bodies) Regulations 2022 which added the Scottish bodies to the schedules. This provides the bodies with access to the powers to share information to better manage debt and fraud against the public sector. Data can only be shared in accordance with the specific purposes set out in the DEA and not for other purposes. Public bodies must have regard to a Code of Practice which provides detail on how these powers should operate.

3.2.4 NHS data sharing

The Scottish public sector holds personal data on a number of topics and issues. Prominent among those data are health and social care data from NHS services in Scotland.

For general NHS data processing, including sharing, the relevant legislation and guidance include:

- **statute law, including the aforementioned data protection law (including the Data Protection Act 2018 and UK GDPR) and Human Rights Act 1998, as well as the National Health Service (Scotland) Act 1978, Infectious Disease (Notification) Act 1889, Adults with Incapacity (Scotland) Act 2000, the Abortion Act 1967 among other pieces of legislation;**
- **the common law in Scotland on confidentiality (which, in summary, requires either consent or a legal or public interest requirement for disclosure);**
- **professional standards such as the Good Medical Practice principles for doctors, and equivalent professional standards for other registered professions, and;**
- **the policies and organisational standards of the Scottish Government (Directorate of Health and Social Care) and NHS Scotland including Chief Medical Officer guidance.**

3.2.5 Beyond the law

Our work proceeds on the basis that the aforementioned legal requirements in data protection, equality and human rights and other areas will be adhered to by all involved in private sector access to public sector personal data. We acknowledge that this is not always the case in practice. For instance, the ICO reprimanded the Scottish Government and NHS National Services Scotland in 2022 for concerns about the NHS Scotland COVID Status app as regards information provided to the public about how the app would use their data in the Privacy Notice. In 2022, we have also seen the Department of Education in Westminster reprimanded by the ICO for its 'poor due diligence' in permitting access to a database of personal data by an employment screening company, Trust Systems Software UK (Trustopia), which then used the database to build age verification systems for online gambling.

Even if we assume that all organisations in all sectors fully comply with data protection law, and other relevant laws such as the Human Rights Act and Equality Act, we also have to look beyond these pieces of legislation in order to understand how and whether private sector organisations should be able to access public sector personal data. For one, data protection law may leave some discretion on how certain provisions could be complied with, which opens up an ethical choice between two compliant outcomes, one of which may be more ethical than the other (O'Keefe & O'Brien, 2018). There are also a number of ethical, social and political issues which relate to this topic that are not clearly covered or resolved by the law as it stands. Among these are the role of the public and the value that the use of personal data could bring. Furthermore, data and corporate infrastructures may be international or transnational whereas legislation is regionalised to particular jurisdiction/s.

However, before we look in more detail at ethical issues, we now look at a series of policies around data and digital issues in Scotland which help implement and explain some of the legal requirements.

3.3 Policy

The Scottish Government has a number of policies in relevant areas for our work, some of which we refer to below.

3.3.1 Open Data

Scotland has had an Open Data strategy since 2015. Open data is non-personal and non-commercially sensitive, and so would exclude personal data held by the public sector, unless it is anonymised. The aim of the strategy is:

> **to create a Scotland where non-personal and non-commercially sensitive data from public services is recognised as a resource for wider societal use and as such is made open in an intelligent manner and available for re-use by others.**

The Strategy envisaged that making data open would achieve the following:

1) **Delivery of improved public services through public bodies making use of the data**

2) **Wider social and economic benefits through innovative use of the data**

3) **Accountability and transparency of delivery of our public services**

In lieu of a single national official portal, a volunteer-run portal, Open Data Scotland, helps people to find open data in Scotland, held by a range of public sector organisations including local councils and Scottish Government agencies. More information about the importance of open data to a healthy data use ecosystem, and a list of recommendations, were published by the David Hume Institute in early 2022 (Watt, 2022) A Statement released from the Scottish Open Data Unconference in 2022 recognises the Scottish Government's public commitment to open data but its implementation of that commitment 'lags far behind what should be delivered' as 'the majority of public bodies… publish no, or very little open data'. The Statement also points to a lack of clear leadership, accountability and responsibility over open data in Scotland, and the deficiencies in the open data which is published.

3.3.2 Data and Intelligence Network

In May 2020 at the beginning of the COVID-19 pandemic, the Scottish Government established the Data and Intelligence Network (D&IN), a 'community of data experts' from across the Scottish public sector and academia whose aim is to provide evidence and analysis to inform decision-making and governance on data in the pandemic context. Among its more specific aims are to ensure information security and ethical data use in its projects, to develop 'frameworks and guidance on the data ecosystem, public participation and ethics', and to combine 'data from across the public sector, to generate actionable insights to make improvements for the people of Scotland, in a safe and transparent way, trusted by the public'.

The Data and Intelligence Network produced an Ethics Framework in 2021:

> **a set of values and principles that can be used by the D&IN either to apply to strategic decisions or to help frame problems or solutions for which members of the D&IN are seeking to use data or digital technology**

The Values are: Competency; Transparency; Fairness; Purpose; Trust; Voice and Agency. The Principles are: Responsible; Accountable; Insightful, Necessary; Beneficial; Observant; and Widely Participatory.

3.3.3 Digital Strategy

In February 2021, the Scottish Government published its Digital Strategy, A changing nation: how Scotland will thrive in a digital world, which emphasised the Scottish Government's aspirations to be an 'Ethical Digital Nation' which engenders trust in how it uses data and digital technologies. It set out its vision as:

> **… a society where people can trust public services and businesses to respect privacy and be open and honest in the way data is being used. But this is about more than the use of data. It is about trust, fair and rewarding work, democratic, social and cultural inclusion, climate change, the circular economy and making sure that the raw materials used in production are ethically sourced.**
>
> **A place where children and vulnerable people are protected from harm. Where digital technologies adopt the principles of privacy, resilience and harm reduction by design and are inclusive, fair and useful. This is not simple, nor quick work – but it is what we must work towards.**

The Scottish Government convened an independent expert group in digital ethics which published a report, Building Trust in the Digital Era: Achieving Scotland's Aspirations as an Ethical Digital Nation, in November 2022. Like the IEG, this was supplemented by public engagement in the form of 'a broadly representative group of 30 people from across Scotland to learn, discuss and deliberate on key aspects of digital ethics'. The report produced a series of recommendations including on environmental aspects of digital ethics, which is referred to above.

3.3.4 AI Strategy

The Scottish Government's AI Strategy for Scotland has been in development since 2021, as part of a partnership with the Data Lab and a multistakeholder steering committee and working groups. The Strategy sets out a vision and principles for AI in Scotland, with the aim of making Scotland 'a leader in the development and use of trustworthy, ethical and inclusive AI'. One activity the AI Strategy aims to achieve is to:

> **Secure safe, proportionate and privacy-preserving access to data for research and innovation in the public interest, including Open Data and Research Data Scotland**

Public sector personal data may be desirable to train AI, especially machine learning models. Work conducted by the GRAIMatter project at the University of Dundee in 2022 looks at this issue in more detail in the context of data from TREs/Safe Haven and makes a series of recommendations about how TREs could better accommodate this research while continuing to ensure privacy and security of TRE data (Jefferson et al., 2022).

3.3.5 Health and social care: data strategy

In February 2023, the Scottish Government and COSLA published the first data strategy for health and social care data, Greater access, better insight, improved outcomes: a strategy for data-driven care in the digital age. As mentioned many times in this document, health data is a very significant and valuable kind of personal data held by the Scottish public sector. While there are public sector personal data which is not related to health and social care, this strategy is still very important given the significance and value of this kind of data.

Among others, the Strategy 'sets a framework for the ethical, transparent use of data by health and social care providers' and introduces a 'shared set of ethical principles' which would apply to all kinds of organisations including 'an NHS organisation, a social care organisation, an academic body or a research company looking to utilise health and social care data' (p. 6). Of particular relevance to the IEG is the following principle:

> **We will always be clear about the intended benefits and potential risks that arise from our use of health and social care data for individual care, performance, and research.**

There is also the following Commitment:

> **As set out in Scotland's Digital Strategy, we will make more of our health and social care data available openly where it is safe, practical and lawful to do so. This will include providing an improved framework for open data to enable non-public sector organisations to access data in a safe way. This will support linking and usage of data to develop new insights and support innovation.**

Specifically on the theme of Supporting Research and Innovation, the Strategy makes the following commitments:

- **'We will seek to maximise the opportunities for data-driven research and innovation, with broad public support, to accelerate realisation of the public benefits.'**
- **'We will openly demonstrate and describe the uses, safeguards, and benefits of the use of health and care data for research and innovation.'**
- **'We will support access to health and social care data through trusted research and innovation environments, such as Scotland's 'Safe Havens', with appropriate approval processes providing assurance that data is used in line with ethical principles.'**
- **'We will consider the use of data for research and innovation in the design of all new developments set out in this Strategy to maximise the opportunities and public benefits.'**

Among the Strategy's deliverables, the following are most relevant to the IEG and UVOD programme:

- **'We will work to create clarification of the terms for access and use of data for industry projects including the approval and controlled access pathways to ensure ethical use in the public interest. This will be refined with the conclusions of the Scottish Government's Unlocking the Value of Data programme once completed.'**
- **'We will examine how we could support collaborative data-driven research and innovation across the UK and internationally where this has public benefits for Scotland, there is suitable agreement and it is ethical to do so' (p. 74).**

3.3.6 Equality Evidence Strategy 2023-2025

In March 2023, the Scottish Government published its new Equality Evidence Strategy, whose aim is:

> **to enable policymakers to develop sound and inclusive evidence-based policies to improve service delivery and outcomes for Scotland's people**

The Scottish Government's Vision is:

> **To tackle structural and intersectional inequality of outcomes, Scotland's equality evidence base will become more accessible, wide-ranging and robust. A stronger evidence base will enable the development and delivery of sound, inclusive policies and services and enable the measurement of improvements in the lives of all of Scotland's people.**

The Vision is supported by three core principles, of which the first is most relevant to the IEG's work:

1. **More robust and comprehensive data and evidence will be gathered on the intersecting characteristics of people in Scotland across a range of outcomes.**
2. **Equality evidence will be made more easily accessible so users will be able to access what they need, when they need it.**
3. **Good practice will be shared and promoted to support increased confidence and competence in the production and use of robust equality evidence.**

This new strategy follows the establishment of the Equality Data Improvement Programme in 2021, which 'aims to strengthen Scotland's equality evidence base which will in turn enable policy makers to develop sound and inclusive policy to improve service delivery and outcomes for people in Scotland with protected equality characteristics'.

3.3.7 Relationship to IEG and UVOD

The UVOD programme may contribute to these other policies by making data available for research and innovation, which may include AI development, and facilitating Scotland as an ethical digital nation through the governance of public sector personal data use by the private sector. Already, as mentioned, there are requests to use public sector personal data in Scotland for AI development, in particular machine learning model training (see Jefferson et al 2022). The UVOD programme is referenced explicitly by the health and social care data strategy and there are clear synergies and alignments there. Ensuring that public sector datasets are inclusive of protected characteristics will be key to ensuring that the Enabling Conditions in Principle #6 are realised.

At a broader level, ethical and appropriate governance of public sector personal data and its use by the private sector in certain circumstances may help fulfil the Scottish

Government’s National Performance Framework to ‘create a more successful country’ which increases wellbeing, decreases inequality and creates ‘sustainable and inclusive growth’, listing a series of outcomes.

3.4 Relevant organisations and initiatives in Scotland

For personal data held by the public sector, there are already some mechanisms for its access for research purposes, by academic and commercial researchers. One main mechanism is the Safe Havens which are also known as Trusted Research Environments (TREs). TREs, also known as 'Data Safe Havens' or 'Secure Data Environments', are highly secure computing environments that provide safe and secure access to personal data such as population data, census data and health data for approved researchers to use in research and development. In some cases, health data is linked to non-health data in TREs, but in other cases, non-health data is also available, not linked to health data, for research via TREs.

There are a series of user governance checks and controls that researchers and their projects must pass before they are granted access to the TRE and its data. There are also export controls that must be satisfied before they can withdraw any materials or outputs from the TRE. Typically, no identifying personal data is permitted to leave a TRE. TREs conduct Statistical Disclosure Checks to ensure that personal data cannot be inferred from publication-ready charts and tables. All data egress from the TRE is subject to inspection to make sure no original data, pseudonymised or otherwise, leaks into the public domain. In this way, TREs strike a balance between facilitating research through data access and preserving privacy and security. TREs in the UK are governed in accordance with aforementioned legal frameworks and the 'Five Safes' model: 1. Safe People; 2. Safe Projects; 3. Safe Outputs; 4. Safe Data; and 5. Safe Setting.

Research Data Scotland (RDS) is a collaborative initiative launched in 2020, involving the Scottish Government, Scottish public bodies and Scottish universities, which aims to 'facilitate insight from data and promote and advance health and social wellbeing in Scotland'. RDS is underpinned by the following principles:

1. **RDS will only enable access to data for research that is for the public good and considers equalities**
2. **RDS will ensure that researchers and RDS staff can only access data once it is deidentified**
3. **RDS will ensure that all data is always kept in a controlled and secured environment, using the FAIR principles of Findability, Accessibility, Interoperability, and Reuse of digital assets, and building upon the 5 safes data privacy framework**
4. **RDS will be user-and problem-led not data-led.**
5. **As a charity, all income that RDS generates will be re-invested into services to help researchers continue to access data, and firms that access public sector data for research in the public good through RDS will share any commercial benefits back into public services**
6. **RDS will be transparent about what data has been made available for research through its services and how it is being used for public benefit**
7. **Aligned with the Scottish data strategy, we will support people's appropriate choice over the use of their data in research.**

At the outset, RDS aims to provide a single point of access to researchers wanting to access data held by the Scottish public sector, with later stages involving RDS developing and cataloguing a dataset portfolio, and helping to streamline and clarify the processes by which researchers can access datasets.

Another initiative which works with RDS is Administrative Data Research Scotland (ADR Scotland). This is a partnership between the Scottish Government's Data for Research Unit and researchers in the Scottish Centre for Administrative Data Research at the University of Edinburgh, which 'help[s] to make administrative datasets more readily linkable and conducting research on a suite of critical issues in Scotland'. This research must be compliant with the ADR Scotland Strategy including the need for public benefit.

In the healthcare space, Public Health Scotland's electronic Data Research and Innovation Service (eDRIS) provides support to researchers who wish to access administrative datasets. eDRIS is another partner involved in RDS. Scotland hosts one of the six Health Data Research UK (HDR-UK) sites, co-ordinated by the University of Edinburgh, whose aim is to unite 'UK's health and care data to enable discoveries that improve people's lives'.

RDS envisages the use of data by academic/not for profit researchers but also by private sector organisations which may make profit. However, the following conditions would apply:

> **All results from research conducted through RDS must be capable of being published for the public benefit. Any commercial benefits will be shared back into RDS to improve public services. For private sector organisations, the same conditions apply for research institutions but a licensing model may be considered which will allow the benefits from the use of the data to be shared with other researchers.**

There are other services such as DataLoch: a collaboration between the University of Edinburgh and NHS Lothian, with other NHS boards in South-East Scotland joining later. The DataLoch service brings together health and social care data from South-East Scotland for research and service-management purposes. In 2021, some concerns about privacy were raised in a Ferret investigation about GP practices contributing patient data to the DataLoch service. The ICO engaged in positive discussion with the NHS Lothian team to consider the concerns raised regarding DataLoch, particularly those over aspects of both transparency and the data protection impact assessment. As a consequence, steps were then taken which improved practice accordingly.

In July 2022, the DataLoch service extended its governance framework to cover the new possibility of private-sector access to data extracts. (To date, no private-sector access to data has yet been granted.) The governance extension was informed by a DARE UK-funded public consultation focused on the principles of trustworthy access for a range of organisations. Furthermore, all research applications undergo a Public Value Assessment, where members of the public from DataLoch's Public Reference Group assess proposals to ensure there is sufficient public value to warrant support by the DataLoch service.

The Industrial Centre for Artificial Intelligence Research in Digital Diagnostics (iCAIRD) is another important collaboration in Scotland. iCAIRD was an Innovate UK research programme funded through the Industrial Strategy Challenge Fund. The programme was active between 1st February 2018 and 31st March 2023. iCAIRD was one of five AI Centres established across the UK. It brought together a pan-Scotland collaboration of 15 founding partners from across industry, the NHS, and academia; including four SMEs. At its peak it had '30 active partner companies, with over 30 current research projects across radiology and pathology'. The industry leads were Canon Medical Research Europe (radiology) and Royal Philips (digital pathology). iCAIRD established secure analytic research environments through the NHS Safe Havens in Glasgow, hosted by NHS Greater Glasgow and Clyde, and Aberdeen, hosted by NHS Grampian and University of Aberdeen. Through the programme collaborations, Canon Medical Research developed the Safe Haven AI Platform (SHAIP), a TRE software system suitable for hosting secure access to de-identified and pseudonymised patient healthcare data (including imaging, and non-imaging electronic healthcare records, reports, letters, and pharmacy data) within a high-performance compute environment for the development of AI and machine learning solutions within a Federated Data Network. The SHAIP system is managed by the Safe Havens and works within the established governance and guidelines. The key principle was to facilitate research on key health challenges in Scotland, providing access to NHS, academia, and industry researchers within a safe and secure environment where the data never left the NHS network. As part of the access arrangements, the appropriate system security procedures were reviewed, data protection impact assessments (DPIAs) were performed, and organisations were required to agree and sign suitable data sharing agreements. Then before individual researcher access could be granted, researchers were required to complete user governance checks, including;

- **Evidence of completion and accreditation of the Medical Research Council (MRC) e-learning course on 'Research, GDPR and confidentiality'.**
- **Confirmation they had read and understood the NHS Code of Practice on Protecting Patient Confidentiality.**
- **Complete basic disclosure checks, as evidenced through application and certification by Disclosure Scotland.**

In many ways, the approaches and advances made by the iCAIRD collaboration have helped to establish the concept and definition of a TRE. Indeed, the governance frameworks and processes established by the iCAIRD programme can provide an exemplar for private sector access to pseudonymised data held by the public sector in an established TRE. At the time of writing, SHAIP continues to support AI and machine learning research and development projects for healthcare applications at sites in Glasgow and Aberdeen.

The Scottish Government has set up two Public Benefit and Privacy Panels to scrutinise requests for public sector data. The first, set up in 2015, is the Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP), which is for requests for secondary use of NHS Scotland (NHSS) data held in NHSS health boards, which is managed and run within NHSS. The other panel, also set up in 2015, is known as the Statistics Public Benefit and Privacy Panel (S-PBPP) which reviews requests for SG and National Records of Scotland census data. Requesters must also demonstrate alignment between their data requests and the National Performance Framework (NPF). These PBPPs work in similar ways, and collaboratively where possible, but are independent due to the different legislation relating to the data involved and the data controllership. Once approval has been given from either panel, the data are usually made available in the Scottish National Safe Haven (for HSC-PBPP) or released directly to the requester (for S-PBPP).

In order to access health data held by the NHS in Scotland, especially from more than one NHS Board, applications are scrutinised by the NHS Scotland Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP):

> **The HSC-PBPP provides robust, transparent, consistent, appropriate and proportionate IG and scrutiny of data access requests to ensure the IG principles of safe people, safe projects, safe data, safe places are maintained.**

The HSC-PBPP is a 'patient advocacy panel' which ensures that public benefit and privacy implications of proposals to access data have been properly addressed and articulated in applications:

> **The HSC-PBPP need to balance public benefit with potential risk to privacy and ensure that the public interest will be furthered by the proposal, detailed in an application, and demonstrate that the social need for the processing of the data requested will result in a reasonable likelihood that it will result in a tangible benefit for society.**

The panel includes representatives of different stakeholders from across Scotland including the general public, NHS representatives, research representatives and technical specialists. Among the panel are also NHS Scotland Caldicott Guardians, who are senior members of organisations which process health and social care personal data and who ensure 'that the personal information about those who use the organisation's services is used legally, ethically and appropriately, and that confidentiality is maintained'. Caldicott Guardians employ eight Caldicott Principles 'to ensure people's information is kept confidential and used appropriately', which are:

- **Justify the purpose(s) for using confidential information**
- **Use confidential information only when it is necessary**
- **Use the minimum necessary confidential information**
- **Access to confidential information should be on a strict need-to-know basis**
- **Everyone with access to confidential information should be aware of their responsibilities**
- **Comply with the law**
- **The duty to share information for individual care is as important as the duty to protect patient confidentiality**
- **Inform patients and service users about how their confidential information is used.**

The HSC-PBPP has devised its own set of principles to address issues raised by private sector use of public sector personal data. The purpose of the principles is for the HSC-PBPP to try to ensure consistency across applications it receives and considers. These principles are not currently publicly available on the HSC-PBPP website but their release is planned as part of the next iteration of updates to HSC-PBPP's application form and guidance notes. The principles include the need for clarity of the partnership and roles of each actor, clarity on data protection law and policy compliance (a DPIA must be in place), clear justifications for the data request, a clear statement of public benefit, clarity about IP allocation over outcomes, ethics approval (where needed) and external independent scientific peer review, and public engagement and transparency.

Individual NHS Boards in Scotland have their own Caldicott Guardians for reviewing access requests to personal data for the purposes of service evaluation, audit and research.

3.5 Scottish Government commissioned research and engagement

As part of the UVOD programme, the Scottish Government has commissioned three literature reviews to accompany and inform the IEG's work. We summarise them here, as they will also be published in full on the Scottish Government's website to accompany this Report.

3.5.1 Public Engagement around the Access of Public Sector Data with or by Private Sector Organisations – August 2021

This literature review was conducted by Sonja Erikainen and Sarah Cunningham-Burley from the University of Edinburgh Centre for Biomedicine, Self and Society, and delivered to the Scottish Government in August 2021, prior to the start of the IEG. The literature review considered public engagement activities on the use of public sector data by or with the private sector from ten years prior to 2021 and looked at developments in Scotland, the UK and internationally. While ostensibly the review looks at 'public sector data', in practice the resources cited mostly concern 'personal data' more specifically that is held by the public sector, and within that personal data, much of it relates to health data.

The authors identified different kinds of public engagement and research methods used which were grouped under 'deliberative', 'dialogic' and 'qualitative', and generated eight key themes from the literature: low public awareness, 'gut reactions', and changing perceptions around data use; acceptability of private sector data uses; the centrality of public benefit; importance of benefit-sharing and distribution; trust and distrust; oversight, governance, and safeguards; public involvement and engagement; and the impact of demographic differences of people's views.

The key findings of the review are:

- **'Deliberative and dialogue based qualitative public engagement and research methods are effective in identifying informed and considered public views on private sector use of public sector data, and they can enable the construction of a public consensus that can be used to inform decision making.**
- **'There is a low level of public awareness and understanding of private sector access to public sector data and how this data is used. Publics tend to express negative 'gut reactions' towards the topic, but when provided with more information and opportunities to reflect on or deliberate it, they often change their minds.**
- **'There is widespread conditional acceptance of private sector use of public sector data especially among informed publics. Acceptability is most conditioned by the rationales for the data use, but also by the type of data being used and the type of the private sector organisation using it. Public benefit is the primary driver of acceptability and commercial gain or private profit the primary driver of unacceptability.**
- **'Demonstratable public benefit is the most prevalent consideration**

that publics have around private sector access to and use of public sector data. While the definition and scope of ‘public benefit’ is open and contested, publics want to see evidence that public benefit of some kind is the primary driver of public sector data access, that it can actually be achieved, and that it outweighs any possible private benefits.

- ‘Publics want to see the development of equitable benefit-sharing models for collaborations or partnerships between private and public sector organisations, as they expect benefits – including profits – to be returned to publics and reinvested into the public sector.
- ‘Public trust and distrust are key factors around private sector access to public sector data. While publics tend to be relatively distrustful of private sector organisations, they generally have a high level of trust in the public sector, and this is shaped by perceptions that the public sector is acting for public benefit whereas the private sector is motivated by private interests. Publics are more trusting of private sector uses of public sector data when public sector organisations retain control over the data during collaborations with the private sector.
- ‘Publics expect to see stringent oversight, governance, and safeguard arrangements around private sector use of public sector data, especially concerning an oversight or governance body, transparency and accountability processes, and arrangements for data security and safety, consent, and confidentiality. However, the precise nature of what the safeguards should be is contested, and it may be that the nature of the safeguards is less important than the fact that effective safeguards exist.
- ‘Publics want there to be public involvement or engagement processes and activities around private sector use of public sector data, but the precise nature of what this should look like, who should be involved and in what ways is contested while some want to be actively involved in decision making, others prefer more passive forms of communication and information distribution, and proportionality matters.
- ‘There is no singular ‘public perspective’ on private sector use of public sector data, but rather, while overarching patterns can be identified, publics are plural, and individuals’ views are shaped by a diverse range of intersecting demographic and attitudinal variables.’

3.5.2 Public sector personal data sharing: Framework and Principles – December 2021

This literature review was conducted by another team from the University of Edinburgh and delivered to the Scottish Government in December 2021, before the start of the IEG. The research team comprised: Steven Earl, Morgan Currie, Matjaz Vidmar and Victoria Gorton, who comprise multidisciplinary backgrounds.

The review contained an analysis of frameworks and practices to provide access to public sector personal data for private sector organisations. The research team noted that 'this practice is extremely rare as it involves considerable legal, moral or ethical risks, including damage to public trust in the private sector'. The team identified two 'broad pathways' for facilitating public to private sector personal data sharing: data sharing agreements (which were the most common); and specific legislation for data sharing. They also identified an emerging third pathway being developed for artificial intelligence (AI) applications. The team also interviewed nine individuals from the public, private and third sectors in Scotland, Europe and globally to gain a deeper understanding of how these pathways worked in practice.

Data sharing agreements are the most common pathway in the UK, other European countries and elsewhere, involving the identification of the public interest and the drawing up of a data sharing agreement. The team notes that 'this pathway is currently predominantly used to facilitate sharing personal data held by the public sector to accredited research organisations'. On the occasions on which public sector personal data is shared with the private sector, this is the pathway used. The research team notes that the technical approaches used to manage the data sharing process vary, from the personal data being further processed and stored in a separate safe environment such as the Safe Havens, to data remaining in the original public sector organisation's database and researchers only being returned the results of their analysis.

Supplementing data protection law (EU General Data Protection Regulation and Law Enforcement Directive in the European Union, Data Protection Act 2018 and UK GDPR in the UK, see discussion above), the second pathway involves further, specific legislative frameworks being used to facilitate or restrict data sharing. UK examples given include the Serious Crime Act 2007 which permits the disclosure of personal data to specific anti-fraud organisations to prevent fraud. Another example is given from Finland of the Act on the Secondary Use of Health and Social Data, to facilitate the reuse of health and social care data, which is at an early stage of implementation and involves:

> **A separate permit authority will be set up – Findata – that will enable a centralized system for the issuing of the data requests and permits, rather than requiring sharing agreements with each data controller (as is the case in the UK).**

The third emerging pathway relates to the 'new demands for larger-scale data sharing' implicated by AI development. Currently much personal data used by AI projects is done on the basis of consent. However, the EU's draft AI Act includes provisions (Articles 53-55) for a 'regulatory sandbox' with terms for the re-use of personal data within the sandbox, and Earl et al. (2021) consider that this might form a third pathway which would be applied to crime, public security, public health and safety and environmental issues.

The team note technical barriers to data sharing (lack of harmonisation across agencies), legal barriers (overlapping and complex legislative frameworks e.g. health data), conservatism about sharing data among public sector organisations and a lack of willingness at times to explain the reasoning behind decisions to refuse access, and public concern about private sector access to public sector personal data. They consider that the current situation can be improved:

> **Existing pathways for data sharing with researchers – and by implication, other parties – can be improved by creating shared data standards and protocols across agencies, demonstrating public value and involving the public in the designs of infrastructure and data sharing models, marketing the value of data sharing to immediate stakeholders and users, developing a central resource that facilitates data sharing and makes these procedures transparent, and sharing ethical standards and best practices internationally.**

3.5.3 Private sector access to public sector personal data: exploring data value and benefit-sharing – December 2022

The third literature review, conducted by Anna Berti Suman (European Commission Joint Research Centre) and Stephanie Switzer (University of Strathclyde Law School), concerned how costs and benefits can be shared between the public and private sector vis-a-vis access to personal data, and intellectual property (IP) and royalty schemes relating to private sector use of public sector personal data.

A summarised version of key findings from their work is:

- **'Public-sector bodies generally lag behind in developing and implementing data sharing regimes compared to the private sector'; however, there are existing good practices in policy areas such as public health.**
- **'Studies demonstrate that ordinary people are supportive of health and social care data being used for public benefit but wish those public benefits to outweigh private profits and interests.'**
- **When assessing costs and benefits, these 'should not be conceived of as solely financial but understood in broader, more social terms'.**
- **Prerequisites for achieving public benefit include transparency and public engagement to ensure a social license.**
- **There is, however, some concern that a 'lack of a definition of public benefit may enable the concept to be exploited to facilitate […] commercialisation of government-held personal data'.**
- **'There is a vast literature on data value in general', with the notion of such value informed by the 'underlying context and socio-technical settlement' prevalent within society.**
- **There were concerns that the '"assetisation" of personal data may influence conceptions of value, thereby potentially resulting in a lack of public scrutiny and inequity'. To overcome such issues, 'value co-creation and exchange beyond the market' was suggested.**
- **'Benefit-sharing is a concept typically associated with international environmental law and in particular, international biodiversity law to deliver commutative and distributive justice. Benefit-sharing is thus linked to justice and emphasises the optimisation of benefits to society, together with the minimisation of harm, and the achievement of equity.'**
- **'If data has the potential to benefit the public, it should be shared. Public benefit cannot be obtained in the absence of such sharing. However, the absence of common principles for trusted government-**

to-businesses (G2B) personal data sharing may lead to restrictions on data flows resulting in detrimental economic impacts.[…] Legal certainty is key for such sharing to take place.'

- Creative personal data sharing schemes are 'being established between civic organisations and private actors (at times also engaging the public sector)' for certain citizen science activities, 'with creative commons licensing schemes, value co-creation, and the reality of "data cooperatives"'.
- 'There is growing attention in the literature for the concept of 'data altruism' as also incorporated in the European Union Data Governance Act; this reflects a tendency to embrace a fair and open sharing of personal data for public benefit.' However it is restricted to not for profit uses of data, which may exclude much if not all private sector involvement.

The researchers also identified a set of key guiding principles:

- 'proportionality,
- transparency,
- public engagement,
- co-creation of the concept of value,
- legal certainty, and
- respect for ethical values and norms'.

3.6 DemSoc Public Engagement

The Scottish Government commissioned the Democratic Society (DemSoc) to conduct some initial public and stakeholder engagement activity on the principles in their draft form (which were published in August/September 2022). Two co-creation workshops with stakeholders and some IEG members, and two public workshops were held between November 2022 and January 2023. DemSoc conducted a feedback questionnaire with workshop participants and did some desk-based research on potential methods for future participatory engagement.

Key messages from participants at the two public workshops are:

- **'Building public trust is really important. To build trust, do not turn the principles into a box-ticking exercise and build public awareness on the security of data and how it is used, stored, shared.**
- **'It's important to make it clear and transparent how someone can follow data and what data is publicly available. There needs to be a robust system in place on how to monitor the data for accountability.**
- **'Review whether our current model of consent, ownership and privacy is efficient and informed. There needs to be a re-evaluation of how people gain access and rights to their personal data and the ability to say 'no' to storage of their personal data.**
- **'Clear and specific language needs to be used. For example, when referring to ethical standards, laws and guidelines, they need to be clearly stated and referenced.**
- **'Need an international approach in order to consider how international laws might impact the UVOD programme in Scotland and also take inspiration and best practice from other countries.'**

3.7 Public benefit, public interest and value

What is public benefit, public interest and value? These terms are key for our work, but are contested and open to different interpretations. We cannot take account of all these contestations and interpretations here, but we put forward a summary.

What can be characterised as public benefit, interest and value are deeply context-specific, depending on the values and objectives of a society, community, nation, individual, etc. As Harvey and Laurie (2021) put it: ‘Actions taken in the public interest can be broadly described as those that promote objectives valued by society’.

3.7.1 Public benefit

The first literature review conducted by Erikainen and Cunningham-Burley (2021) clearly sets out the importance of public benefit in the public sector data context:

> **Demonstrable public benefit is the most prevalent consideration that publics have around private sector access to and use of public sector data. While the definition and scope of ‘public benefit’ is open and contested, publics want to see evidence that public benefit of some kind is the primary driver of public sector data access, that it can actually be achieved, and that it outweighs any possible private benefits. (Erikainen & Cunningham-Burley, 2021, p.1)**

This relationship – between acceptability and public benefit – is further illustrated by a Wellcome study (Ipsos MORI, 2017) in relation to health data and public attitudes to commercial access. This specifically considered private sector access to data and the conditions under which this may or may not be permissible, and describes how participants applied four key tests (Figure 1.3) when considering the acceptability of data usages.

Decisions around acceptability may exist on a sliding scale, with those that have clear public benefit at one end, and those that have solely private benefit at the other. Further, it points to a space where these benefits may be ‘mixed’ in nature.

In the academic sphere, Aitken and colleagues have written extensively about the public engagement work they have conducted in relation to health data sharing, including in the Scottish context (Aitken et al., 2016). In particular, their work in relation to public expectations of public benefits from data-intensive health research (Aitken et al., 2018) has indicated that the term ‘public’ may be construed broadly, so that data usage can benefit as many people as possible. However, understandings of relevant publics may also be needs-led: in other words, there may be broader public benefit in research using data that benefits a smaller group or number of people in need (for example, research in relation to rare diseases). Similarly, Aitken and colleagues found that participants’ preference in terms of the types of benefits was to keep this broad – so, in the context of health research, these benefits were not just seen as medicalisation, but also related to living longer, happier, and healthier lives. Perhaps more notably, publics were also concerned that such benefits should be measurable, and that these would actually be realised through the actions of key policy and government stakeholders.

The Office for National Statistics gives some guidance on how public benefit can be demonstrated by those seeking to conduct research using its data, whereby it stipulates that one of the criteria must be demonstrated:

- **provide or improve evidence bases that support the formulation, development or evaluation of public policy or public service delivery**
- **provide an evidence base for decisions that are likely to significantly benefit the UK economy, society or quality of life of people in the UK**
- **significantly extend existing understanding of social or economic trends or events, either by improving knowledge or challenging accepted analyses**
- **replicate, validate, challenge or review existing research (including official statistics) in a way that leads to improvements in the quality, coverage or presentation of existing research.**

In 2022, the ONS and Administrative Data Research UK (ADR UK) published a report comprising insights gleaned from research conducted with publics in the UK (including in Glasgow) on what they considered to be 'public good' (considered interchangeable with 'public benefit' and 'public interest') use of data for research and statistics. The research produced five 'key findings' which emerged from discussions which took place with a diverse sample of participants:

- **'Public involvement: Members of the public want to be involved in making decisions about whether public good is being served'**
- **'Real-world needs: Research and statistics should aim to address real-world needs, including those that may impact future generations and those that only impact a small number of people'**
- **'Clear communication: To serve the public good, there should be proactive, clear, and accessible public-facing communication about the use of data and statistics (to better communicate how evidence informs decision-making)'**
- **'Minimise harm: Public good means data collected for research and statistics should minimise harm (and not contribute to anything harmful), including an awareness of unintended harmful consequences of the misrepresentation of data research and statistics'**
- **'Best practice safeguarding: Universal application of best practice safeguarding principles to ensure secure access to data should help people feel confident to disclose data.'**

Another recent public dialogue, which was co-funded by the National Data Guardian for Health and Social Care (for England) amongst others, provides a deep dive into public benefit, exploring how this might be assessed in the data context (Hopkins Van Mil, 2021). This was conducted in the context of health and care data with around 100 participants, and its findings underline the need for transparency throughout the data lifecycle, and for authentic public engagement with a cross-section of society, amongst other matters.

In late 2022, the National Data Guardian issued guidance on evaluating public benefit for uses of health and social care data for purposes beyond individual care, which include but are not limited to research and innovation. While this guidance is not applicable to Scotland, it may be useful for us to take on board in considerations of public benefit. The NDG's public dialogue informed this definition of 'public benefit':

> **Public benefit means that there should be some 'net good' accruing to the public; it has both a benefit aspect and a public aspect. The benefit aspect requires the achievement of good, not outweighed by any associated risk. Good is interpreted in a broad and flexible manner and can be direct, indirect, immediate or long-term. Benefit needs to be identifiable, even if it cannot be immediately quantified or measured. The public aspect requires demonstrable benefit to accrue to the public, or a section of the public.**

The NDG recognises that its definition of public benefit also reflects the Charity Commission's interpretation of the public benefit required in charity law, discussed in more detail below. The Guidance reiterates the need for transparency and public engagement for earning public trust in secondary uses of unconsented data, along with 'proportionate governance processes and building in ongoing evaluation and learning'.

As regards use of data by the private sector, the NDG states that:

> **If the only benefit of a specific data use is the generation of profit by a commercial organisation, that use cannot be deemed for public benefit. However, the generation of proportionate commercial profit may be acceptable to the public if the use also delivers a public benefit, such as improved services or improved NHS knowledge and insights. When assessing proportionality, the public benefit evaluation process should ask the data applicant to provide a transparent assessment of how the commercial interests are proportionately balanced with the benefits to the public.**

The NDG points to guidance for NHS (England) organisations entering data sharing agreements with third parties to help realise patient and NHS benefits. The NDG also points to the importance of 'fairness' in weighing public and private benefit, which is further elaborated in a report from Understanding Patient Data and the Ada Lovelace Institute, and DHSC Guidance on creating frameworks for realising patient and NHS benefit. NDG also points to the Centre for Improving Data Collaboration, part of the former NHSX in England (which has now been integrated into the NHS Transformation Directorate), whose remit is to support fair data sharing partnerships. In terms of understanding benefit, the NDG public dialogue findings demonstrated that:

> **people think the concept of public benefit should be broad and flexible and include direct, indirect, and long-term benefits. People also told us**

the benefit needs to be identifiable, even if it cannot be quantified or measured.

From the dialogue, a list of indicative questions was formulated to help determine whether an intended purpose can be considered for public benefit, which range from very concrete and measurable benefits to more abstract benefits such as the support of knowledge creation and exploratory research.

For partnerships with the private sector, the NDG drawing on the public dialogue presents three (illustrative, non-exhaustive) suggestions for discerning public rather than private benefit:

- **'Will any private profit, or progress made by a commercial organisation, also lead to benefits for the health and care system that will ultimately benefit patients? For example, improving how the NHS operates by increasing service or administrative efficiency?**
- **'Where a commercial organisation makes private profit or progress that serves its own interest, is the agreement that underpins its partnership with the NHS based on fair terms? Does that agreement recognise and safeguard the value of the NHS data on which the organisation's profit or progress is founded?**
- **'Will research findings be openly shared with others who can use them to maximise benefits to patients, the wider public, and the health and social care system?'**

The NDG further recommends that data users should be prepared to demonstrate the public benefit being delivered, as specified by the public sector organisation providing the data and should be shared with the public e.g. in a data uses register, with this being particularly important when the user is seeking renewed or additional access to data, in which case public benefit up to that point should be demonstrable.

Once public benefit has been established, the NDG recommends a consideration of the risks inherent in that data use. Risk should be avoided, and if not possible, minimised with sufficient safeguards, and if it still exists, an assessment of whether 'on balance, the public benefit is sufficient to justify running that residual risk'? Anonymous data will significantly reduce risks to privacy and 'are unlikely to outweigh a public benefit'. Furthermore the risks of not using data may be more detrimental to public benefit than the risks of using the data, and this should also be taken into consideration (see e.g. Jones et al., 2017). The risks of non-use can be economic in nature, that placing overly burdensome barriers in the way of accessing public sector personal data could damage favourable economic activities related to research, development and innovation.

Public benefit is not a concept confined to data issues, as recognised by the NDG above. In Scottish charity law (Charities and Trustee Investment (Scotland) Act 2005 section 7) a charity is a body which only has charitable purposes and which provides or intends to provide public benefit in Scotland or elsewhere. Section 8 of the 2005 Act stipulates that public benefit cannot be presumed from any particular purpose, and in determining whether a body provides or intends to provide public benefit, regard must be had to:

> (a) how any–
>
> (i) benefit gained or likely to be gained by members of the body or any other persons (other than as members of the public), and
>
> (ii) disbenefit incurred or likely to be incurred by the public, in consequence of the body exercising its functions compares with the benefit gained or likely to be gained by the public in that consequence, and
>
> (b) where benefit is, or is likely to be, provided to a section of the public only, whether any condition on obtaining that benefit (including any charge or fee) is unduly restrictive.

The Scottish Charity Regulator (OSCR) explains that:

> **To see whether an organisation provides public benefit or (in the case of applicants) intends to provide public benefit, we look at what it does or plans to do to achieve its charitable purposes.**

Public benefit under charity law relates to a subcategory of activities providing public benefit in a charitable sense which is to advance an organisation's charitable purposes. Nevertheless, looking at charity law can be useful for considerations of public benefit in other contexts.

OSCR takes a broad view of what 'benefit' and 'public' mean, acknowledging many forms of benefit, tangible and intangible, but that they must be identifiable. 'Public' can refer to the general public but also to subsets of the public, e.g. a particular community, children or people with specific needs. To demonstrate that a charity provides public benefit, OSCR states that it must describe the work they do and their achievements in their annual report, which is publicly available as well as subject to review by trustees. In assessing public benefit, OSCR adopts the following process:

> - **The comparison between the benefit to the public from an organisation's activities; and**
>   - **any disbenefit (which is interpreted as detriment or harm) to the public from the organisation's activities**
>   - **any private benefit (benefit to anyone other than the benefit they receive as a member of the public).**
> - **The other factor that we must take into account in reaching a decision on public benefit is whether any condition an organisation imposes on obtaining the benefit it provides is unduly restrictive. This includes fees and charges. See undue restrictions for more information**

It considers public benefit from a holistic perspective, 'based on all the facts and circumstances applying to the organisation'.

In England and Wales, the regulator, the Charity Commission, has also provided guidance on the public benefit requirement in the context of the Charities Act (Charity Commission, 2013; plus updated format 2017). Again, to satisfy the 'benefit aspect' of public benefit, 'a purpose must be beneficial' and 'any detriment or harm that results from the purpose must not outweigh the benefit'; to satisfy the 'public aspect' of public benefit the purpose must 'benefit the public in general, or a sufficient section of the public' and 'not give rise to more than incidental personal benefit' (Charity Commission, 2013, p. 5). As noted above, this is also a distinction explored in research conducted by Aitken et al. (2018), and adopted and adapted by the NDG in its guidance for England discussed above.

3.7.2 Public interest

To turn next to notions of 'public interest', it is apparent that this term can be equally, if not more, elusive. In the context of health research regulation, it has been claimed that 'actions taken in the public interest can be broadly described as those that promote objectives valued by society' (Harvey & Laurie, 2021).

More specifically, in the context of data use, the public interest is a prominent feature of the policy and legal regimes that govern the use of confidential data – for example in data protection legislation and the common law duty of confidentiality in the UK. However, neither this legislation nor case law provide a definition of what is, or is not, 'in the public interest'. Indeed, what emerges from these discussions is that, much like public benefit, the public interest is deeply contextual, and so perhaps we should consider what the public interest 'does', rather than solely what it 'is', and how it may relate to other similar terminology, such as the public benefit.

The Information Commissioner's Office (ICO) recently (2022) consulted on guidance on the research provisions in the UK's DPA 2018 and GDPR, and stated in the published guidance:

> **The legislation does not define the 'public interest'. However, you should broadly interpret public interest in the research context to include any clear and positive public benefit likely to arise from that research.**
>
> **The public interest covers a wide range of values and principles about the public good, or what is in society's best interests. In making the case that your research is in the public interest, it is not enough to point to your own private interests.**

The 'public interest' is not defined in the legislation although as mentioned in section 3.2.1 above, the ICO has given some indicative examples of what it may constitute. For special category data, a 'substantial public interest' is one of the grounds on which special category data can be processed (UK GDPR Art 9(2)(g), see also section 10(3) of the DPA 2018). There are 23 specific substantial public interest conditions set out in Schedule 1 of the DPA 2018:

- **Statutory and government purposes**
- **Administration of justice and parliamentary purposes**
- **Equality of opportunity or treatment**

- Racial and ethnic diversity at senior levels
- Preventing or detecting unlawful acts
- Protecting the public
- Regulatory requirements
- Journalism, academia, art and literature
- Preventing fraud
- Suspicion of terrorist financing or money laundering
- Support for individuals with a particular disability or medical condition
- Counselling
- Safeguarding of children and individuals at risk
- Safeguarding of economic well-being of certain individuals
- Insurance
- Occupational pensions
- Political parties
- Elected representatives responding to requests
- Disclosure to elected representatives
- Informing elected representatives about prisoners
- Publication of legal judgments
- Anti-doping in sport
- Standards of behaviour in sport

As ‘public interest’ is broader than ‘substantial public interest’, the public interest may encompass these substantial public interest conditions but may also encompass other conditions which are not listed here. We also note the limitations of these high level conditions which provide some detail, but little in the way of context. Furthermore, some of these public interest conditions such as ‘insurance’ may not be appropriate for the reuse or further use of public sector personal data by the private sector, as opposed to the private sector collecting personal data directly for its own services and products.

Turning to other research, the connection is made between public interest and public benefit, to argue that a principal function of the public interest in law is ‘to carve out a legally legitimate space within which [research] activities that infringe on individual interests but have potential public benefits can be lawfully conducted, which otherwise would not be permitted’ (Sorbie, 2022). However, the argument is also made for a conception of the public interest that is socially (as well as legally) legitimate, pointing to the difficulties of defining this term on the basis of a homogenised conception of who ‘the public’ are, and in the absence of engagement with actual publics’ views (for example, see Sorbie, 2020; 2021).

Indeed, as Erkainen and Cunningham-Burley (2021) recognise:

> **There is no singular ‘public perspective’ on private sector use of public sector data, but rather, while overarching patterns can be identified, publics are plural, and individuals’ views are shaped by a diverse range of intersecting demographic and attitudinal variables.**

Taken together, it has been argued that the public interest is best understood in ways that foreground relationality, temporality and accountability (Sorbie, 2022). In short, relationality requires that, as noted above, the diversity of and within ‘publics’ should be explored, as well as how context can shape these interests. Temporality points to the ways in which data use, on the one hand, and the public interest, on the other, overlap and intersect each other throughout the entire data lifecycle, therefore underlining the need for ongoing review. Finally, accountability emphasises the nuanced role of transparency in multifactorial decision making, yet underlines that mere transparency is in no way a synonym for accountability. These are all features that are reflected in our principles.

Furthermore, in the UK context, Cheung (2020, pp. 7-8) points to the mis-alignment between what publics may consider to be of public benefit in health data use and government priorities ‘of stimulating economic growth through maximising value from NHS data, particularly through private-sector collaboration’. Indeed, ultimately what the public interest and public benefit are may be, as Scassa and Vilain (2019, p. 11) put it, ‘perceived differently depending on social circumstance or ideology’.

In our formulations of public interest and public benefit in the Guiding Principles we have aimed to take account of the diversity of the publics, the need for meaningful and ongoing engagement on these and other issues, as well as the need for transparency and accountability. We hope this also goes some way to correcting the misalignment identified by Cheung (2020) above as regards what the public views as beneficial and what the government may view as beneficial when using public sector personal data by the private sector.

3.7.3 Value

We view the concept of 'value' in a very broad sense encompassing economic, social and environmental aspects. We do not define what 'value' is beyond this, only noting that the value produced by private sector access to public sector personal data should not be solely economic or financial but should also encompass social and environmental value. Yet, what value is in any of these contexts, like the terms public benefit and public interest discussed above, will be contextual and dependent on the values and objectives of the society, community and individual.

At a societal or national level, we find a vision of value in the Scottish Government's National Performance Framework (which is also Scotland's localisation of the UN Sustainable Development Goals) with its aims to:

- **create a more successful country**
- **give opportunities to all people living in Scotland**
- **increase the wellbeing of people living in Scotland**
- **create sustainable and inclusive growth**
- **reduce inequalities and give equal importance to economic, environmental and social progress.**

The NPF also contains three values:

- **treat all our people with kindness, dignity and compassion**
- **respect the rule of law**
- **act in an open and transparent way.**

These could guide what 'value' means when it comes to private sector access to public sector personal data producing 'value'.

Nevertheless, the idea of 'value' or the kinds of steps which are required to achieve it may be deeply ideological and individualised. Notions such as 'growth' are not universally accepted; indeed, especially in the context of environmental economics, there is a rich discussion of the need for 'degrowth' (see e.g. Kallis et al., 2018; Enough! Collective, 2022). Even if the NPF is followed, there may be differing opinions on how the aims are achieved e.g. via more government intervention in markets, by the private sector leading economic activity with minimal interference, or by individuals and local communities taking a lead, etc.

We will not engage more in these debates here (as there is unlikely to be consensus on these issues from IEG members). Suffice it to say that if 'unlocking' the 'value' of public sector personal data for use by the private sector in Scotland is to be achieved, questions about what 'value' this is require resolution as part of broader democratic (political economic) discussions involving the Scottish Government, Parliament and people in Scotland. Equally, there needs to be parallel conversations about what 'harm' is and any harm and costs which might also be generated by data use. Conflicting values must also be taken account of in such democratic debates.

3.8 Critical views on (digital) data

There is a critical vein of research, especially from humanities and social sciences, on the involvement and role of (large) private sector organisations, especially transnational corporations, in digital data and technologies. Some of these companies, such as Google (Alphabet), Meta (Facebook), Apple, Amazon and Microsoft possess significant economic - and political - power in many countries including Scotland and the UK, and in some cases they are economically bigger and more powerful than countries (see e.g. Daly, 2016). From this economic power also comes computational power, especially in the form of the resources and infrastructures needed to facilitate the level of data processing capacities that increasingly only the private sector can provide (Durante, 2021).

Concern has also been raised about such large transnational private sector organisations in digital technologies offshoring their tax obligations and paying only minimal amounts in countries such as the UK (see e.g. Klinge et al., 2022). Furthermore, there is concern about the labour practices of some of these large companies including Amazon in the UK (Briken & Taylor, 2018). While it is the labour practices of low-waged Amazon workers in fulfilment centres which has caused most concern, it is of note that the company is an infrastructure provider for some TREs through its Amazon Web Services cloud service.

Although beyond the scope of the IEG's work, there is also concern about the role of governments/the public sector in digital technologies and data gathering, including surveillance activities (see e.g. Keenan, 2021) and/or the often unintentional monetisation of personal data via third party platforms used in the public sector (e.g. Microsoft), situated within the larger global digital infrastructure (see e.g. Srnicek, 2017; Van Dijck et al., 2018). These concerns often relate directly to issues surrounding inequality and human rights. From biased, predictive policing based on digital data (Browning & Arrigo, 2021; Eubanks, 2018), to data gathered for health purposes which are then used for immigration enforcement purposes, which particularly affects asylum seekers and undocumented migrants (Waterman et al., 2021; see also Papageorgiou et al., 2020): existing debates thus critique such discriminatory practices through the weaponisation of digital data against vulnerable groups already marginalised in society (see e.g. O'Neil, 2017).

The involvement of large digital private sector organisations in using public sector personal data, especially in health, has proved controversial in other parts of the UK. One example is the Google DeepMind-Royal Free partnership (Powles & Hodson, 2017), which the ICO ultimately found did not comply fully with data protection law. Current controversies relate to the involvement of Palantir in providing data infrastructure for the NHS in England (see Dyer, 2021; Iliadis & Acker, 2022; Salisbury, 2023). Cheung (2020, p.1) has pointed to the involvement of such players in the health data space as rendering public sector health data 'potentially subject to the logics of data accumulation seen elsewhere in the digital economy'.

While commentators have critiqued and raised concerns about these (and other) aspects of data, there is also a vein of research on what more progressive and inclusive data and digital futures might look like, including concrete proposals for models and approaches which would better serve the public interest. Among these are the work on Good Data (Daly et al., 2019; see also Hartman et al., 2020) and Data Justice (Dencik et al., 2022). We can also look to Indigenous Data Sovereignty (IDS), developed by First Nations scholars to ensure that the creation and use of data realises their rights under the United Nations Declaration on the Rights of Indigenous Peoples (Kukutai & Taylor, 2016). The approaches and models developed by IDS scholars can inform more equitable data collection and use for non-Indigenous people and communities as well (Carroll Rainie et al., 2019).

We have very briefly touched on models which may facilitate greater public participation and control over (personal) data in Recommendation #10, which include personal data stores, data cooperatives and data trusts (Nanada & Narayan, 2022). However it is important to note the limits and shortcomings of certain applications of these models as well, such as the example of a data trust given by Scassa (2020) which was top-down and originating from a single stakeholder. While there was no consensus among the IEG on recommending an opt-out function, opt out can be considered as an 'ultimate' form of individual control, especially vis-a-vis private sector use of public sector personal data.

Another issue on which there was no IEG consensus was intellectual property (IP) arrangements between the public and private sector over (aspects of) the process and outputs of using public sector personal data. Private sector use of IP has a long and contested history, including as regards (personal) data and benefit-sharing (see e.g. Lucas et al., 2013; Andanda 2019).

Issues have arisen more recently around IP, especially commercial confidentiality, blocking access to public sector personal data including use by other public sector organisations (see e.g. Goldacre & MacKenna, 2020 on this issue in NHS England). The Financial Times, in an investigation of data sharing from NHS England in 2021, found that:

> **insights from the data were often shared or sold on to other commercial entities and providers that use it to price products being sold back to the NHS, or conversely restrict the NHS's access to analysis of its own data, creating conflicts of interest. Among the biggest criticisms focused on the opacity around the data's fate after it leaves the NHS's servers, and the lack of an auditing trail beyond the companies on the [Data Use] register (Murgia & Harlow 2021).**

To remedy this, Pasquale (2013, p. 683) advocates that:

> **Policymakers need to skillfully navigate areas of law often used to stop the sharing of data, including intellectual property rights and contractual obligations.**

This should be taken into account in devising contracts and equitable benefit-sharing for the use of public sector personal data by the private sector in Scotland.

References

Ada Lovelace Institute. (2020). Foundations of Fairness: Where next for NHS health data partnerships. Retrieved from https://understandingpatientdata.org.uk/sites/default/files/2020-03/Foundations%20of%20Fairness%20-%20Summary%20and%20Analysis.pdf

ADR-UK. (2022). A UK-wide public dialogue exploring what the public perceive as 'public good' use of data for research and statistics. Retrieved from https://www.adruk.org/fileadmin/uploads/adruk/Documents/PE_reports_and_documents/ADR_UK_OSR_Public_Dialogue_final_report_October_2022.pdf

Aitken, M., Cunningham-Burley, S., & Pagliari C. (2016). Moving from trust to trustworthiness: Experiences of public engagement in the Scottish Health Informatics Programme. Science and Public Policy, 43(5) 713–723. doi:10.1093/scipol/scv075

Aitken, M., Porteous, C., Creamer, E., & Cunningham-Burley, S. (2018). Who benefits and how? Public expectations of public benefits from data-intensive health research. Big Data & Society, 5(2). doi:10.1177/2053951718816724

Andanda, P. (2019). Towards a Paradigm Shift in Governing Data Access and Related Intellectual Property Rights in Big Data and Health-Related Research. IIC - International Review of Intellectual property and Competition Law 50, 1052–1081. doi:10.1007/s40319-019-00873-2

Berti Suman, A. & Switzer, S. (2022). Private sector access to public sector personal data: exploring data value and benefit-sharing. (Scottish Government commissioned literature review).

Briken, K., and Taylor, P. (2018) Fulfilling the 'British way': beyond constrained choice–Amazon workers' lived experiences of workfare. Industrial Relations Journal, 49, 438–458. doi:10.1111/irj.12232.

Browning, M., and Arrigo, B. (2021) Stop and Risk: Policing, Data, and the Digital Age of Discrimination. American Journal of Criminal Justice, 46 (2), 298-316. doi:0.1007/s12103-020-09557-x

Caroll Rainie, S., Kukutai, T., Walter, M., Figueroa-Rodriguez, O.L., Walker, J., & Axelsson, P. (2019). Indigenous data sovereignty. In T. Davies, S. Walker, M. Rubinstein & F. Perini (Eds.), The State of Open Data: Histories and Horizons. Cape Town and Ottawa: African Minds and International Development Research Centre.

Charity Commission for England and Wales. (2013). Public benefit: an overview. Retrieved from https://www.gov.uk/government/publications/public-benefit-an-overview/public-benefit-an-overview

Cheung, S. (2020). Disambiguating the benefits and risks from public health data in the digital economy. Big Data & Society, 7(1). doi:10.1177/2053951720933924

Daly, A. (2016). Private Power, Online Information Flows and EU Law: Mind the Gap. Oxford: Hart Publishing.

Daly, A., Devitt, S.K., & Mann, M. (Eds.) (2019). Good Data. Amsterdam: Institute of Network Cultures.

Democratic Society (2023). Unlocking the Value of Data - Overview of Engagement, Review of Principles and Next Steps for Practical Use. (Scottish Government commissioned report).

Dencik, L., Hintz, A., Redden, J., & Trere, E. (2022). Data Justice. Thousand Oaks, CA: SAGE.

Digital Ethics Expert Group. (2022). Building Trust in the Digital Era: Achieving Scotland's Aspirations as an Ethical Digital Nation. Retrieved from https://eprints.gla.ac.uk/284484/1/284484.pdf

Durante, M. (2021). Computational Power: The Impact of ICT on Law, Society and Knowledge. Abingdon: Routledge.

Dyer, C. (2021). Government faces legal action over £23m deal involving patient data. BMJ, 372. doi:10.1136/bmj.n587

Earl, S., Currie, M., Vidmar, M., & Gorton, V. (2021). Public Sector Personal Data Sharing. (Scottish Government commissioned literature review.)

Enough! Collective. (2022). Less: A Journal of Degrowth in Scotland. Issue 4, Summer 2022. Retrieved from https://www.enough.scot/wp-content/uploads/2022/12/LESS4.pdf

Equality and Human Rights Commission (2016). Assessing impact and the Public Sector Equality Duty: A guide for public authorities in Scotland. Retrieved from https://www.equalityhumanrights.com/sites/default/files/assessing-impact-public-sectory-equality-duty-scotland.pdf

Erikainen, S. & Cunningham-Burley, S. (2021). Unlocking the Value of Scotland's Data: Public Engagement Around the Access to Public Sector Data With or By Private Sector Organisations. (Scottish Government commissioned literature review.)

Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor. New York: St Martin's Press.

Goldacre, B., & MacKenna, B. (2020). The NHS deserves better use of hospital medicines data. BMJ, 370. doi:10.1136/bmj.m2607

Hartman, T., Kennedy, H., Steedman, R., & Jones, R. (2020). Public perceptions of good data management: Findings from a UK-based survey. Big Data & Society, 7(1). doi:10.1177/2053951720935616

Harvey K, & Laurie G. (2021). Concept Note: Public Interest. Retrieved from https://www.law.ed.ac.uk/sites/default/files/2021-03/Public%20interest%20concept%20note.pdf

Hopkins Van Mil. (2021). Putting Good into Practice: A Public Dialogue on Making Public Benefit Assessments When Using Health and Care Data. (National Data Guardian research report). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977737/PGiP_Report_FINAL_1304.pdf

Iliadis, A., & Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. The Information Society, 38(5), 334-363. doi:10.1080/01972243.2022.2100851

Ipsos MORI. (2017). The One-Way Mirror: Public attitudes to commercial access to health data. (Report prepared for the Wellcome Trust). Retrieved from https://wellcome.figshare.com/articles/journal_contribution/The_One-Way_Mirror_Public_attitudes_to_commercial_access_to_health_data/5616448/1

Jefferson, E., et al. (2022). GRAIMATTER Green Paper: Recommendations for disclosure control of trained Machine Learning (ML) models from Trusted Research Environments (TREs). doi:10.5281/zenodo.7089491

Jones, K., Laurie, G., Stevens, L., Dobbs, C., Ford, D. & Lea, N. (2017). The other side of the coin: harm due to the non-use of health-related data. International Journal of Population Data Science 1(1.035) Proceedings of the IPDLN Conference (August 2016). doi:10.23889/ijpds.v1i1.52

Kallis, G., Kostakis, V., Lange, S., Muraca, B., Paulson, S., & Schmelzer, M. (2018). Research on degrowth. Annual review of environment and resources, 43, 291-316. doi:10.1146/annurev-environ-102017-025941

Keenan, B. (2022), The Evolution Of Elucidation: The Snowden Cases Before The Investigatory Powers Tribunal. The Modern Law Review, 85: 906-937. doi:10.1111/1468-2230.12713

Klinge, T. J., Hendrikse, R., Fernandez, R., & Adriaans, I. (2023). Augmenting digital monopolies: A corporate financialization perspective on the rise of Big Tech. Competition & Change, 27(2), 332–353. doi:10.1177/10245294221105573

Kukutai, T., & Taylor, J. (Eds). (2016). Indigenous Data Sovereignty: Towards an Agenda. Canberra: ANU Press.

Kuntsman, A., & Miyake, E. (2022). Paradoxes of Digital Disengagement: In Search of the Opt-Out Button. London: University of Westminster Press.

Life Sciences in Scotland Industry Leadership Group Digital & Data Subgroup. (2021). Opportunities and Priorities. Retrieved from https://www.evaluationsonline.org.uk/evaluations/Documents.do?action=download&id=1013&ui=basic

Lucas, J. C., Schroeder, D., Arnason, G., Andanda, P., Kimani, J., Fournier, V., & Krishnamurthy, M. (2013). Donating human samples: who benefits? Cases from Iceland, Kenya and Indonesia. In D. Schroeder & J. Cook Lewis (Eds.), Benefit sharing: From Biodiversity to Human Genetics (pp. 95-127) Dordrecht: Springer.

Murgia, M., & Harlow, M. (2021, July 27). NHS Shares English Hospital Data with Dozens of Companies. Financial Times. Retrieved from https://www.ft.com/content/6f9f6f1f-e2d1-4646-b5ec-7d704e45149e

Nanda, A. & Narayan, V. (2022). Data stewardship for responsible sharing of public data – an analysis of stewardship models for better urban governance. doi:10.5281/zenodo.7396011

National Data Guardian. (2022). What do we mean by public benefit? Evaluating public benefit when health and adult social care data is used for purposes beyond individual care. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1124013/NDG_public_benefit_guidance_v1.0_-_14.12.22.pdf

O'Keefe, K. & O'Brien, D. (2018). Ethical Data and Information Management: Concepts, Tools and Methods. London: Kogan Page.

O'Neil, C. (2017) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. UK, USA, Canada: Penguin Books.

Papageorgiou, V., Wharton-Smith, A., Campos-Matos, I., et al. (2020). Patient data-sharing for immigration enforcement: a qualitative study of healthcare providers in England. BMJ Open, 10 (e033202). doi:10.1136/bmjopen-2019-033202

Pasquale, F. (2013). Grand Bargains for Big Data: The Emerging Law of Health Information. Maryland Law Review, 72, 682 . Retrieved from http://digitalcommons.law.umaryland.edu/mlr/vol72/iss3/2

Powles, J., & Hodson, H. (2017) Google DeepMind and healthcare in an age of algorithms. Health and Technology, 7, 351–367. doi:10.1007/s12553-017-0179-1

Salisbury, H. (2023). Doubts about a database. BMJ, 380. doi:10.1136/bmj.p292

Scassa, T., & Vilain, M. (2019). Governing Smart Data in the Public Interest: Lessons from Ontario's Smart Metering Entity. CIGI Papers No. 221. Retrieved from https://www.cigionline.org/static/documents/documents/Paper%20no.221_1.pdf

Scassa, T. (2020). Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto. Technology and Regulation 44-56. Retrieved from https://techreg.org/article/download/10994/11968

Scottish Government & COSLA. (2023). Greater access, better insight, improved outcomes: a strategy for data-driven care in the digital age. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2023/02/data-strategy-health-social-care-2/documents/greater-access-better-insight-improved-outcomes-strategy-data-driven-care-digital-age/greater-access-better-insight-improved-outcomes-strategy-data-driven-care-digital-age/govscot%3Adocument/greater-access-better-insight-improved-outcomes-strategy-data-driven-care-digital-age.pdf

Scottish Government. (2021). Scotland's AI Strategy: Trustworthy, Ethical and Inclusive. Retrieved from https://static1.squarespace.com/static/62cd519a0b49ae6dcee5dc8c/t/62d80552ad77dc084206e679/1658324316824/Scotlands_AI_Strategy_Web_updated_single_page_aps.pdf

Scottish Government. (2021). A Changing Nation: How Scotland will Thrive in a Digital World. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2021/03/a-changing-nation-how-scotland-will-thrive-in-a-digital-world/documents/a-changing-nation-pdf-version/a-changing-nation-pdf-version/govscot%3Adocument/DigiStrategy.FINAL.APR21.pdf

Scottish Government. (2021). An Ethics Framework for the Data and Intelligence Network. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/factsheet/2021/09/ethics-framework-data-intelligence-network/documents/ethics-framework-data-intelligence-network/ethics-framework-data-intelligence-network/govscot%3Adocument/ethics-framework-data-intelligence-network.pdf

Scottish Government. (2021). Review of the Information Governance Landscape across Health and Social Care in Scotland. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-analysis/2022/04/information-governance-review-executive-summary/documents/information-governance-review-executive-summary-review-information-governance-landscape-health-social-care-scotland/information-governance-review-executive-summary-review-information-governance-landscape-health-social-care-scotland/govscot%3Adocument/information-governance-review-executive-summary-review-information-governance-landscape-health-social-care-scotland.pdf

Scottish Science Advisory Council. (2022). Building on the Science Legacy of COVID-19 in Scotland. Retrieved from https://scottishscience.org.uk/sites/default/files/article-attachments/SSAC%20Report%20-%20Building%20on%20the%20Science%20Legacy%20of%20Covid-19%20in%20Scotland.pdf

Sorbie, A. (2022). Operationalising 'publicness' in data-intensive health research regulation: an examination of the public interest as a regulatory device. Edinburgh Research Archive, University of Edinburgh.

Sorbie, A. (2021). The Public Interest. In G. Laurie, E. Dove, A. Ganguli-Mitra, C. McMillan, E. Postan, N. Sethi, et al. (Eds.), The Cambridge Handbook of Health Research Regulation (Cambridge Law Handbooks, pp. 65-72). Cambridge: Cambridge University Press. doi:10.1017/9781108620024.009

Sorbie, A. (2020). Sharing confidential health data for research purposes in the UK: where are 'publics' in the public interest?. Evidence & Policy, 16(2), 249-265. doi:10.1332/174426419X15578209726839

Srnicek, N. (2017). Platform capitalism. Cambridge, UK ; Malden, MA: Polity Press.

Standing Committee on Pandemic Preparedness (2022). Appendix to the Interim Report. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2022/08/standing-committee-pandemic-preparedness-appendix-interim-report/documents/standing-committee-pandemic-preparedness-appendix-interim-report/standing-committee-pandemic-preparedness-appendix-interim-report/govscot%3Adocument/standing-committee-pandemic-preparedness-appendix-interim-report.pdf

Stevens, L., & Laurie, G. (2017). From a culture of caution to a culture of confidence: facilitating the good governance of administrative data in the UK. International Journal of Population Data Science, 1 (1:358) Proceedings of the IPDLN Conference (August 2016). doi:10.23889/ijpds.v1i1.380ezEmmanuel etouzé

Tetley-Brown, L., & Klein, E. (2021). Exploring data-in-use: the value of data for Local Government/Data-in-Use: Der Wert von Daten für die Kommunalverwaltung. dms–der moderne staat–Zeitschrift für Public Policy, Recht und Management, 14(1), 11-12. doi:10.3224/dms.v14i1.07

Van Dijck, J., Poell, T., & de Waal, M. (2018). The platform society: Public Values in a Connective World. New York: Oxford University Press.

Waterman, L. Z., Pillay, M., & Katona, C. (2021). Sharing health data for immigration control affects marginalised communities. BMJ, 373. doi:10.1136/bmj.n1042

Watt, I. (2022). What is open data and why does it matter? The David Hume Institute in partnership with Open Data Scotland. Retrieved from https://static1.squarespace.com/static/59b82ed532601e01a494df34/t/621f59b041e2b77397a61b42/1646221746023/20200126_What+is+open+data+and+why+does+it+matter%3F.pdf

Scottish Government
Riaghaltas na h-Alba

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80525-776-9 (web only)

Published by The Scottish Government, May 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1238762 (08/23)

www.gov.scot