Northern Ireland Assembly

Research and Information Service
Research Paper

8 May 2025

Glenn Williams and James Coburn

Data sharing and linkage in the Northern Ireland Executive

NIAR 078-2025

This Paper considers the current legal basis for data sharing and linkage between Executive departments in Northern Ireland for both service delivery and research. It also considers barriers to sharing data and practice in the rest of the United Kingdom and the Republic of Ireland.

Paper 50/25 08 May 2025

Research and Information Service briefings are compiled for the benefit of MLAs and their support staff. Authors are available to discuss the contents of these papers with Members and their staff but cannot advise members of the general public. We do, however, welcome written evidence that relates to our papers and this should be sent to the Research and Information Service, Northern Ireland Assembly, Room 139, Parliament Buildings, Belfast BT4 3XX or e-mailed to Raisecsu@niassembly.gov.uk

Key Points

- Data sharing between government departments can improve the quality and efficiency of public services, aid research in better informing public policy, and help drive research and development innovations.
- Data sharing in Northern Ireland is legislated through the UK General Data Protection Regulation and Data Protection Act 2018, and the Digital Economy Act 2017. These aim to both provide organisations with a framework to help them share data lawfully and protect the people whose data is being shared.
- This legislation is viewed as being sufficient for government departments to share data with each other, however there exists cultural and operational barriers.
- Culturally, the disconnect between the party sharing the data (who shoulder the risks and effort of administering the data) and the party receiving the data (who are perceived as reaping the benefits) can lead to hesitancy around data sharing and contribute to a sense of disconnect between departments. The perceived lack of a clear data sharing mandate exacerbates these issues.
- Operationally, siloed departmental working creates a fragmented data landscape which in turn creates barriers to sharing, including a lack data standardisation, poor awareness of what data is available, quality inconsistency, and inefficient interoperability.
- Public trust is also important when considering sharing data, specifically trust in the organisation itself. The UK Government is viewed low on the trust spectrum compared to other organisations.
- Moving forward, further legislative efforts in Northern Ireland may not be the strongest solution to encourage better data sharing between departments. Instead, addressing the cultural and operational barriers may lead to improved data sharing.

Contents

1 Introduction

This paper considers the legal basis for data sharing and linkages between Executive departments in Northern Ireland. Beginning with a brief overview of what data sharing and data linkage is and the benefits it can bring, it then describes the legislative basis for data sharing and linkage in Northern Ireland, Great Britain and the Republic of Ireland. An overview of the current data sharing initiatives in the UK is given, followed by a consideration of the barriers to increasing data sharing and linkage. The paper concludes with a summary of the changes that may be required to improve data sharing and linkage in Northern Ireland.

2 Data sharing

2.1 What is data sharing?

Data sharing traditionally means making data accessible to other users, whether they are within the same organisation or external third parties. It covers a wide range of situations, from ‘open data’ which is available publicly for use by anyone (e.g. census data hosted online by NISRA) through to personal data which can only be shared if certain conditions are met (e.g. a patient’s medical records held by their GP).

2.2 What is data linkage?

Data linkage involves combining multiple data sources that refer to the same individual or entity to create richer data that can provide better insight.[1] For example, in England the Department for Education and Ministry of Justice link education data with criminal records to research the relationships between educational and criminal justice outcomes and the drivers of offending, which can assist in identifying those who require early intervention.[2]

[1] UK Parliament, *POSTnote 664 Sharing Public Sector Data* (2022)

[2] Office for National Statistics, *Joined up data in government: the future of data linking methods* (2021)

Although data sharing and data linkage are distinct concepts, they are frequently intertwined. Data is often shared with the intention of linking it to other data sources, and similarly, linking data sources typically requires sharing access to them.[3] For the purposes of being succinct this paper will refer to 'data sharing' to encompass both concepts.

Data sharing is then, understandably, a dense topic. While this paper primarily focuses on data sharing between government departments for the purposes of service delivery and research, it will also touch on data sharing in a wider sense insofar as it is applicable, for example when considering public perceptions of data sharing in general.

2.3 Benefits of data sharing between government departments

Data sharing between government departments can improve the quality and efficiency of public services, aid research in better informing public policy, and help drive research and development innovations.[4] For example, in 2015 the Driver and Vehicle Licensing Agency (DVLA) shared driving license data with Home Office to identify individuals who no longer had the right to remain in the UK but still held a Great British driving license, and as a result nearly 10,000 licenses were revoked.[5]

Commentators have also identified hypothetical examples where sharing data between organisations could:

- Better predict the likelihood of 'at risk' children ending up in prison.
- Significantly improve employment outcomes for people with a serious health condition.
- Facilitate the transition of buying or selling residential and commercial property, from a paper-based system to a digital system.

[3] Office for Statistics Regulation, *Data Sharing and Linkage for the Public Good* (2023)

[4] As cited in footnote 1

[5] Driver & Vehicle Licensing Agency, *DVLA Data Sharing Strategy* (2017)

- Make better use of Council Tax information in partnership with and supporting local authority intervention programmes for positive citizen outcomes.
- Create a simpler and more effective way for businesses to interact with administration processes, (allowing them to provide their data once rather than multiple times).[6]

Outside of these benefits gained from the specific purposes for sharing data within government departments, there are also wider secondary benefits. Collaboration between departments can be strengthened to ensure consistency in the approach to shared challenges, data workflows can be streamlined to increase efficiency, frameworks for sharing data can be shaped and improved, and trust can be built by focusing on privacy and addressing security concerns.[7] Essentially, the benefits gained from sharing data between government departments can, if done effectively, lead to operational improvements that encourages further data sharing.

3 Legislative basis for data sharing

3.1 Northern Ireland

Within Northern Ireland the sharing of data is covered by certain data protection laws which aim to both provide organisations with a framework to help them share data lawfully, and protect the people whose data is being shared.[8] This legislative framework consists of the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA), and the Digital Economy Act 2017 (DEA). The GDPR and DPA provide overarching regulations for data protection across all sectors, while the DEA contains provisions specifically focussing on data sharing within public authorities.

[6] Office for National Statistics and the Infrastructure and Projects Authority, *Data-sharing: The beating heart of a successful public sector* (2025)

[7] M Soncul, UK Government blog, *Unlocking data sharing across government* (2025)

[8] Information Commissioner's Office, *Data sharing myths busted* (2023)

3.1.1 Global Data Protection Regulation and Data Protection Act 2018

The GDPR and DPA came into effect in Northern Ireland on 25 May 2018 and together formed a new framework for regulating and processing of personal data, replacing the former Data Protection Act 1998. The GDPR and DPA complement each other, with the DPA in essence providing the framework for implementing GDPR. While the origins of the GDPR are in EU regulations, it is UK law and is applicable after Brexit.

Article 5 of the GDPR sets out seven key principles that form its general data protection. These principles to 'data processing' which includes organising, restructuring, and sharing the data.[9] Failure to comply with these principles can result in substantial fines and reputational damage to organisations. The seven key principles are:

- Lawfulness, fairness and transparency – data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Purpose limitation – data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data minimisation – data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy – data shall be accurate and, where necessary, kept up to date.
- Storage limitation – data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Integrity and confidentiality – data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

[9] Information Commissioner's Office, *Key data protection terms you need to know* (2023)

- Accountability – being responsible for, and being able to demonstrate compliance with, the principles.

Both the ‘principle limitation’ and ‘storage limitation' principles make allowance for further processing and longer periods of storage insofar as the personal information is processed for archiving purposes[10] in the public interest, scientific or historical research purposes or statistical purposes.

The GDPR applies to processing carried out by organisations operating within the UK, and to organisations outside the UK that offer goods or services to individuals in the UK.[11]

The DPA was to be amended by the Data Protection and Digital Information Bill, however this did not complete before Parliament was dissolved in May 2024 and the bill is no longer being progressed.[12]

3.1.2 Digital Economy Act 2017

The DEA provides a framework for sharing personal data for defined purposes across specific parts of the public sector. Its aim is to improve public services through the better use of data while ensuring privacy, clarity and, consistency in how the public sector shares personal data.[13] The DEA does not cover data sharing relating to the provision of health and social care.

Part 5 of the Digital Economy Act (DEA) addresses digital government by establishing gateways for specified public authorities to share data. These gateways facilitate the exchange of both personal and non-identifying data. Section 35 specifically refers to the disclosure of information to improve public security, and allows certain public authorities (or service providers) to share

[10] Recital 158 of the EU GDPR provides a definition for processing for archiving purposes, stating should be carried out by bodies that under law have “a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest”

[11] Information Commissioner’s Office, *Who does the UK GDPR apply to?* (2023)

[12] Information Commissioner’s Office, *The Data (Use and Access) (DUA) Bill* (2024)

[13] Information Commissioner’s Office, *Data sharing across the public sector: the Digital Economy Act codes* (2023)

information with each other to achieve specified objectives which must focus on enhancing public services, providing benefits, or improving well-being.

The powers to share data are supplemented by codes of practice (the DEA codes) which must be consistent with the Information Commissioner's data sharing code of practice, which contains the following principles:[14]

1. In deciding whether to include persons in information sharing activity, consider if the sharing is necessary and proportionate to achieve the desired objective.
2. Privacy impact assessments (or data protection impact assessments) are carried out before any data sharing takes place and reviewed at critical milestones throughout the lifecycle. They should be made available to citizens in line with ICO guidance.
3. Information about information sharing agreements[15] under the public service delivery, debt and fraud powers is made available to citizens in a searchable electronic list, unless there are particular national security issues or other sensitivities which would outweigh the public interest in doing so.
4. Steps should be taken to minimise the amount of data shared and ensure this is the minimum required for the purpose of achieving the specified objective, using methods which avoid unnecessarily sharing or copying of large amounts of personal information.
5. Data is always held securely to the appropriate security standards.
6. Data held is maintained to the appropriate quality and where appropriate citizens can view, correct and delete data held about them.
7. Data held can only be used for specified purposes.

[14] Digital Economy Act 2017 part 5: Codes of practice, Guidance, *Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017* (2020)

[15] Information sharing agreements are a common set of rules binding on the organisations involved in the information share. The agreement should identify all the organisations that will be involved in the information share.

8. The ethical issues around the use of data are factored into the decision-making process and any new data analysis techniques are assessed against the Data Ethics Framework.[16]
9. Relevant codes of practice (e.g. Technology Code of Practice[17] and Code of Practice for Official Statistics[18]) are adhered to when accessing and analysing data.
10. Data is only kept as long as necessary and is then securely deleted.

Principle 2 makes reference to a data protection impact assessment (DPIA). This is an assessment carried out to help identify and minimise the data protection risks of a project. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. In assessing the level of risk, both the likelihood and the severity of any impact on individuals must be considered, i.e. high risk could result from either a high probability of some harm, or a lower possibility of serious harm. It is also considered good practice to do a DPIA for any major project that requires the processing of personal data.[19]

While the DEA predates both the GDPR and DPA, it was drafted to be consistent with the GDPR provisions as these were already known and specifically states that any processing or disclosure of data must comply with data protection legislation.[20]

3.1.3 Data (Use and Access) Bill 2025

This bill is not currently law and is at the report stage in the House of Commons.[21] One of the core objectives of the bill is improving public services,

[16] Government Digital Service, Data Ethics Framework (2020)

[17] Government Digital Service and Central Digital and Data Office, *The Technology Code of Practice* (2025)

[18] Office for Statistics Regulation and UK Statistics Authority, *Code of Practice for Statistics* (2022)

[19] Information Commissioner’s Office, *Data protection impact assessments* (2024)

[20] Information Commissioner’s Office, *Data sharing across the public sector: the Digital Economy Act codes* (2023)

[21] UK Parliament, Parliamentary Bills, *Data (Use and Access) Bill [HL]* (2025)

which it aims to do through using data to drive efficiencies within the NHS and law enforcement.

Within the NHS, this legislation will make information standards mandatory for all suppliers of IT services to the health and care system, ensuring health and care data is recorded and managed in the same way. This will improve the flow of data through the health and care system, providing quicker access to patient data and saving an estimated 140,000 hours of NHS staff's time in one year alone.[22]

Within law enforcement, the bill will remove the current legal requirement for a police officer to record the reason they are accessing or disclosing someone's personal data, freeing up an estimated 1.5 million hours a year of police time.

While neither of these outcomes relate directly to the sharing of data across government departments, they do indicate the importance of both standardising data to improve sharing and the need to make the process of retrieving data more efficient.

The Bill includes provisions that fall under the legislative competence of the NI Assembly, and as such agreement has been sought by the Secretary of State for Science, Innovation and Technology to initiate the legislative consent process and to support a legislative consent Motion.[23]

3.2 England, Scotland and Wales

Data protection as a subject is a reserved matter under paragraph 40 of schedule 3 to the Northern Ireland Act 1998, and as such both the GDPR and DPA[24] apply equally to Northern Ireland and Great Britain (subject to minor exceptions regarding recordable offences).[25]

[22] Department for Science, Innovation & Technology, *Data (Use and Access) Bill factsheet: improving public services* (2024)

[23] House of Lords Debate 5 February 2025 *Vol.843 c.697*

[24] *Data Protection Act 2018*, Explanatory Notes, Territorial extent and application

[25] *Northern Ireland Act 1998*, sch.3, para. 40

Similarly, section 35 of part 5 of the DEA is applicable across the UK, and as such the legislation described above is also valid for England, Scotland and Wales.[26]

3.3 Republic of Ireland

Data sharing policy in the Republic of Ireland (RoI) is directed by a national strategy for data linkage in the public sector and must work within the framework provided by both domestic and European Union (EU) legislation.

3.3.1 EU and European Free Trade Association (EFTA) obligations

As an EU member state, the Republic of Ireland is subject to EU directives and law. The responsibilities placed on governments, and the rights created for Irish citizens act as a framework for data-sharing policy.

The EU2017.EE Talinn Declaration on eGovernment commits the RoI (and all EU, EFTA states) to linking their public eServices, and to the once-only principle, where data should only be collected once, and retained for future use.[27] The EU GDPR is equivalent to the UK GDPR, though with a broader remit covering organisations processing personal data of individuals located within the EU, regardless of where the organisation is based. The Data Governance Act 2022 requires EU members states to establish domestic oversight of data sharing and usage, reuse public sector data that cannot be shared publicly, and facilitate data sharing in medical, agricultural, environmental and transport sectors.[28]

To meet these obligations, the Irish Government published the Public Service Data Strategy 2019-2023.[29] This strategy was designed to optimise data management within the Irish Government, setting out the path to an integrated

[26] *Digital Economy Act 2017*, pt. 5, sec. 5

[27] *Tallinn Declaration on eGovernment* (2017)

[28] Department of Public Expenditure and Reform, *Public Service Data Strategy 2019-2023*

[29] As cited immediately above

approach to the improved use of data, particularly across Public Service Bodies (PSBs). This vision would be achieved through several key themes:

- Interoperability Platform: development of a digital interface where PSBs can cooperate, securely sharing and reusing data through the use of Application Programming Interfaces (APIs[30]).
- Legislation: legislation to be introduced to create a framework for personal data sharing, between citizens, businesses and the Irish Government – codified as the Data Sharing and Governance Act 2019.
- Governance: oversight and governance policies are to be put in place to ensure data is managed, and public trust maintained.
- Privacy: personal data will be protected via various security, and data protection methods, whether privacy-by-design, or privacy-by-default.
- Analytics: data analysis should follow a ‘structured approach’, aiding evidence-based policy.
- Base Registries: central repositories of data will be established, reducing the need for individuals, and organisations to provide the same data to government, over and over.
- Trusted Identifiers: official data identifiers, such as the Individual Health Identifier, or Personal Public Service Number, will be used to allow data to be linked across different data holders.
- Transparency: Government will establish a Data Portal to allow them to identify personal data held by the government, and via ‘citizen-accessible’ agreements on data sharing.
- Discovery: identify data and services that can be reused, promote awareness of this strategy and available resources.

3.3.2 Data Sharing and Governance Act 2019

Data sharing in the Republic of Ireland is now underpinned by the Data Sharing and Governance Act 2019 (DSGA), which provides the statutory basis for

[30] An API is a set of tools that allows different software applications to communicate with each other. It can be thought of like a bridge that allows two different programs to share data with each other.

personal data to be shared between public bodies.[31] The Act builds on the General Data Protection Regulation 2018 (GDPR), and Data Protection Act 2018.[32]

Under the Act, if public bodies seek to share data, this is only possible if it has been permitted, or ordered, directly by legal provision. If no such provision exists, the two bodies looking to share data must put a Data Sharing Agreement in place. These agreements must undergo public consultation, and be reviewed and endorsed by the Data Governance Board.

The Data Governance Board has, as of 15 April 2025, approved twenty Data Sharing Agreements, on a diverse range of issues.[33] Examples include: [34]

- Agreement permitting next of kin data to be shared between the Department of Foreign Affairs and Department of Social Protection, so the former department can easily notify next of kin and provide consular services if an Irish citizen dies abroad.
- Agreement permitting personal data-sharing between Department of Social Protection, and the Health Information and Quality Authority, identifying valid participants for the National End of Life Survey.
- Agreement between the Department of Foreign Affairs, and Department of Social Protection, to share, and verify details on applicants for the Foreign Birth Register, which the former department maintains.

Each agreement includes a series of rules and communication responsibilities that the bodies looking to share data must comply with. The duration that data will be required, and maintained, is typically included in the text of the

[31] *Data Sharing and Governance Act 2019*

[32] Office of the Government Chief Information Officer, *Data Governance* (2025)

[33] Department of Public Expenditure, NDP Delivery and Reform, *Data Governance Board – Data Sharing Agreement Register* (2025)

[34] Mason, Hayes & Curran, *Data Sharing Agreements and the Data Sharing Agreement Register* (2023)

agreement, with the understanding that shared data will be destroyed by the receiving department in the aftermath – in line with GDPR's Article 5.[35]

3.3.3 The Competition and Consumer Protection Commission

The Competition and Consumer Protection Commission (CCPC) is the statutory body, established in 2014, responsible for oversight and enforcement of competition and consumer protection law in the Republic of Ireland.

In 2024, the CCPC was appointed as the Republic of Ireland's regulator, to oversee the nation's compliance with the EU Data Governance Act (DGA).[36] Under the DGA, each EU nation is required to designate a competent authority responsible for registering and overseeing "data altruism" organisations. These organizations facilitate data sharing for purposes such as healthcare research, climate change studies, and the enhancement of public services.[37]

In this role CCPC monitors compliance with EU data protection law, with the power to initiate investigations and sanction bad actors. The DGA is a component of the European Commission's "European Strategy for Data", designed to foster more effective data sharing between companies and EU Member States, with a view to bolster research and innovation.[38]

4 Current data sharing initiatives in the UK

Within the UK there exists a number of initiatives that focus on better facilitating data sharing between government departments. These range from higher level strategies (e.g. the Open Data Strategy for Northern Ireland and Data Sharing Governance Framework) through to specific project-driven programs (e.g. Administrative Data Research Northern Ireland and Better Outcomes through Lined Data), all of which recognise the value data sharing can bring to the

[35] Data Protection Commission, *Data Sharing in the Public Sector* (2019)

[36] Competition and Consumer Protection Commission, *CCPC given responsibility for enforcement of EU Data Governance Act* (2024)

[37] Pinsent Masons *Ireland's CCPC confirmed in EU Data Governance Act role* (2025)

[38] As cited in footnote 34

public sector, and in their own way each attempts to better facilitate the matter. This section outlines some of these initiatives.

4.1 Administrative Data Research Northern Ireland (ADR NI)

ADR NI is a partnership between the Administrative Data Research Centre Northern Ireland (which is itself a partnership between Queen's University Belfast and Ulster University) and the Northern Ireland Statistics and Research Agency (NISRA), supported by the Health and Social Care Research and Development (HSC R&D) Unit. [39] Established in 2018, ADR NI is one of four national partnerships, alongside ADR Scotland, ADR England, and ADR Wales, that together comprise ADR UK.

ADR NI aims to give decision makers the answers they need to solve important policy questions by linking together data held by different parts of government and facilitating safe and secure access for accredited researchers to these newly joined-up and de-identified datasets. Research projects must be approved by UK Statistics Authority Research Accreditation Panel and may take up to one year to create, or more than one year if the data is requested is new or has not been linked before.[40]

Current active projects include socio-demographic analyses of drug-related deaths in NI (linking the NI Mortality Study with census data)[41], understanding the predictors and consequences of homelessness in NI (linking NI Housing Executive data with health and social care data)[42], and examining mental health in prisons in NI (linking healthcare, prescriptions, hospital admissions, income deprivation and mortality data).[43]

[39] Queen's University Belfast, *Administrative Data Research Centre Northern Ireland* (2022)

[40] Northern Ireland Statistics and Research Agency, *Administrative Data Research Northern Ireland (ADR NI)* (2020)

[41] Administrative Data Research Northern Ireland, Drug-related deaths in Northern Ireland: Socio-demographic analyses (2020)

[42] Administrative Data Research Northern Ireland, Understanding the predictors and consequences of homelessness in Northern Ireland (2024)

[43] Administrative Data Research Northern Ireland, Mental health in prisons in Northern Ireland (2025)

4.2 Open Data Strategy for Northern Ireland 2020-2023

Published by the NI Department of Finance, The Open Data Strategy for Northern Ireland 2020-2023 is a blueprint for driving a transparency agenda across government and creating a resource which will improve the economy and lives of people in Northern Ireland. Its four main themes are:

1. Increasing the rate of publication and sharing of government information as Open Data.
2. Promoting the innovative use of Open Data as a means for advocating its benefits.
3. Engaging with the NI public sector to promote Open Data and its potential through a series of events, including the establishment of an innovation fund, and running Open Data competitions.
4. Placing strong emphasis on the need for training in Open Data leading to a more skilled and aware workforce who will, in turn, embed and sustain Open Data as a business function, rather than as an ad hoc activity carried out by specialists.

Several principles are laid out to help meet these themes, including that NI public sector data should be open by default, proactive data publication should be encouraged, and data should be accessible and easy to use.

The Strategy highlights an example of data sharing between Belfast City Council and the Land and Property Services to solve a problem of how to identify business premises being occupied and used where the appropriate business rates revenues were not being collected. Using machine learning techniques on a range of data sources, including open data sources such as the Food Standards Agency Rating ‘Scores on the Doors’ and Companies House, they were able to identify a total of £500,000 of uncollected rates.[44]

4.3 NISRA Corporate Plan 2025-29

[44] Department of Finance, *Open Data strategy for Northern Ireland - 2020-2023*

NISRA's Corporate Plan 2025-29, Statistics, Analysis, Research and Registration Services to Drive Decision Making for the Public Good, builds on its central purpose to provide trusted and independent insights on life in Northern Ireland. It aims to achieve this through delivering trustworthy, high-quality statistics, analysis, research, and registration services which provide evidence to inform policy discussions and public debate in Northern Ireland.

The Plan states that NISRA will continue to develop their expertise in data sharing, and create new learning resources to promote and encourage data sharing. They also aim to enhance the interoperability of public sector data which will allow analysts, researchers and policy makers to draw on a wider array of data.[45]

4.4 Data Sharing Governance Framework

The Data Sharing Governance Framework was published in May 2022 and sets out the UK government's collective commitment for proactive, simpler and faster data sharing, with clear principles for building consistent and coordinated cross-government data sharing governance. It highlights that where government data is assessed as not personally identifying or otherwise sensitive or restricted, the default position should be to make it available for sharing. It recommends following five principles to make data sharing more efficient:

- Commit to leadership and accountability for data sharing.
- Make it easy to start data sharing.
- Maximise the value of the data you hold.
- Support responsible data sharing.
- Make your data findable, accessible, interoperable and reusable.

The Framework applies to UK government departments and agencies of UK government departments, however it recognises that as data management is a

[45] Northern Ireland Statistics and Research Agency, *NISRA Corporate Plan 2025-29*

devolved issue the Northern Ireland Executive, Scottish Government and Welsh Government have their own approaches to data sharing governance.[46]

4.5 Data Sharing Network of Experts (DSNE)

Established in September 2022, the DSNE is a cross-government virtual team who help solve problems with sharing data between departments and agencies. It aims to understand how government shares data, learn from best practice, identify common challenges and reduce duplication. By achieving these, the DSNE will support a privacy-positive culture and foster more efficient government data sharing, ultimately benefitting public services. The team have worked with a wide range of government bodies, including the Cabinet Office, HM Revenue and Customs, and Department for Transport – these examples may suggest the DSNE is for central government departments (and potentially not for devolved administrations) however this is not explicitly stated.[47]

4.6 Data Marketplace

The Data Marketplace is a project in development, started by the Central Digital and Data Office (CDDO).[48] The CDDO aimed to support and enable responsible data sharing across government, and the Data Marketplace would achieve this by providing a way for users to discover, access and share government data in a legal, ethical and trusted way, and also offer supporting guidance and tools to help data sharing across government. The Data Marketplace would not host or provide data directly, rather it would help users find datasets, assess their usefulness, and create data sharing agreements more efficiently through guided workflows. An alpha version of the Data Marketplace was assessed in March

[46] Government Digital Service and Central Digital & Data Office, *Data Sharing Governance Framework* (2022)

[47] As cited in footnote 7

[48] K Millard, UK Government blog, *Discovering data across government – Government Digital and Data* (2023)

2023[49] and reassessed September 2023, with the assessment team reporting that the service met standards and could proceed to a private beta phase.[50]

It was initially introduced as part of the Government's 2022-25 Roadmap for Digital and Data which was for central government departments and did not directly apply to devolved administrations though the CDDO was to work closely with these administrations to ensure close alignment with the roadmap and their plans.[51] The CDDO was merged with other departments in January 2025 to form the new Government Digital Service, and the Data Marketplace remains aligned with the current government's priorities to maximise the value of government-held data.[52]

4.7 Better Outcomes through Linked Data (BOLD)

BOLD is a government data-linking programme which aims to improve the connectedness of government data in England and Wales. Led by the Ministry of Justice, BOLD uses de-identified data from the Ministry of Justice, Department of Health and Social Care, the Ministry of Housing, Communities and local government, Public Heath Wales, Department for Education, police forces, and the Welsh Government, to provide better data and evidence to support policy and the design of more effective services to people with multiple complex needs. Specifically, BOLD currently has four pilot projects: reducing homelessness, supporting victims of crime, reducing substance abuse, and reducing reoffending.[53]

[49] Government Digital Service, *Data Marketplace alpha assessment* (2023)

[50] Government Digital Service, *Data Marketplace alpha reassessment report* (2024)

[51] Central Digital and Data Office, *Transforming for a digital future: 2022 to 2025 roadmap for digital and data* (2023)

[52] *DSA Steering Board Minutes, Wednesday, 8 January 2025*

[53] Ministry of Justice, *Ministry of Justice: Better Outcomes through Linked Data (BOLD)* (2022)

4.8 Integrated Data Service (IDS)

The IDS is a UK cross-government service that provides secure access to high-quality data, enabling faster and wider collaborative analysis to produce research projects that inform vital decision-making and improve public services. Some of its key aims include providing access to linked data, creating integrated data products that link national data assets, and encouraging greater collaboration across government and academia.

The IDS is designed for devolved administrations, alongside government analysts, and external accredited researchers. To view and analyse data in the IDS a user must become an accredited researcher under the DEA and be approved for access to a project. To become a full accredited researcher, individuals must have an undergraduate degree (or higher), including a significant proportion of maths or statistics, or must be able to demonstrate at least three years quantitative research experience.[54]

5 Barriers to data sharing between government departments

> "*Despite welcome pockets of innovation, there continues to be a failure to deliver on data sharing and linkage across government, alongside many persisting barriers to progress.*"
>
> Office for Statistics Regulation (2024), Data Sharing and Linkage for the Public Good: Follow-Up Report[55]

Barriers to data sharing across government departments can be categorised into three themes: cultural, operational, and public perception. This section will take each theme in turn, though it should be noted that they are not mutually exclusive and can impact on each other.

[54] Office for National Statistics, *Become an accredited researcher* (2022)

[55] As cited in footnote 3

5.1 Cultural barriers

A 2023 report by the Institute for Government focusing on government data sharing during the pandemic stated that while the existing data protection legislation was sufficiently flexible to allow the government to respond quickly to the crisis, the most significant challenges with data sharing were cultural and organisational.[56] The report highlighted how traditionally there can be a disconnect between the party sharing the data, who take on the legal risk and administrative burden of preparing the data, and the party who receive the data.

A 2025 report produced by the Office for National Statistics and Infrastructure and Projects Authority (IPA) concerning data sharing within the public sector found similar barriers, identifying how sharing data across government departments is seen as transactional and not collaborative, with not enough trust existing between the data sharers (who are concerned with how the data will be used and stored) and the data receivers (who are concerned about the data quality). As a result, the perceived risks (e.g. reputational damage or exposing potential department inefficiencies) associated with data sharing were seen to outweigh the benefits. The report also found that leadership guidance and a strong central mandate for data sharing could help address these barriers, but unfortunately these were perceived as currently lacking. [57]

A 2020 report produced for the Department for Digital, Culture, Media & Sport looking at motivations and barriers to data sharing across government also found that there was culture of risk aversion preventing effective data sharing. They cited that the public perceptions of data sharing, the punitive role of the ICO around fines, and differences of opinions amongst data sharing experts combined with a lack of emphasis on the benefits of data sharing to form key barriers. They also stated there was a lack of visible leadership which could help address these issues.[58]

[56] Institute for Government, *Data sharing during coronavirus: lessons for government* (2023)

[57] As cited in footnote 6

[58] Department for Digital, Culture, Media & Sport, *Motivations for and barriers to data sharing* (2020)

5.2 Operational barriers

The 2025 ONS and IPA report also identified several operational barriers to effective government sharing:[59]

- Funding: there is currently little to no tracking to assess the returns on investment in sharing data, and as a result there is a reluctance to put in the effort and investment.
- Dataset awareness: as each department gathers, stores, and analyses its own data there is an inconsistency of quality to the data, and a lack of wider knowledge about what datasets exist and how they can be accessed.
- Policy and legislation: a limited understanding of existing legislation means government workers think it is all about data protection and punishment for misuse. Requesting data can also be difficult as individual departments own their data, resulting in different departments requiring agreements with one another in order to share.
- Standardisation: each department operates with their own data practices using different technologies, frameworks, and standards, resulting in a fragmented data landscape making sharing data inefficient, ineffective or impossible.

Similar themes have been noted in other research. The Office for Statistics Regulation (ORS) stated in a 2023 report that:[60]

- There is variation within government over how much data holders and researchers understand the process to share data under different legal bases.
- When applying for data through a secure data platform, the process is often lengthy and can appear overly burdensome to researchers.

[59] As cited in footnote 52

[60] As cited in footnote 3

- For every data share there will be many teams involved, within the same organisation or from many different ones. Not getting these teams together at the very start can cause major delays to data sharing.
- When researchers have a question about a dataset or process, it can be a challenge to find the right person who can help.
- Funding structures across government tend to be set up so that each department controls its own spend, making successful funding highly dependent on the priorities and vision within each department. This siloed approach is hampering efforts of collaboration and means projects with external funders are often more successful.
- It can be a challenge for those linking data to get enough information about the data to provide a high-quality linked output with a measurable rate of error.
- Variation in data standards and definitions used across government is making linking harder.

5.3 Public perception

Public trust has been identified as integral to the long-term sustainability of data sharing[61], and more specifically trust in the organisations involved in the data sharing.[62]

The UK Government’s Public Attitudes to data and AI: Tracker survey (Wave 4) evidenced that there is is a prevailing belief that government departments exchange data about specific individuals. Nearly half (46%) assume data sharing occurs occasionally, while over a quarter (27%) believe this ‘always’ takes place. This sentiment is particularly strong in Northern Ireland, where 78% believe data is always or sometimes shared between government departments;

[61] Centre for Data Ethics and Innovation, *Addressing trust in public sector data use* (2020)

[62] Department for Science, Innovation & Technology, *Public attitudes to data and AI: Tracker survey (Wave 4) report* (2024)

a sentiment more pronounced than in England (73%), Wales (71%), and Scotland (68%).[63]

Concerning trust, the survey found that 38% of respondents trusted the Government to act in their best interest. While this showed an upward movement from the previous wave (31%), it was the lower end of the trust spectrum behind the NHS (85%), academic researchers (76%), pharmaceutical researchers (68%), banks and financial institutions (68%), regulators (67%), HR and recruitment services (53%), and utilities providers (53%). Only social media companies (33%) placed lower than the Government.

The Centre for Data Ethics and Innovation (CDEI) found similar emphasis as part of its independent report on public sector data sharing, highlighting that the sharing of personal data must be in a way that is trustworthy, aligned with society's values and people's expectations.[64] CDEI followed up this report with polling data to gauge public attitudes towards data sharing. Respondents were shown a series of statements and asked "*To what extent would the following steps make you feel more or less comfortable with the data you have provided to one part of government being shared with another part of government?*", with a response of 0 representing "*Much less comfortable*" and 10 representing "*Much more comfortable*".[65]

Table 1 shows that statements relating to the value of sharing data (i.e. creating either national or personal benefit) rank lowest in terms of providing comfort, whereas statements relating to control, transparency and accountability (i.e. option to opt-out, knowing who the information is being shared with, and punishments for those misusing data) are ranked highest, indicating that addressing the perceived risks associated with data sharing may improve comfort more than promoting the benefits.

[63] As cited immediately above

[64] As cited in footnote 55

[65] Centre for Data Ethics and Innovation, *Polling data: Data sharing between government departments* (2021)

Table 1 Mean comfort levels concerning data provided to one part of government being shared with another part of government

Statement	Mean
You have the option to opt-out of your local council sharing this information if you choose	7.29
You are informed of exactly who this information is shared with	7.22
There are heavy fines and possible prison sentences for anyone caught misusing this information	7.15
There are strict controls on who can access this information and how it is used	7.07
Only the minimum necessary information about you is shared with central government to provide the service	7.06
There is a guarantee that this information is anonymised (i.e. personal information that could identify you is removed) before being shared	6.93
There is an independent board of experts who approve requests for information to be shared	6.56
There is a clear and published explanation on a Government website of why this information is being shared	6.54
If it means I don’t have to provide the same information again	6.44
There is a national benefit for the UK as a whole in sharing this information e.g. reducing crime and preventing fraud	6.32
There is a direct personal benefit of sharing this information, e.g. it might be to access particular services, like speeding up the process to reapply for a passport, or better continuity of healthcare between GPs and other NHS branches	6.19

Source: Centre for Data Ethics and Innovation

Specifically focussing on data in NI, the Northern Ireland Life and Times (NILT) Survey 2020[66] revealed that 62% of respondents either definitely or probably trust government departments to keep information and data secure, a decrease of 11pp from when the question was last asked in 2015.[67] This figure is lower among younger generations, with roughly half (51%) of 18-34 year olds trusting government departments to keep information and data secure. By comparison, 90% of respondents either definitely or probably trust the NHS to keep information secure, an increase of 4pp from 2015.

Respondents to the NILT Survey were asked to rate their agreement to certain statements, with two relating specifically to data privacy as shown in Table 2.

Table 2 Responses to NILT Survey 2020 v 2015

	Agree	
Statement	**2020**	**2015**
I don't care who uses data about me	13%	20%
The right to privacy has to be respected over everything else	75%	83%

Source: Northern Ireland Life and Times Survey

6 Facilitating better data sharing between departments in Northern Ireland

The research presented in this paper indicates that the legislation concerning data sharing is generally considered to be sufficient to facilitate data sharing between government departments. The research also suggests there is a lack of awareness and understanding of this legislation, and considering any future legislative efforts would have to be made in accordance with the principles established by the DEA, GDPR and DPA, efforts to improve data sharing may

[66] ARK, *Northern Ireland Life and Times Survey, 2020*

[67] ARK. *Northern Ireland Life and Times Survey, 2015*

be better spent on education and training of the existing legislation rather than implementing new law.

The main barriers appear to be cultural and operational. From a cultural perspective, work needs to be done to better communicate the value of data beyond its original use. Risk needs to be better and more clearly understood by the actors involved so that it can be mitigated effectively, and departments can feel empowered to share. There also needs to be strong support and direction from leadership, who can address issues as and when they arise. Operationally, standardisation of data can help to make it more shareable. Interoperability is also important, having technologies in place (e.g. APIs) that can facilitate data moving between different platforms.

Promoting the use of open data would also aid better data sharing. Northern Ireland appears to have good initiatives and frameworks in place for this (i.e. ADR NI, the Open Data Strategy for Northern Ireland, and the NISRA Corporate Plan), though it may be the case that awareness and education of the tools that exist is required.