



Bill Digest

Data Sharing and Governance Bill 2018

No. 55 of 2018

Niall Watters,
Senior Parliamentary Researcher, Public Administration

Monday,
June 18, 2018

Abstract

The [*Data Sharing and Governance Bill 2018*](#) seeks to provide for the regulation of the sharing of information, including personal data, between public bodies. The Bill provides for the regulation of the management of information by public bodies and provides for the establishment of base registries. The Bill provides for the collection of public service information and the establishment of the Data Governance Board.



Contents

Abstract	1
Contents	2
Glossary	3
Summary	4
Introduction.....	14
Policy context and background	16
Sharing personal data in the public service	27
Pre-legislative Scrutiny (PLS)	35
Principal provisions.....	44
Costs and implications.....	56

Bill published 12 June 2018: Second Stage Debate 19 June 2018.

This Digest may be cited as:

Oireachtas Library & Research Service, 2018. *Bill Digest – Data Sharing and Governance Bill 2018*

Legal Disclaimer

No liability is accepted to any person arising out of any reliance on the contents of this paper. Nothing herein constitutes professional advice of any kind. This document contains a general summary of developments and is not complete or definitive. It has been prepared for distribution to Members to aid them in their parliamentary duties. Some papers, such as Bill Digests are prepared at very short notice. They are produced in the time available between the publication of a Bill and its scheduling for second stage debate. Authors are available to discuss the contents of these papers with Members and their staff but not with members of the general public.

© Houses of the Oireachtas 2018

Glossary

Data protection law	“data protection law” means— (a) the Data Protection Acts 1988 to 2018, (b) the General Data Protection Regulation, (c) all law of the State giving further effect to the General Data Protection Regulation, and (d) all law of the State giving effect or further effect to Directive 2016/680.
Data-sharing agreement	“data-sharing agreement” means an agreement between two or more public bodies which provides for the disclosure of information by one or more of the parties to the agreement to one or more of the other parties to the agreement
Data-sharing	“data-sharing” means the disclosure of information, including personal data, by a public body to another public body.
Base registry	“base registry” means a database which is designated as such in an order made under <i>section 37(1) of the Bill</i> ;
Public body	“Public body” shall be construed in accordance with <i>section 9 of the Bill</i> .
Personal data	‘Personal data’ means 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.
Special categories of personal data	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.

Summary

The [Data Sharing and Governance Bill 2018](#) proposes to provide a generalised legal basis for the sharing of data between public bodies while also setting out appropriate safeguards under which such sharing should take place.¹ The Bill's objectives include, among other things:²

- "Making public services more seamless by reducing the burden of providing the same information to different public bodies;
- Facilitating the effective administration, supervision and control of public services;
- Establishing entitlements to public services;
- Identifying and correcting erroneous information; and,
- Evaluating the effectiveness of public services."

Background

The Bill stems from a wider Government programme to use information communication technologies ('ICT') to develop a more integrated public service network, such as the eGovernment³ agenda and open government data.⁴ The focus of the Bill, sharing of data including personal data between public bodies, is relevant in the context of the new data protection legal framework introduced by the General Data Protection Regulation and recently enacted *Data Protection Act 2018*.

According to the Regulatory Impact Analysis (RIA) accompanying the Bill, data sharing presently occurs extensively across the public service under "a number of existing legal provisions".⁵ The RIA argues that the current level of public service delivery would "not be possible without this data sharing taking place".⁶

¹ Department of Public Expenditure and Reform, Explanatory Memorandum for the *Data Sharing and Governance Bill 2018*. Available here: <https://data.oireachtas.ie/ie/oireachtas/bill/2018/55/eng/memo/b5518s-memo.pdf>

² *ibid*.

³ The OECD defines eGovernment as "[t]he term 'e-government' focuses on the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government". OECD (2001), *E-government: Analysis Framework and Methodology* [online]. OECD Public Management Service, Public Management Committee. Available here: <https://stats.oecd.org/glossary/detail.asp?ID=4752>

⁴ The OECD explain open government data as "[t]he two main elements of OGD are normally defined as follows: Government data is any data and information produced or commissioned by public bodies; Open data are data that can be freely used, re-used and distributed by anyone, only subject to (at the most) the requirement that users attribute the data and that they make their work available to be shared as well." OECD Working Papers on Public Governance No. 22, Open Government Data, 2015, *"Towards empirical analysis of open data government initiatives"* [online]. Available at: https://www.espap.pt/Documents/espap_lab/2015_04_Open_Government_Data.pdf

⁵ Department of Public Expenditure and Reform, 2015. *Data Sharing and Governance Bill, Regulatory Impact Analysis*. Available [here](#).

⁶ *Ibid*

However, according to the Bill's RIA, increased efforts at optimising data sharing between public bodies would potentially lead to "a more seamless and efficient service delivery to citizens and businesses fully consistent with data protection requirements".⁷

In light of the above, the key policy problem informing the Bill, from the Government's perspective, is:⁸

"that [an] overly restrictive interpretation of current Data Protection Law on the part of some Public Bodies can lead them to...be reluctant to share data with other Public Bodies where it would otherwise be beneficial. Furthermore, where a cross-departmental requirement exists, there may not be sufficient incentive for any particular Department to meet it."

Pre-legislative Scrutiny

The Oireachtas Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach undertook Pre-legislative Scrutiny (PLS) of the General Scheme of the Data Sharing and Governance Bill in 2017. As part of its scrutiny of the General Scheme, the Committee met in public session on 18 May 2017 and 23 May 2017. In July 2017 the Joint Committee published its [report](#) on its pre-legislative scrutiny of the General Scheme. The report makes 30 recommendations. Based on the response received from the Department of Public Expenditure and Reform and the Library & Research Service's assessment of the Bill, of the Joint Committee's 30 recommendations made in its PLS report on the General Scheme of the Bill:

- 15 recommendations have had an impact on the drafting of the Bill;
- In the case of 13 recommendations, the Bill can be described as adopting an approach consistent with the key recommendations; and
- 2 recommendations have not had an impact on the drafting of the Bill.

Commentary

There has been limited direct commentary on the specifics of the current Bill. There was however significant input to the consultation process leading to the General Scheme of the Bill and also during the Pre-legislative Scrutiny hearings held by the Joint Committee on Finance, Public Expenditure and Reform and Taoiseach. Links to these sources are set out below:

- [Department of Public Expenditure and Reform website for data sharing](#)
- [18 May 2017 - Meeting of the Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach.](#)
- [23 May 2017 - Meeting of the Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach](#)

⁷ *ibid*

⁸ *Ibid*: 02.

Summary of the provisions in the *Data Sharing and Governance Bill 2018*

The Bill is comprised of 10 parts which together account for 72 sections. A summary of the Bill is set out in Table 1 below.

Table 1: Summary of the Bill's provisions

Section	Title	Effect
Part 1: Preliminary and General		
1.	Short title and commencement	Standard provision that defines the short title of the Bill and provides for commencement by Ministerial order. Commencement orders may be limited to particular provisions of the Bill or purposes.
2.	Definitions	Defines terms used in the Bill, including 'base registry' and 'data-sharing agreement'.
3.	Regulations and orders	Provides for the Minister to make regulations and orders for the purpose of the proposed Act. These must be laid before the Houses of the Oireachtas and are subject to annulment by a resolution of either House.
4.	Expenses	Provides that the Minister's expenses in the administration of the proposed Act are to be met from funds provided by the Oireachtas.
Part 2: Application of Act		
5.	Interaction with Data Protection Acts and GDPR	Provides for the relationship between the proposed Act and existing data protection law. Subsections (2) and (3) provide that section 38 of the <i>Data Protection Act 2018</i> and regulations made under it do not apply to disclosures of information by one public body to another. The effect is that such disclosures will not be deemed lawful simply because they are made in the performance of functions under legislation: they must meet the requirements of the proposed Act.
6.	Interaction with Social Welfare Consolidation Act 2005	Provides for sharing of individuals' "public service identity" (i.e. name, date of birth, PPSN and other identifying information) between specified bodies where the information is disclosed in accordance with the proposed Act. Specified bodies are defined in the <i>Social Welfare Consolidation Act 2005</i> . Sharing of public service identity information is not however permitted for the purpose of 'organisational studies of public bodies'.
7.	Interaction with other enactments	Provides (subject to limited exceptions) that the proposed Act will not affect other specified Acts relating to sharing of information.
8.	Data-sharing: meaning	Defines "data-sharing" to mean any disclosure by one public body to another of information, including personal data. Where changes in information held by one public body automatically changes information held by another, this is also deemed to be data-sharing.

9.	Public body: meaning	<p>Defines “public body” to include Ministers, specified officers of the State (e.g. the Attorney General), certain bodies established by law or funded and operated by the State and bodies designated as such by Ministerial Order. The definition excludes however:</p> <ul style="list-style-type: none"> • schools not established and maintained by Education and Training Boards, • commercial State-owned bodies listed in the Schedule (including An Post and CIE), and • bodies designated by way of Ministerial Order.
10.	Deceased persons	Provides that the proposed Act applies to information concerning deceased persons as well as living persons.
11.	Exclusions	<p>Excludes the proposed Act from applying to data-sharing for purposes including:</p> <ul style="list-style-type: none"> • criminal investigation, prosecutions or detention, • the functions of the Criminal Assets Bureau, • State defence, security and intelligence activities, and • international relations of the State.
Part 3: Regulation of data-sharing		
12.	Data-sharing: requirements	Provides for the conditions upon which public bodies may share personal data (other than special categories of personal data) in cases where no other law (whether domestic or EU) sets the conditions for doing so.
13.	Directions	Provides for the Minister (with, where appropriate, the consent of any other Minister concerned) to direct a public body to disclose information to one or more other public bodies.
Part 4: Data-sharing agreements		
14.	Application (Part 4)	<p>Provides that Part 4 applies to disclosures by public bodies to other public bodies of personal data in cases where no other law (whether domestic or EU) permits or requires them to do so.</p> <p>Transfers of “special categories of personal data”, such as information about health, political opinions or sexual orientation, are specifically excluded from the application of Part 4.</p> <p>Disclosures relating to public service pensions and provided for in Part 5 and so are also excluded from Part 4.</p>
15.	Obligation to enter into data-sharing agreements	Requires public bodies that propose to share data in circumstances to which Part 4 applies to enter into data-sharing agreements before doing so.
16.	Formal requirements	Requires data-sharing agreements to be in writing.
17.	Accession to data-sharing agreement	Provides for that a public body may accede to an existing data-sharing agreement.
18.	Content of a data-sharing agreement	Specifies the minimum contents of a data-sharing agreement. These include:

		<ul style="list-style-type: none"> the information to be disclosed, the purpose and legal basis for doing so, how the information is to be processed, security measures, and provisions concerning retention and deletion of the information.
19.	Review of operation of data-sharing agreement	Requires the parties to a data-sharing agreement to review its terms and operation, at intervals of no more than 5 years, taking into account any technical, policy and legislative changes.
20.	Lead agency	Requires every data-sharing agreement to specify a party as the lead agency with responsibility for <ul style="list-style-type: none"> keeping the identities of parties up to date, publishing details of reviews of the agreement, and receiving data access requests concerning information disclosed under the agreement and (where appropriate) forwarding them to the relevant data controller.
21.	Cessation	Provides that a lead agency must notify the Minister of the expiry or termination of a data-sharing agreement. The Minister publishes a notice of the cessation and ensures that website, maintained by the Minister, providing access to the agreement make clear that it has expired.
Part 5: Public service information		
22.	Definitions (Part 5)	Contains definitions relevant to sharing and disclosure of information concerning public service pensions.
23.	Application (Part 5)	Provides that Part 5 applies to data, including personal data. Part 5 also applies to special categories of personal data (such as data concerning a person's health) where it is processed for the administration or valuation of a public service pension scheme.
24.	Administration of Single Public Service Pension Scheme	Provides for the transfer of information to a Minister of Government or relevant authority (as defined in the Public Service Pensions (Single Scheme and Other Provisions) Act 2012) for the purpose of the performance of their functions or the administration of the Single Public Service Pension Scheme.
25.	Administration of pre-existing public service pension schemes	Provides for the transfer of information to a Minister of Government or public service body (as defined in the Public Service Pensions (Single Scheme and Other Provisions) Act 2012) for the purpose of the performance of a statutory function or the administration of a pre-existing public service pension schemes.
26.	Public service policy analysis	Provides for the transfer of information to the Minister for a variety of reasons including the performance of a statutory function, actuarial calculations and policy analysis.
27.	Information requests	Authorises the Minister to specify, in relation to information to be supplied under sections 24, 25 and 26, classes of information to be supplied, the

		periods to which it relates, the format in which it is to be supplied and the date by which it must be provided.
28.	Data protection impact assessment	Requires the Minister to assess the potential impacts on data protection before requiring any additional information under sections 24, 25 and 26.
29.	Anonymisation	Requires personal data provided to the Minister under section 26 (that is, for policy analysis) to be provided in anonymised (or, if required, pseudonymised) form.
30.	Pension scheme information systems	Authorises the Minister to establish a database to support his or her functions in relation to administering the Single Public Service Pension Scheme. Requires public service bodies to establish and maintain connections with the database to transfer required information to the Minister and to query information about public service pensions in it.
31.	Transparency	Requires the Minister to publish information concerning information provided and processed under Part 5 of the proposed Act.
Part 6: Business information		
32.	Definitions (Part 6)	<p>Contains definitions relevant to the transfer of business information.</p> <p>“Business information” is defined to include details of undertakings such as names, registration numbers (if any), addresses and information derived from accounts such as numbers of employees, net assets and turnover.</p> <p>“Undertaking” is defined to include natural persons engaged in business activities, as well as partnerships, companies and unincorporated bodies.</p>
33.	Application (Part 6)	<p>Provides that Part 6 applies to disclosures by public bodies to other public bodies of business information in cases where no other law (whether of domestic or EU) permits or requires them to do so.</p> <p>Expressly authorises the Revenue Commissioners to disclose business information that is taxpayer information in accordance with Part 6.</p>
34.	Allocation of unique business identifier number	Authorises the Minister to allocate and issue in respect of any undertaking a ‘unique business identifier number’.
35.	Disclosure of business information	<p>Authorises public bodies to disclose business information to other public bodies for:</p> <ul style="list-style-type: none"> the purposes of the performance of their respective functions, and purposes specified in section 12(2)(a)(ii) of the Bill (which include verification of identities, improving the delivery of services or avoiding duplication of effort).
Part 7: Base registries		
36.	Application (Part 7)	Provides that Part 7 does not apply to special

		categories of personal data (such as data concerning a person's health, political opinions or sexuality), or to databases containing such data.
37.	Designation of base registry	Authorises the Minister (with the consent of other Ministers as appropriate) to designate any database of which the copyright is owned by a public body as a base registry.
38.	Base registry owner	Provides that the public body that owns a base registry must ensure that the information in it is accurate, up to date, complete and accessible to authorised users. If the base registry contains personal data, the owner must be the lead agency in respect of a data-sharing agreement relating to disclosure to public bodies.
39.	Processing of information	Authorises a base registry owner to process information in order to comply with its obligations under section 38, even if no other Irish or EU law authorises such processing.
40.	Terms of service	Requires a base registry owner, following consultation with the Data Governance Board and the consent of the Minister, to prepare terms of service for the access by other public bodies to the base registry. These must be published by the Minister.
41.	Access to information	Authorises a base registry owner, for the purpose of ensuring that information is accurate, up to date and complete, to modify information in a base registry and to access relevant information held by other public bodies.
42.	Obligation to use base registry	Provides that, where a data source has been designated a base registry for a particular purpose, public bodies must have recourse to that base registry (rather than other sources) when collecting data for that purpose.
Part 8: Personal data access portal		
43.	Application (Part 8)	Provides that Part 8 applies to personal data including special categories of personal data.
44.	Establishment of personal data access portal	Authorises the Minister to develop an information system to be known as the "Personal Data Access Portal" which will allow data subjects to make requests to public bodies relating to rights under the GDPR. The rights expressly mentioned include: <ul style="list-style-type: none"> • viewing personal data held by a public body, and • Article 15 (right of access), • Article 16 (rights of rectification) • Article 17 (right to be forgotten) • Article 18 (right to restrict processing), • Article 20 (right to data portability) • Article 21 (right to object to processing)
Part 9: Data governance		
Chapter 1: Data Governance Board		
45.	Appointment of Board	Provides for the Minister to appoint the Data

		Governance Board.
46.	Functions of Board	Describes the general functions and purposes of the Board which includes review of data-sharing agreements.
47.	Membership of Board and related matters	Provides that the Board is to comprise between 6 and 12 members.
48.	Committees	Authorises the Board to establish committees, which may include persons who are not members of the Board.
49.	Disqualification from membership of Board	Standard provision dealing with disqualification of persons from becoming or remaining a member of the Board.
50.	Resignation from membership	Standard provision dealing with resignation of members of the Board.
51.	Casual vacancies	Standard provision for filling casual vacancies in the Board.
52.	Reporting	Standard provision requiring the Board to produce an annual report and lay it before the Houses of the Oireachtas.
Chapter 2: Review of data-sharing agreements		
53.	Definitions (Chapter 2)	Defines terms relevant to the functions of the Board in reviewing data-sharing agreements.
54.	Exclusions (Chapter 2)	Excludes less significant changes to data-sharing agreements, such as accession of a public body to an existing agreement or a change of lead agency.
55.	Public consultation	Requires public bodies to undertake a public consultation before entering into a data-sharing agreement.
56.	Submission of documentation and information to Board	Requires a public body nominated to be lead agency under a proposed data-sharing agreement to submit the terms of the proposed agreement to the Board for review.
57.	Review of data-sharing agreement	<p>Provides for the Board to review proposed data-sharing agreements. The review criteria include:</p> <ul style="list-style-type: none"> • compliance with the proposed Act, • compliance with any model data-sharing agreement produced by the Minister under section 66, • compatibility with data protection law, • security measures applicable to personal data, • submissions made in response to the public consultation, and • the public interest. <p>The parties to the agreement must take account of any recommendations the Board may make and amend the agreement accordingly.</p>
58.	Amendments following review	Provides where the Board recommends changes dealing with 'substantial issues', the proposed agreement must be amended accordingly and re-submitted for review.
59.	Execution of agreement	Provides for execution by the parties of agreements

		approved by the Board and incorporating all recommended amendments.
60.	Publication (laying of documents)	Provides for publication of data-sharing agreements following their execution or amendment by accession or withdrawal of a public body. Data-sharing agreements must be laid before the Houses of the Oireachtas.
61.	Effective date of agreement	Provides that the effective date of a data-sharing agreement is the date of its publication.
62.	Time periods and documentation	Provides for the Board to set the periods for public consultations on proposed data-sharing agreements and for the submission to it of documents relating to proposed agreements and the information to be submitted.
Chapter 3: Governance		
63.	Application (Chapter 3)	Provides that Chapter 3 of Part 9 applies to personal data (including special categories of personal data) and to information that is not personal data.
64.	Rules, procedures and standards	Authorises the Minister to prescribe rules, procedures and standards in relation to the operation and use of base registries for the processing and management of data by public bodies.
65.	Guidelines	Authorises the Minister (after consultation with other Ministers as appropriate) to prepare and issue guidelines to public bodies concerning their functions under the proposed Act and other legislation concerning data-sharing.
66.	Model agreements	Authorises the Minister (after consultation with other Ministers as appropriate) to prepare or revise model agreements concerning data-sharing for the purpose of the proposed Act or other relevant legislation. Where a model agreement has been prepared, public bodies must use it as the basis for any data-sharing agreement they enter into.
67.	Publication of regulations and guidelines	Requires the Minister to publish rules, procedures and standards prescribed under section 64 and any guidelines issued under section 65.
68.	Compliance report	Authorises the Board to require a public body to issue a report on the body's compliance with the proposed Act and any orders or regulations made under it.
Part 10: Miscellaneous		
69.	Prohibition on requests for certain documents	Provides for the Minister to require public bodies to avoid duplication of tasks and use information (by means such as data-sharing) more efficiently. For that purpose, the Minister (after consultation with other Ministers as appropriate) may direct public bodies not to request that persons provide them with particular documents or classes of document.

		Similarly, the Minister may prescribe purposes for which public bodies may not request persons to produce original or copy documents.
70.	Specification of information	<p>Authorises the Minister (with the consent of other Ministers as appropriate) to direct public bodies to collect information (or particular classes of information) for specified purposes (including modernising and developing public services) in formats specified by the Minister.</p> <p>This provision applies to all types of information (including special categories of personal data), whether or not the disclosure of the information is regulated by the proposed Act or any other legislation.</p>
71.	Provision of information on data-sharing	Provides that the Minister may direct a public body to provide him or her with information concerning the public body's data-sharing arrangements, whether under the proposed Act or other legislation.
72.	Amendment of Ministers and Secretaries (Amendment) Act 2011	Amends the <i>Ministers and Secretaries (Amendment) Act 2011</i> to authorise the Minister to collect data concerning public service pensions in relation to Part 5 of the proposed Act.

Source: Prepared by the L&RS based on the [Data Sharing and Governance Bill 2018](#)

Introduction

The [Data Sharing and Governance Bill 2018](#) (hereafter ‘the Bill’) was published on 12 June 2018. According to the Bill’s [Explanatory Memorandum](#), the purpose of the Bill is:⁹

“to provide a generalised legal basis for the sharing of data between public bodies while also setting out appropriate safeguards under which such sharing should take place.”

Key objectives of the Bill

As noted above, the Bill seeks to provide for a generalised legal basis for data sharing between public bodies for specific, legitimate purposes, including:¹⁰

- “Making public services more seamless by reducing the burden of providing the same information to different public bodies;
- Facilitating the effective administration, supervision and control of public services;
- Establishing entitlements to public services;
- Identifying and correcting erroneous information; and
- Evaluating the effectiveness of public services.”

The press release accompanying publication of the Bill states that:¹¹

“Enactment of this legislation will deliver tangible benefits to the public and to business. Sharing and reusing data will cut down on waste and duplication by ensuring that individuals and businesses should not have to supply the same information more than once to public bodies. More extensive data sharing will also support better policy development and more efficient and effective policy implementation.

The Bill also sets out a series of important governance measures to ensure that personal data is shared by public bodies in a lawful, proportionate and transparent manner in accordance with national and EU data protection law, including the new General Data Protection Regulation (GDPR)”

In the press release for the Bill, the Minister for Public Expenditure and Reform, Paschal Donohue, TD, stated that:¹²

“[T]he Bill is key to delivering on our public service reform commitments to expand digital delivery of services and make greater use of data. It will also provide for stronger governance and transparency by public service bodies in the way they share and manage data, which will assist public bodies in meeting the more stringent data protection requirements provided for under the GDPR.”

The press release continues with further statements from Minister of State for Public Procurement, Open Government and eGovernment, Mr Patrick O’Donovan, TD, who added:

⁹ Department of Public Expenditure and Reform, Explanatory Memorandum for the *Data Sharing and Governance Bill 2018*. Available here: <https://data.oireachtas.ie/ie/oireachtas/bill/2018/55/eng/memo/b5518s-memo.pdf>

¹⁰ *ibid.*

¹¹ “Ministers Donohue and O’Donovan publish the Data Sharing and Governance Bill 2018”, Department of Public Expenditure and Reform Press Release, 12 June 2018. Available here: <https://www.per.gov.ie/en/ministers-donohue-and-odonovan-publish-the-data-sharing-and-governance-bill-2018/>

¹² *Ibid.*

“Significant opportunities are offered by making better use of data. Citizens and businesses can receive better services. Public bodies can operate more effectively and efficiently at a lower cost to the Exchequer. Better access to data will improve decision making and planning in the delivery of services”

Minister of State O'Donovan continued:¹³

“The public also has a strong expectation that their data protection rights will be respected and public bodies will use personal data responsibly, proportionately and securely. As the volume of data and our capacity to deliver digital services grow, the opportunities to improve services increase — but so too must our governance of citizens' data. This Bill will ensure that appropriate safeguards, accountability and transparency are in place to build the public's trust in public bodies' usage of their data. Accordingly, this Bill will be a very important stepping stone in helping take forward the Government's ambition to be an exemplar in the processing of citizen data.”

Principal themes

Given the short time between publication of the Bill (12 June 2018) and its Second Stage debate (19 June 2018), this Bill Digest takes a broad approach to its treatment of the Bill. In this context, the subsequent sections of this Digest discuss the following:

- Policy context and background;
- Sharing personal data in the public sector;
- Pre-legislative scrutiny;
- Principal provisions; and,
- Cost and implications.

Further related Library & Research Service resources¹⁴

On this Bill:

- L&RS [Bills Tracker page on the Data Sharing and Governance Bill 2018](#)

On previous Bills:

- Bills Digest: [Data Protection Bill 2018](#)

Other related L&RS resources:

- L&RS Note: [“European Union Data Protection Law and Policy”](#), October, 2016
- [“The EU-US privacy shield – a safe harbour for data transfers?”](#), Article in L&RS Research Matters (for the 32nd Dáil and 25th Seanad) (at page 77)

¹³ *Ibid.*

¹⁴ Please note that some of these sources are not available outside of the Houses of the Oireachtas ICT environment.

Policy context and background

Introduction

The Bill stems from a larger Government agenda to use information communication technologies ('ICT') to develop a more integrated public service network, such as the eGovernment¹⁵ agenda and open government data.¹⁶

The first national policies to specifically mention promoting data sharing within the public service appear to be:

- the 2011 Government Programme '[Towards Recovery: Programme for a National Government 2011–2016](#)';¹⁷ and
- the 2011 Department '[Public Service Reform Plan](#)'.¹⁸

Appendix 1 provides a timeline of policy developments concerning the development of the eGovernment and open government data agenda in Ireland, and the emergence of a specific agenda to promote data sharing within the public service in Ireland.¹⁹

Key parts of the timeline include:

- In 2013, the Department of Public Expenditure and Reform brought a Memorandum to Government setting out a series of actions to improve data-sharing in the public service, including the development of the heads of a Data-Sharing and Governance Bill.
- In August 2014, the Department of Public Expenditure and Reform published the policy paper entitled '[Data Sharing and Governance: Policy Proposals](#)' setting out key elements of proposed data sharing and governance legislation and the accompanying public consultation in August 2014.
- In October 2014, the Department of Public Expenditure and Reform published [The Civil Service Renewal Plan](#). Action 24 of the Civil Service Renewal Plan is to improve how data is collected, managed and shared within the civil service. One of the ways identified as necessary for achieving this is to "develop a coordinated approach to

¹⁵ The OECD defines eGovernment as "[t]he term "e-government" focuses on the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies has the potential to transform the structures and operation of government". OECD (2001), *E-government: Analysis Framework and Methodology* [online]. OECD Public Management Service, Public Management Committee. Available here: <https://stats.oecd.org/glossary/detail.asp?ID=4752>

¹⁶ The OECD explain open government data as "[t]he two main elements of OGD are normally defined as follows: Government data is any data and information produced or commissioned by public bodies; Open data are data that can be freely used, re-used and distributed by anyone, only subject to (at the most) the requirement that users attribute the data and that they make their work available to be shared as well." OECD Working Papers on Public Governance No. 22, Open Government Data, 2015, "[Towards empirical analysis of open data government initiatives](#)" [online]. Available at: https://www.espap.pt/Documents/espap_lab/2015_04_Open_Government_Data.pdf

¹⁷ Available at: https://www.taoiseach.gov.ie/eng/Work_Of_The_Department/Programme_for_Government/Programme_for_Government_2011-2016.pdf

¹⁸ Department of Public Expenditure and Reform (2014), '[Public Service Reform Plan 2014-2016](#)'. Available here: <http://www.reformplan.per.gov.ie/2014/downloads/files/Reform%20Plan%202011.pdf>

¹⁹ The reports and strategies set out above may not represent the full spectrum of such policy developments or be directly connected to the development of the General Scheme of the Data Sharing and Government Bill. Rather they are set out to illustrate the range of development behind the State's public service data agenda more generally.

data sharing and infrastructure as part of the forthcoming ICT Strategy” (at p. 34). Furthermore, Action 19 identifies the need to “recognise data as a corporate asset and develop a common data model and coordinated data infrastructure, underpinned by legislation” (at p. 30).

- The [Public Service ICT Strategy](#) 2015 notes that “sharing of data on a whole of government basis to support better decision making, drive efficiency and deliver a range of new digital Government services to citizens and businesses, subject to relevant legislation”²⁰
- Subsequent to this the Department of Public Expenditure and Reform published in July 2016 the [‘General Scheme of the Data Sharing and Governance Bill’](#).
- The Department of Public Expenditure and Reform referred the General Scheme to the Joint Committee on Finance Public Expenditure and Reform, and Taoiseach for PLS in July 2016.
- The Joint Committee published its [“Report on Pre-legislative scrutiny on the General Scheme of the Data Sharing and Governance Bill”](#) in July 2017.

Policy background

According to the [Regulatory Impact Analysis](#) (RIA) for the Bill, originally published in 2015 in tandem with the General Scheme of the Bill, data sharing presently occurs extensively across the public service under “a number of existing legal provisions”.²¹ The RIA argues that the current level of public service delivery would “not be possible without this data sharing taking place”.²²

However, according to the Bill’s RIA, increased efforts at optimising data sharing between public bodies would potentially lead to “a more seamless and efficient service delivery to citizens and businesses fully consistent with data protection requirements”.²³

In light of the above, the key policy problem informing the Bill, from the Government’s perspective, is set out below:²⁴

“Experience has been that overly restrictive interpretation of current Data Protection Law on the part of some Public Bodies can lead them to...be reluctant to share data with other Public Bodies where it would otherwise be beneficial. Furthermore, where a cross-departmental requirement exists, there may not be sufficient incentive for any particular Department to meet it.”

This is, in the view articulated in the Bill’s RIA, partially due to the legal framework for data sharing provisions being included in specific legislation related to the requirements of specific

²⁰ Department of Public Expenditure and Reform, 2015: 06. *Public Service ICT Strategy*. Available [here](#).

²¹ Department of Public Expenditure and Reform, 2015. *Data Sharing and Governance Bill, Regulatory Impact Analysis*. Available [here](#).

²² *ibid*

²³ *ibid*

²⁴ *ibid*: 02.

departments or related public bodies. The RIA identifies the following disadvantages with the current legal landscape for public sector data sharing:²⁵

1. “Where a public body identifies a need for data-sharing, it will, for the avoidance of doubt, usually seek to have an explicit legal basis in primary legislation before the sharing can take place. However, access to the legislative schedule is limited (especially for smaller bodies) and there can be a significant delay in establishing the necessary legal basis;
2. Where a cross-departmental data-sharing requirement exists, there may not be sufficient incentive for any particular Department to meet it; and
3. Whereas data-sharing represents an important and growing area of government activity, the fact that the relevant provisions are spread over many Acts make the process opaque and leads to a lack of legal clarity regarding the legal basis to appropriate data-sharing.”

Legal background

The broader policy context in which the Bill is situated relates in the main to individual data privacy. In this regard, the right to privacy and protection of personal data are protected under both European Union and national legislation. This section summarises the main pieces of national law regulating the processing of (personal) data.²⁶

Constitution of Ireland / Bunreacht na hÉireann

In Ireland, the right to privacy has been recognised by the courts as an unenumerated right under Article 40.3 of the Constitution of Ireland.²⁷ Irish courts have also recognised the right to privacy as including the right to privacy of private communications free from interference by the State, e.g. interception or surveillance.²⁸

Furthermore, in *Schrems v Data Protection Commissioner*²⁹ the High Court stated that the accessing of private communications originating within a person’s home by State Authorities directly engages the Constitutional right to privacy and the right to inviolability of the dwelling under Article 40.5.

Data Protection Acts 1988 to 2018

The *Data Protection Acts 1988 to 2018 (Data Protection Acts)* are the main pieces of legislation governing the processing of data in Ireland. In accordance with the *Data Protection Acts*, where a person gives their personal data to an organisation, the organisation has a duty to keep those details private and safe. In addition to placing certain

²⁵ *Ibid*: 02

²⁶ For information on pre GDPR European Union data protection law and policy please refer to the L&RS’ Note (October 2016), *European Union Data Protection Law and Policy*. Available here: http://vhlms-a01/AWDData/Library2/LRSNote_EuropeaDataProtectionLawPolicy_154828.pdf

²⁷ *McGee v Attorney General* [1973] IESC 2; *Kennedy and Arnold v Attorney General* [1987] IR 587; *Re a Ward of Court* (No 2) [1996] 2 IR 79

²⁸ *Kennedy and Arnold v Attorney General* [1987] IR 587 at p. 592 and *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.47

²⁹ *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.48

obligations on the organisations, the *Data Protection Acts* give people certain rights relating to their personal data.³⁰

The recently enacted [Data Protection Act 2018](#) provides for enforcement of the General Data Protection Regulation (GDPR) – discussed below - by means of complaints to the new Data Protection Commission (DPC), investigations, information and enforcement notices, court action and – a new feature under the GDPR – administrative fines. The DPC may impose administrative fines on data controllers or data processors that infringe the GDPR up to maximum of 4% of worldwide turnover or €20 million, whichever is higher.

The [Directive](#) deals with data protection for the purposes of law enforcement, including police, prosecution and prison functions.³¹ It provides for rights of data subjects to information about the processing of their personal data, to complain to the DPC about breaches, and to seek remedies in court or through the Commission.

The General Data Protection Regulation

[Regulation EU 2016/679](#), commonly called the General Data Protection Regulation (shortened to 'GDPR'), is a 2016 Regulation of the EU that is intended to harmonise and update rules relating to the processing of personal data:

- of data subjects who are in the EU, and
- by businesses that have operations in the EU, or that offer goods and services to EU residents.

The GDPR, which came into effect on 25 May 2018, replaces the EU's [1995 Data Protection Directive](#), which was adopted when the internet was only beginning to emerge as a central component of social, commercial and administrative activities. The GDPR is intended to enhance the protection of EU citizens' rights, adapt rules to reflect the enormous increase in reliance on digital information, respond to changes in technology and business practices and to reduce administrative overheads.

The GDPR retains many of the key components of existing EU data protection laws, including the 'data protection principles' that underlie the rights of data subjects and the

³⁰ Data Protection Commissioner, *A guide to your rights* [online]. Available here:

<https://www.dataprotection.ie/docs/A-guide-to-your-rights-Plain-English-Version/r/858.htm>

³¹ DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Available [here](#).

responsibilities of data controllers and processors.³² The principal changes introduced by the GDPR include:

- **a uniform data protection regime in all Member States:** unlike the 1995 Data Protection Directive, the core provisions of the GDPR have direct effect across the EU and do not need to be transposed through national legislation;
- **increased territorial scope:** the GDPR applies to any organisation that processes personal data of EU residents for the purposes of its activities in the EU, regardless of where the organisation is based or where it processes the data. Similarly, it applies to organisations throughout the world that process personal data of EU residents for the purpose of offering them goods or services, or monitoring their behaviour within the EU³³;
- **establishment of a European Data Protection Board:** this is to coordinate the actions of Member States' regulatory authorities and ensure consistent enforcement of the GDPR across the EU;
- **transfers and processing of personal data outside the EU** to be governed by standards provided for in the GDPR and to be formalised by the EU Commission,
- **a risk-based approach**, whereby data processors are responsible for assessing the potential effect of their operations and planning suitable protections accordingly,
- **strengthened provisions on consent:** the GDPR requires data controllers to be able to demonstrate that all required consents have been given. Required consents must be requested in clear and easily understood terms, and the data subject must be able to withdraw consent as easily as giving it;³⁴
- **right of access:** a data subject can ask a data controller to confirm if they hold his or her personal data, and if so, to provide a free electronic copy and explain where and for what purpose the data is being processed;³⁵
- **data portability:** data subjects can arrange for the transfer from one controller to another of personal data they have provided, either by having it provided to them in a structured, machine-readable format, or having one controller forward it to another;³⁶
- **right to be forgotten:** a data subject can require personal data to be erased in circumstances including where the data is no longer necessary for the purpose for which it was supplied, where the data is being processed unlawfully or where the data subject withdraws consent to processing;³⁷
- **privacy by design:** data controllers and processors must ensure that appropriate measures to protect privacy are an integral part of their systems and organisational processes;³⁸
- **supervisory arrangements:** Member States must ensure that data protection supervisors (such as the new Data Protection Commission) are fully independent.³⁹ Data controllers that operate in multiple Member States can nominate a lead supervisory authority as their principal supervisor.⁴⁰

³² Article 5. The principles have been a basic element of data protection laws since their inclusion (in a slightly different form) in the 1981 [Council of Europe Convention on Data Protection](#), which was implemented in Ireland by the [Data Protection Act 1988](#), and subsequently in EU law under the 1995 [Data Protection Directive](#).

³³ Article 3

³⁴ Article 7

³⁵ Article 15

³⁶ Article 20

³⁷ Article 17

³⁸ Article 25

³⁹ Article 52

⁴⁰ Article 56

- **compliance procedures:** rather than registering extensive information with supervisors, data controllers that employ 250 or more persons must keep records demonstrating compliance, which must be produced when requested.⁴¹ Data controllers that regularly and systematically process large amounts of personal data or sensitive personal data (this includes many public authorities) must appoint data protection officers to oversee compliance.⁴²
- **breach notifications:** breaches of data security that pose risks to the rights and freedoms of persons must be notified to supervisory authorities within 72 hours. Data processors must notify the data controllers for whom they act without undue delay;⁴³
- **penalties and compensation:** the GDPR provides for administrative fines to be imposed on data processors or controllers that breach its provisions. The maximum penalty is 4% of global turnover or €20 million, whichever is higher.⁴⁴ The data processor or controller is also liable to pay compensation to persons who suffer damage as a result of the breach.⁴⁵

The GDPR applies generally to personal data processing that occurs as part of activities that come within the scope of Union law – that is, all areas and subject matters in which the EU has competence to act. However, it specifically excludes several types of activity from its application. A significant exclusion is the processing of personal data by ‘competent bodies’ for the purpose of preventing, investigating, or prosecuting crime, executing penalties or safeguarding public security. Processing of personal data in those circumstances is to be regulated under Directive (EU) 2016/680.

GDPR seeks to define data protection rules for more than 510 million EU inhabitants, and will affect governments, businesses and social institutions in Member States and beyond.

The Directive

The GDPR does not apply to the processing of personal data in the context of law enforcement. That issue is addressed by [Directive \(EU\) 2016/680](#) (for convenience, ‘the Directive’), which the EU adopted in April 2016. Member States must transpose the Directive into their national laws by 6 May 2018.

It addresses processing of personal data by ‘competent authorities’ within Member States’ police, prosecution and prison services, as well as transfers between Member States. Similarly to the GDPR, the Directive requires competent authorities to process personal data in accordance with the data protection principles, to respect the principle of proportionality and to deal in a transparent fashion with data subjects in relation to their rights.

The Directive provides for the security of personal data, the exercise of data subjects’ rights, and oversight and enforcement by regulatory authorities. It does so in terms similar to and consistent with the GDPR. The rights of data subjects under the Directive include:

⁴¹ Article 30

⁴² Article 37

⁴³ Article 33

⁴⁴ Article 83

⁴⁵ Article 82

- the right of access (to establish whether, and if so, why a controller is processing personal data),
- the right to have incorrect data rectified, and
- where personal data has been improperly acquired, processed or retained, the right to have it erased.

Data subjects whose rights are breached may complain to the supervisory authority and seek a remedy either through actions of that authority or in the courts. In view of the requirements of law enforcement and penal systems, the Directive allows Member States to set limits on the exercise of data subjects' rights where, for example, it could obstruct justice or prejudice public security.

The Directive provides for the supervisory authority to investigate and take corrective action in response to breaches of its provisions. However, a significant difference from the GDPR in this regard is that the Directive does not provide for administrative fines on controllers or processors that breach its requirements. As under the GDPR, data subjects have the right to an effective judicial remedy (including, where appropriate, compensation) for wrongful acts of controllers, processors or the supervisory authority.

Similarly to the GDPR, the Directive requires competent authorities to designate data protection officers to oversee data protection compliance in their organisations and liaise with their Member State's supervisory authority. Competent authorities must assess the data protection risks faced by their organisations, and plan and execute their operations accordingly. The Directive requires comprehensive record keeping to ensure transparency and accountability to the supervisory authority.

The Directive regulates the transfer of personal data by competent authorities both within Member States and outside them. It requires transfers to be secure and to be effected only if and to the extent necessary. Senders and receivers must be identified and are obliged to maintain detailed records of transfers for the purpose of accountability.

The GDPR and its relevance to the Bill

The core themes of the GDPR are transparency and accountability. The former requires, among other things, that individuals know the reasons for the processing of their data, how it is being used and by whom. Accountability requires data controllers and processors to be responsible for complying with data protection law and to demonstrate their compliance with it.

The GDPR, as with existing data protection law, is principles-based. It requires persons processing personal data to carry out assessments before processing in order to ensure the

processing is lawful. Article 5 of the GDPR sets down the data processing principles.⁴⁶ Text box 1 below sets out those principles.

Text box 1: Data processing principles in Article 5 of the GDPR

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**‘purpose limitation’**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**‘data minimisation’**);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**‘accuracy’**);
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**‘storage limitation’**); and,
- 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, using appropriate technical or organisational measures (**‘integrity and confidentiality’**).

Source: <https://gdpr-info.eu/art-5-gdpr/>

⁴⁶ At present under s.2 of the *Data Protection Acts* personal data may only be processed provided the data controller complies with the rules for processing personal data. The Data Protection Commissioner provides that a data controller must: “Obtain and process the information fairly; Keep it only for one or more specified and lawful purposes; Process it only in ways compatible with the purposes for which it was given to you initially; Keep it safe and secure; Keep it accurate and up-to-date; Ensure that it is adequate, relevant and not excessive; Retain it no longer than is necessary for the specified purpose or purposes; Give a copy of his/her personal data to any individual, on request.” (see Data Protection Commissioner, *‘The Data Protection Rules Your legal responsibilities as a Data Controller’*. Available at: <https://www.dataprotection.ie/docs/Data-Protection-Rules/y/21.htm>)

EU data protection law⁴⁷

Charter of Fundamental Rights of the European Union 2000⁴⁸

Article 7 of the Charter of Fundamental Rights of the European Union 2000 ('EU Charter') provides for the right to respect for private and family life ('right to privacy').⁴⁹ Article 8 of the EU Charter formally recognised the right to protection of personal data.⁵⁰

The EU Charter became legally binding on the EU institutions and Member States when they are implementing EU law after the adoption of the Treaty on the Functioning of the European Union ('the Lisbon Treaty') in 2009. In doing so the right to data protection contained therein became a specific fundamental right in EU law.⁵¹

Limitations to the right to privacy and right to data protection

Neither the right to privacy nor the right to data protection are absolute rights. The Lisbon Treaty recognises that the right to data protection must be balanced against other rights and freedoms.⁵² In addition to the obligation to set down data protection rules under Article 16 of the Lisbon Treaty, it also requires EU legislators to set down rules for the free movement of personal data.⁵³

The EU Charter also provides that the rights contained in it may be limited, where the limitation is set down in law and it respects the essence of the right being limited. Under Article 52 any limitations must be limited to what is proportionate and necessary, and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.⁵⁴

In Ireland, the High Court in *Schrems v Data Protection Commissioner* recognised that the interception of private communications by the State is not in itself necessarily unlawful. The Court stated that where appropriate safeguards are in place, the interception or electronic

⁴⁷ For more information on the GDPR and the Directive (EU) 2016/680 please refer to the L&RS' Note on 'European Union Data Protection Law and Policy' (October 2016)

⁴⁸ The EU Charter may only be invoked when a domestic court is applying EU law (for more information on the EU Charter please refer to the L&RS Spotlight No.2 of 2016 'International human rights law: operation and impact', at pp.12-13. Available at: http://data.oireachtas.ie/ie/oireachtas/libraryResearch/2016/2016-09-28_spotlight-international-human-rights-law-operation-and-impact_en.pdf

⁴⁹ Available here: <http://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life>

⁵⁰ Available here: <http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data>

⁵¹ EU Agency for Fundamental Rights and Council of Europe (2014), 'Handbook on European data protection law', at p.20. Available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

⁵² Karen Murray (2016), 'EU Data Protection Reform', (2016) 34 Irish Law Times 26-28

⁵³ <http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-the-functioning-of-the-european-union-and-comments/part-1-principles/title-ii-provisions-having-general-application/158-article-16.html>. See also: <http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-5-general-provisions-on-the-unions-external-action-and-specific-provisions/chapter-2-specific-provisions-on-the-common-foreign-and-security-policy/section-1-common-provisions/126-article-39.html>

⁵⁴ http://www.europarl.europa.eu/charter/pdf/text_en.pdf, at Ch. 364, p.21.

surveillance of communications may be lawful where it is indispensable for the preservation of State security.⁵⁵

European Union case law

There have been a number of judgments by the Court of Justice of the European Union ('CJEU') affirming the importance of the fundamental right to protection of personal data. Of particular relevance to data sharing by public authorities is [C-201/14 Bara & Others v CNAS and ANAF](#) ('*Bara*'). In *Bara*, the CJEU highlighted that the transfer of personal data between public authorities must have a legal basis and that data subjects must be informed of the transfer or processing.⁵⁶ Text box 2 below summarises the *Bara* judgment.

Text box 2: [C-201/14 Bara & Others v CNAS and ANAF](#)

In *Bara*, the Romania National Tax Administration Agency (ANAF) transferred income tax details relating to the applicants to the Romanian National Health Insurance Fund (CNAS) to determine the amount of health insurance contributions owed by the applicants. The data was transferred on the basis of a protocol agreed between the ANAF and CNAS. That protocol was not officially published.

As a result of the transferred data, the CNAS required payment of health insurance arrears from the applicants. The applicants challenged the lawfulness of the data transfer on the basis that the data was used for purposes other than that which it was originally collected for without their consent, and without them being given prior notice of the transfer.

The Romanian court asked the CJEU, among other questions, if a national administrative measure can permit a public body to transfer to another public body personal data, and for the subsequent processing of that data by the receiving public body, without the data subject being informed of the transfer and processing.

The CJEU held that a national administrative measure cannot permit a public body to transfer to another public body, personal data and its subsequent processing without the data subjects having been informed of the transfer or processing.

As a result of the decision in *Bara*, the Data Protection Commissioner ('DPC') updated its guidance on data sharing in the public sector. The DPC guidance on '[Data Sharing in the Public Sector](#)' recommends that public sector data sharing arrangements should.⁵⁷

- "Have a basis in primary legislation;
- Be made clear to individuals that their data may be shared and for what purpose;
- Be proportionate in terms of their application and the objective to be achieved;
- Have a clear justification for individual data sharing arrangements;
- Share the minimum amount of data to achieve the stated public service objective;
- Have strict access and security controls; and
- Ensure secure disposal of shared data."

⁵⁵ *Schrems v Data Protection Commissioner* [2014] IEHC 310 at para.49

⁵⁶ [C-201/14 Bara & Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate \(CNAS\), Agenția Națională de Administrare Fiscală \(ANAF\)](#) available here:

<http://curia.europa.eu/juris/document/document.jsf?docid=168943&doclang=EN>

⁵⁷ Available here: <https://dataprotection.ie/docs/Data-Sharing-in-the-Public-Sector/m/1217.htm>

In addition, on its website [GDPRandYou](#) the Data Protection Commission provides directions as to the obligations of organisations and the rights of individuals arising from the GDPR.

Text box 3 below sets out the relevant section on the site dealing with 'legal basis'.

Text Box 3: Data Protection Commission, 2018: What we mean when we talk about a 'Legal Basis'

[Organisations] should look at the various types of data processing [they] carry out, identify [their] legal basis for carrying it out and document it. This is particularly important where consent is relied upon as the sole legal basis for processing data. Under the GDPR, individuals will have a stronger right to have their data deleted where customer consent is the only justification for processing. [Organisations] will have to explain [their] legal basis for processing personal data in [their] privacy notice and when [they] answer a subject access request.

For government departments and agencies, there has been a significant reduction in the number of legal bases they may rely on when processing data. It will no longer be possible to cite legitimate interests. Instead, there will be a general necessity to have specific legislative provisions underpinning one or more of the methods organisations use to process data. All organisations need to carefully consider how much personal data they gather, and why. If any categories can be discontinued, do so. For the data that remains, consider whether it needs to be kept in its raw format, and how quickly you can begin the process of anonymisation and pseudonymisation.

Source: Data Protection Commission, 2018. *GDPR 12 Steps*, Available [here](#). (Emphasis added by the L&RS)

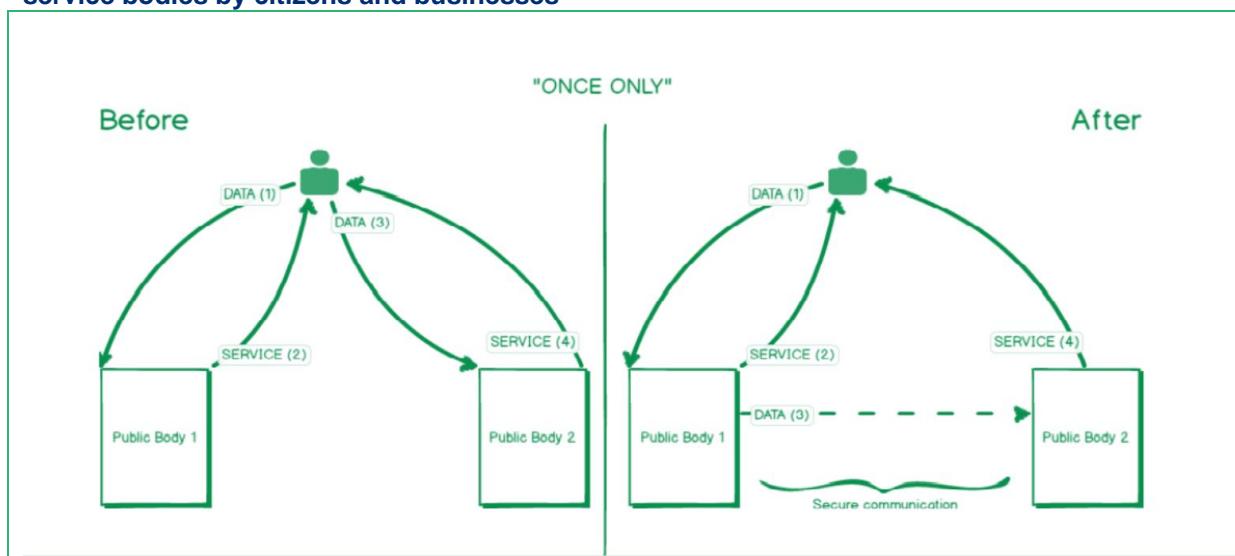
Sharing personal data in the public service

What does the Bill propose?

The Bill proposes a dual approach to regulating data sharing within the public service. First, it proposes to provide a general legislative basis for the sharing of data between public service bodies or their agents.⁵⁸ Second, it proposes to provide a governance framework for public service data sharing in a manner which conforms with data protection principles,⁵⁹ e.g. that data sharing adheres to the data processing rules under the *Data Protection Acts*.

The data sharing provisions proposed in the Bill are, according to Department of Public Expenditure and Reform's (DPER) Policy Proposals, intended to facilitate "an ask-once, use-many vision" within the public service,⁶⁰ e.g. a person will only be asked for their information once, but that information can be shared within the public service for the provisions of other services. The Policy Proposals for data sharing in the public sector published in 2014 by DPER provide an illustrative example of how the general legislative basis being provided by the proposed legislation will work in practice. Figure 1 below reproduces that example.

Figure 1: Ask-once, use-many to reduce duplication of provision of information to public service bodies by citizens and businesses



Source: Department of Public Expenditure and Reform (2014), *Data Sharing and Governance: Policy Proposals* (at p.3). Available here: <http://www.per.gov.ie/en/datasharing/>

According to the Policy Proposals the implementation of an ask-once, use-many vision will help to considerably reduce costs and the administrative burden on citizens and businesses,

⁵⁸ Department of Public Expenditure and Reform (2015), *Regulatory Impact Assessment (RIA) for Data Sharing and Governance Bill*.

⁵⁹ *ibid.*

⁶⁰ Department of Public Expenditure and Reform (2014), *Data Sharing and Governance: Policy Proposals* (at p.2). Available here: <http://www.per.gov.ie/en/datasharing/>

and will allow citizens and businesses to use more coordinated public services.⁶¹

Current data sharing in the Irish public service

The Policy Proposals leading to the development of the Bill provide a number of examples where current data sharing simplifies access to public services. These are set out in text box 4.

Text box 4: Current examples of data sharing within the Irish public service to simplify access to public services

- Details of birth registrations are forwarded by the General Register Office to the Department of Social Protection to automatically generate Child Benefit claims on behalf of parents.
- The Centenarian Bounty is a national award made by the President to people who have reached 100 years of age. The Department of Social Protection automatically forwards information about people who are about to reach 100 and who are in receipt of DSP pensions to the office of the President. Centenarians receive €2,540 and a congratulatory letter signed by the President.
- The Public Service Card Free Travel scheme was launched by the Department of Social Protection in December 2013. This scheme provides for the re-use of passport photographs held by the Department of Foreign Affairs in some circumstances. As a result of this data-sharing, applicants can register for free travel by post, reducing the burden on the service user.
- Since 2013, Student Universal Support Ireland (SUSI) has shared data with The Department of Social Protection, The Department of Education and Skills, and the Revenue Commissioners to streamline and simplify the student grant application process. This initiative enables SUSI to receive relevant information directly to assist in the evaluation and processing of grant applications. This reduces the need for applicants to provide documents.

Source: Department of Public Expenditure and Reform (2014), *Data Sharing and Governance: Policy Proposals* (at p.3). Available here: <http://www.per.gov.ie/en/datasharing/>

The Policy Proposals provide a number of examples where current data sharing is carried out between public service bodies under existing legislation. These are set out in text box 5.

Text box 5: Current examples of data sharing⁶²

- The Central Statistics Office conducts statutory surveys of Irish businesses. In 2009, a Memorandum of Understanding was signed between the Revenue Commissioners and the Central Statistics Office to allow for the exchange of business data. This data-sharing arrangement has reduced the need to survey businesses directly, while generating statistics in support of evidence based policy making.
- The Department of Social Protection, in conjunction with the Revenue Commissioners, has developed data exchanges to enhance the detection of fraud and control compliance. The legislative basis for the exchange of information is contained in Section 261 of the [Social Welfare Consolidation Act 2005](#). In one such exchange, information was provided by Revenue on persons

⁶¹ Department of Public Expenditure and Reform (2014), *Data Sharing and Governance: Policy Proposals* (at p.2). Available here: <http://www.per.gov.ie/en/datasharing/> [accessed on 10/11/2016]

⁶² It is also worth noting that "[f]rom 17 June 2017 any person sitting the Driver Theory Test will be required to present a valid Public Services Card at the Driver Theory Test Centre as proof of ID. At the time of booking the test, applicants will be asked to confirm that they possess a Public Services Card." See RSA website here: [Changes to Identification Required for Driver Theory Test](http://www.thejournal.ie/psc-theory-test-4026814-May2018/). See also article in the Journal.ie here: <http://www.thejournal.ie/psc-theory-test-4026814-May2018/>

who had received large amounts of interest on investments made. This data was matched with Department of Social Protection records to identify individuals who had failed to disclose large personal investments when applying for welfare payments. As a direct result of this data-sharing, millions of Euro in overpayments have been recovered.⁶³

- The Property Registration Authority has provided property data to the Revenue Commissioners under Section 151 of the *Finance (Local Property Tax) Act 2012* to establish and maintain a register of residential properties and associated liable persons in the State.
- The Department of Education and Skills shares post-primary student information with the State Examinations Commission in order to assist in planning state examinations.

Source: Department of Public Expenditure and Reform (2014), *Data Sharing and Governance: Policy Proposals* (at p.4). Available here: <http://www.per.gov.ie/en/datasharing/>

In its brief to the then incoming Minister for [Employment Affairs and] Social Protection in May 2016, the then Department of Social Protection outlined its current operations in respect of data matching programmes. The Department's main data matching programmes include the following:⁶⁴

- the Revenue Commissioners in respect of the commencement of employment, PRSI and related income data;
- the Irish Prison Service regarding prisoner data;
- third level Education Institutions;
- the Commission on Taxi Regulation;
- Health Services Executive mainly regarding the Fair Deal Scheme; and,
- the UK and Northern Ireland social services and pensions agencies.

The Department also operates what it refers to as “less systematic” data matches with the Personal Injuries Assessment Board, the Private Residential Tenancies Board and the Private Security Authority.⁶⁵

In this regard also, table 2 below lists the bodies that received the Public Service Identity data from the Department of Social Protection in 2016 along with the relevant legislative basis under which it was released.⁶⁶

⁶³ Department of Social Protection *Compliance and Anti-Fraud Strategy 2014-2018*, available at <http://www.welfare.ie/en/pdf/Compliance-and-Anti-Fraud-Strategy-2014-2018-.pdf>

⁶⁴ Department of Social Protection (2016), *Department of Social Protection Ministerial Brief May 2016 – Part B* [online]. Available at: <http://www.welfare.ie/en/downloads/MinisterialBriefPartBMay2016.pdf>

⁶⁵ *Ibid.*

⁶⁶ Department of Social Protection, 2017. *Comprehensive Guide to Safe Registration and the Public Services Card*. Available here: http://www.welfare.ie/en/downloads/DEASP_Comprehensive_Guide_to_SAFE_Registration_and_the_PSC.pdf

Table 2: Data sharing and the Public Services Card: Public Bodies whom received the public service identity data from the Department of Social Protection in 2016.

Legislative basis	Destination organisation
S262 <i>Social Welfare Consolidation Act 2005</i>	<ul style="list-style-type: none"> • Department of Agriculture, Food & the Marine • Department of Children & Youth Affairs • Department of Education & Skills • Department of Foreign Affairs (Passport Service) • Department of Justice (Citizenship section) • Central Statistics Office • Revenue Commissioners • Tusla - Child and Family Agency • Student Universal Support Ireland • Office of the Refugee Applications Commissioner • Local Authorities • HSE • Hospitals (Specified Body Only) • Nursing Homes (HSE Run i.e., Specified Body) • National Cancer Screening • BreastCheck Agency • ColoRectal Cancer Screening • Solicitors (Legal Aid Board Scheme and Client PPSN Verification requests) etc.
Section 8 of the <i>Health Identifiers Act 2014</i> (provided solely for the purpose of establishing, or maintaining the accuracy of, the National Register of Individual Health Identifiers)	<ul style="list-style-type: none"> • Department of Health/HSE (Individual Health Identifier)
Section 8d of the <i>Data Protection Acts</i> (required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property)	<ul style="list-style-type: none"> • Irish Blood Transfusion Service
<i>Immigration Act 2003</i> S8 (for the sharing of information regarding non-nationals)	<ul style="list-style-type: none"> • Irish Naturalisation and Immigration Service
S146 <i>Residential Tenancy Act 2004</i> (supply of information which to the Board is reasonably necessary for the performance by the Board of its functions)	<ul style="list-style-type: none"> • Residential Tenancies Board
Section 8b of the <i>Data Protection Acts</i> (required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid)	<ul style="list-style-type: none"> • Chief State Solicitor • An Garda Síochána • Garda Síochána Ombudsman Commission

Source: [Department of Social Protection, 2017](#).

What is administrative or public sector data?

Administrative or public sector data is information that is collected by public service bodies in “the day-to-day management or supervision of a scheme or service or revenue collection system”.⁶⁷ Administrative or public sector data includes personal data that has been provided as part of citizens interactions with public service bodies. A vast amount of administrative data is collected, maintained and updated on a frequent basis by the Irish public service.⁶⁸ A significant amount of resources are used in maintaining this data and ensuring it is accurate and up-to-date.⁶⁹

What is personal data?

The *Data Protection Acts* define ‘personal data’ as meaning:⁷⁰

“data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.”

The Bill proposes to define ‘personal data’ by reference to its definition in the GDPR:

‘personal data’ means 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

Source: [The GDPR, Article 4\(1\)](#) “Definitions” at p.L 119/33

Special categories of personal data

The *GDPR* defines “special categories of personal data” as meaning:⁷¹

Processing of 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 shall be prohibited

Source: [The GDPR, Article 9\(1\)](#) “Processing of special categories of personal data” at p.L 119/38

The Bill proposes to define “special categories of personal data” by reference to its definition in the *GDPR*.

⁶⁷ NES (1985), *Information for policy. Report no. 78* cited in MacFeely and Dunne (2014). *Joining up public service information: The rationale for a national data infrastructure* [online]. Administration, vol. 61, no.4 (2014), pp. 93-107, at p.95. Available here:

https://www.researchgate.net/publication/292986553_Joining_up_public_service_information_The_rationale_for_a_national_data_infrastructure

⁶⁸ *ibid*

⁶⁹ *ibid*

⁷⁰ Section 1, [Data Protection Act 1988](#), see also section 165 (“Reference to personal data in enactment”) of the [Data Protection Act 2018](#).

⁷¹ This definition is also used Part 1, Section 2(1) of the [Data Protection Act 2018](#).

What is data sharing?

For the purposes of the Bill, section 8 defines data-sharing “means the disclosure of information, including personal data, by a public body to another public body”.⁷² More broadly, data sharing involves the transfer of data between two or more parties.⁷³ It can be one or two way or it can involve multiple parties or it can be made publically available, i.e. open data.⁷⁴ Many different forms of data can be shared, for example metadata (information about data), aggregate data, survey or unit record data or administrative data.⁷⁵

What is the difference between data sharing and data matching?

Data sharing is not the same as data matching. Data matching is also known as ‘data linking’, ‘record matching’, ‘duplicate detection’ and ‘deduplication’.⁷⁶ Data matching involves bringing together data from two or more datasets thereby joining different data records on the same person or business.⁷⁷

Data matching can be carried out on data that has been shared where the level of detail allows it.⁷⁸ The Australian National Statistics Boards states that:

“[d]ata linking takes data sharing one step further. The legal and privacy issues for data linking go beyond those related to data sharing. In this guide, data sharing does not include data linking.”⁷⁹

Privacy and personal data

This section will examine potential issues regarding the protection of the right to privacy and protection of personal data.

Privacy

In its 2008 Public Management Review ‘[Ireland: Towards an integrated Public Service](#)’, the OECD noted that matters relating to privacy and security are a culturally sensitive issue in Ireland.⁸⁰ The OECD Review stated that (at p. 211):⁸¹

“[t]he sharing of individuals’ personal information, however, does raise privacy protection issues, and the potential trade-offs between increased efficiency and privacy protection, need to be carefully assessed. The cultural resistance in Ireland to population identity cards and concerns regarding the security of information that

⁷² Section 8(1), *Data Sharing and Governance Bill 2018*.

⁷³ National Statistics Service (Australia) (2009), *A Good practice guide to sharing your data with other* [online]. Available here:

<http://www.nss.gov.au/nss/home.nsf/NSS/E6C05AE57C80D737CA25761D002FD676?opendocument>

⁷⁴ *ibid.*

⁷⁵ *ibid.*

⁷⁶ *ibid.*

⁷⁷ *ibid.*

⁷⁸ *ibid.*

⁷⁹ *ibid.*

⁸⁰ OECD Public Management Review (2008), *Ireland: Towards an integrated Public Service* [online] at p. 211.

[Available here](#)

⁸¹ *ibid.*:199

would be held to facilitate the development of such shared services must be taken into account in both formulating future initiatives in the egovernment arena, and in communicating the benefits to the public.”

The issue of trust between the citizen and the State in the handling of their personal data was also raised by the former Data Protection Commissioner, Billy Hawkes, in the Data Protection Commissioner’s 2013 Annual Report. The then Data Protection Commissioner when discussing the handling of personal data in the public sector stated that (at pp. 4-5):⁸²

“[I]audable objectives such as fraud prevention and greater efficiency must meet a test of proportionality in the manner in which personal data is used. Failure to treat personal data with respect can only lessen the trust that should exist between the individual and the State. It will also lead inevitably to more formal enforcement action by my Office unless system-wide action is taken to improve current practice.”

MacFeely and Dunne (2014) in a paper analysing the need for a national data infrastructure, state that the necessary trade-off between increased efficiency and privacy protection does not appear to be well understood.⁸³

Personal data

This section will explore possible issues concerning protection of personal data in the context of the requirement under the *Data Protection Acts*.

Processing personal data

The *Data Protection Acts* define ‘processing’ of information or data, both manual⁸⁴ and automated data⁸⁵, as meaning:⁸⁶

“performing any operation or set of operations on the information or data, whether or not by automatic means, including—

- (a) obtaining, recording or keeping the information or data,
- (b) collecting, organising, storing, altering or adapting the information or data,
- (c) retrieving, consulting or using the information or data,
- (d) **disclosing the information or data by transmitting, disseminating or otherwise making it available**, or
- (e) aligning, combining, blocking, erasing or destroying the information or data.”⁸⁷

Emphasis added by the L&RS

As noted, the *Data Protection Acts* define disclosure, in relation to personal data, as including:

⁸² Data Protection Commissioner (2013), *Twenty-Fifth Annual Report of the Data Protection Commissioner 2013* [online] at pp. 4-5. Available here:

<https://www.dataprotection.ie/docimages/documents/Annual%20Report%202013.pdf>

⁸³ MacFeely and Dunne (2014). *Joining up public service information: The rationale for a national data infrastructure* [online]. Administration, vol. 61, no.4 (2014), pp. 93-107, at p.101.

⁸⁴ Manual data is “information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system” (section 1 of the [Data Protection Act 1988 \(as amended\)](#))

⁸⁵ Automated data is information that is “(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, or (b) is recorded with the intention that it should be processed by means of such equipment” (section 1 of the [Data Protection Act 1988 \(as amended\)](#))

⁸⁶ Section 1 of the [Data Protection Act 1988 \(as amended\)](#)

⁸⁷ *ibid.*

“the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed”.⁸⁸

Thus, the sharing of personal data between public service bodies or their agents falls under the definition of processing data under the *Data Protection Acts*. Accordingly, public sector bodies when sharing personal data must comply with the obligations in the *Data Protection Acts*.

Rules for processing personal data

Under the *Data Protection Acts* personal data may only be processed provided the data protection principles are complied with. The data processing principles are found in section 2 of the *Data Protection Act 1988 (As amended)*.⁸⁹ The Data Protection Commissioner summarises the data protection principles in terms of eight rules that data controllers must comply with. Table 3 summarises the eight data processing rules.

Table 3: Eight rules for processing personal data under the *Data Protection Acts*

No.	Rule	Summary
1.	Fair obtaining and processing	The fair obtaining and processing rule requires the data subjects, at the time of giving their personal information, are made aware of certain information including: <ul style="list-style-type: none"> • who is collecting the information; • what the information will be used for; • to whom the information will be disclosed.
2.	Specifying the purpose	The purposes specification rule requires that a data controller must have a specified explicit and legitimate purpose for collecting personal data.
3.	Use and further processing	The use and further processing rule requires that personal data may only be processed in a manner that is compatible with the purpose(s) for which it was collected.
4.	Security	The security rule requires that appropriate security measure must be taken against unauthorised access to or unauthorised alteration, disclosure or destruction of personal data, in particular where the process involves the transmission of data over a network, and against all other unlawful forms of processing personal data.
5.	Accuracy and up-to-date	The accuracy rule requires that personal data must be accurate, complete and where necessary up-to-date.
6.	Adequate, relevant and not excessive	The adequate, relevant and not excessive rule requires that personal data must be adequate, relevant and not excessive. It should enable data controllers to achieve the purpose(s) for collecting or processing the personal data and no more than that.
7.	Retention	The data retention rules requires that personal data shall not be maintained for longer than is necessary for achieving the purpose(s) for collecting or processing the personal data.
8.	Right of access	A data subject has a right to access their personal data held by an organisation or individual.

Source: <https://www.dataprotection.ie/docs/A-Guide-for-Data-Contollers/y/696.htm>

⁸⁸ *ibid.*

⁸⁹ See Section 2, *Data Protection Acts*, available here:

<http://revisedacts.lawreform.ie/eli/1988/act/25/revised/en/pdf?annotations=true>

Pre-legislative Scrutiny (PLS)

The Government approved the drafting of the General Scheme of the “Data-Sharing and Governance Bill” (‘General Scheme’) on 7 July 2015.⁹⁰

On 2 July 2016, the Minister for Public Expenditure and Reform, Paschal Donohue, TD, requested the Oireachtas Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach (‘Committee’) to consider the General Scheme in terms of pre-legislative scrutiny (‘PLS’). A Regulatory Impact Assessment (‘RIA’) for the Data Sharing and Governance Bill was sent to the Committee with the request for PLS.

As part of its scrutiny of the Draft Heads of the General Scheme, the Committee met in public session on 18 May 2017 and 23 May 2017.

The following stakeholders appeared before the Committee on 18 May 2017:

- Officials from the Department of Public Expenditure and Reform;
- Officials from the Department of Justice and Equality; and
- Representatives from the then Office of the Data Protection Commissioner (‘DPC’).

The following stakeholders appeared before the Committee on 23 May 2017:

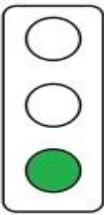
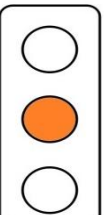
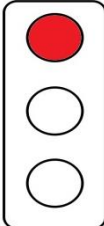
- Representatives from Digital Rights Ireland (‘DRI’); and
- Denis Kelleher, barrister-at-law.

In July 2017 the Joint Committee published its [report](#) on its pre-legislative scrutiny of the General Scheme. The report overall makes 30 recommendations under the following headings:

- Compliance with Data Protection Law
- Application of the proposed legislation
- Governance Framework
- Sanctions
- Transparency

As part of research work in preparation for Bill Digests, the Library & Research Service asks the relevant Department, in this case the Department of Public Expenditure and Reform, to indicate to what extent, if any, the Bill reflects the recommendations put forward by the Joint Committee. The following illustration acts as a key for categorising the responses received from the Department in relation to the main issues raised by the Committee in its report. The ‘traffic light system’ employed below is intended to highlight the impact the Committee’s PLS report had on the drafting and final content of the published Bill.

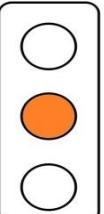
⁹⁰ Department of Public Expenditure and Reform, ‘Letter of Referral to the Oireachtas Joint Committee on Finance, Public Expenditure and Reform for Pre-legislative Scrutiny on the Data Sharing and Governance Bill’ (2/07/2016)

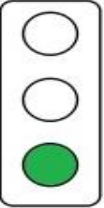
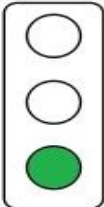
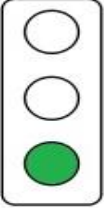
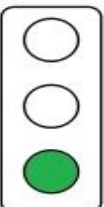
L&RS categorisation of the Department's response to the key issues identified by the Committee	'Traffic light dashboard' used in Table 3 to highlight the impact of the Committee's PLS report
Key issue has had an impact on the drafting of the Bill.	
The Bill may be described as adopting an approach consistent with the key issue or the impact of the key issue on the drafting of the Bill is unclear.	
Key issue has not had an impact on the drafting of the Bill.	

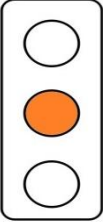
Source: L&RS

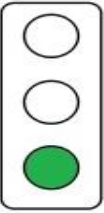
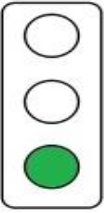
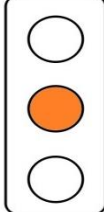
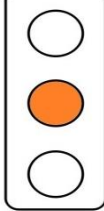
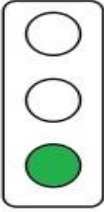
Table 4 below has been compiled by the Oireachtas Library & Research Service (L&RS) and sets out the L&RS' summary of each of the key issues identified by the Committee (in relation to the General Scheme of the Bill). The Department's responses to these issues have been summarised and categorised by the L&RS in accordance with the traffic light system set out below.

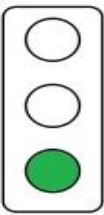
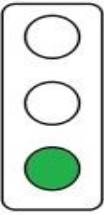
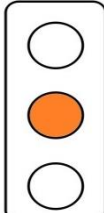
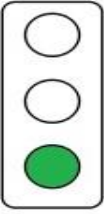
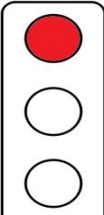
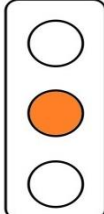
Table 4: The impact of pre-legislative scrutiny (PLS) – Department's response to the Joint Committee's recommendations

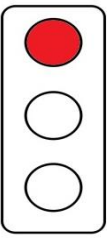
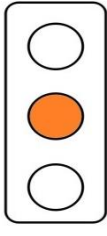
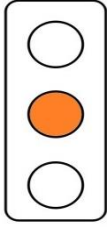
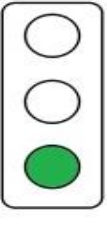
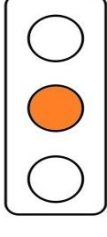
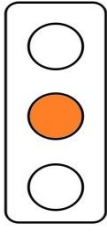
No.	Recommendation as per Joint Committee Report	Response from DPER on whether addressed (either in whole or in part) in the Bill
1	Principles-based legislation To ensure harmony with EU and national data protection law which is principles-based, it is recommended that the proposed legislation reflects the theme and ethos of that principles-based legislation and that its provisions will ensure that those principles are applied in practice.	 <p>"The Bill follows the key principles of data protection as enunciated in the GDPR and it would not be appropriate to repeat them in this legislation. The governance provisions set out in the Bill will ensure that these principles are applied by public bodies in practice."</p>

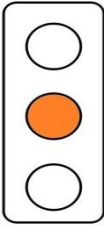
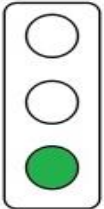
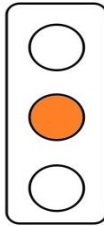
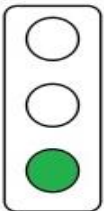
No.	Recommendation as per Joint Committee Report		Response from DPER on whether addressed (either in whole or in part) in the Bill
2	<p>Compliance with the protection law</p> <p>In view of the recent developments in data protection law at the EU and national level, it is recommended that (i) the underlying assumptions underpinning the General Scheme and (ii) the full text of the General Scheme be reviewed and revised, as necessary, to reflect the content and principles set out in the GDPR and other data protection legislation, e.g. the forthcoming Data Protection Bill and the <i>Data Protection Acts</i>, and also the <i>Barra Judgement</i>, to ensure it complies with the changed data protection landscape.</p>		<p>“A comprehensive review of the scheme of the Bill was conducted during the drafting process to ensure that the provisions of the Bill were fully aligned with the GDPR and the <i>Barra judgement</i>. Section 5 of the Bill states explicitly that the Bill shall not affect the operation of data protection law.”</p>
3	<p>Continued consultation with the Office of the Data Protection Commissioner and the Department of Justice and Equality</p> <p>In view of the evidence of the DPC regarding the necessity for further enhancements and amendments to the General Scheme to ensure consistency with the forthcoming Data Protection Bill, it is recommended that the Department should continue its engagement with the DPC and with the Department of Justice and Equality in relation to these issues, to ensure the proposed legislation achieves its objectives in a manner that is consistent and compliant with the Data Protection Bill and the GDPR.</p>		<p>“The Department engaged with both the Department of Justice and the DPC, as appropriate, throughout the drafting of the Bill, as well as with other key Departments and Offices, including the Departments of Education and Skills; Health; and Employment Affairs and Social Protection; and the Revenue Commissioners.”</p>
4	<p>Full regard should be had to the Data Protection Commissioner guidance</p> <p>It is recommended that full regard is had to the DPC’s guidance on ‘Data Sharing in the Public Sector’ as drafting of the proposed legislation progresses. This will help to ensure that any data sharing carried out under the proposed legislation is lawful</p>		<p>“The DPC’s guidance on data sharing was taken into consideration in the drafting of the Bill.”</p>
5	<p>Revisions to the proposed legislation</p> <p>The Department is considering a number of additional measures to enhance the governance, oversight and transparency provisions in the legislation. To date these revisions have not been circulated or published. Such revisions must be compliant with data protection law and requirements and ensure that the personal data of citizens are adequately safeguarded. The Committee considers that there is merit in the Department publishing these revisions.</p>		<p>“Additional Heads to enhance the governance, oversight and transparency provisions of the Bill were agreed by Government in December 2017. The key provisions in the Bill to enhance governance, oversight and transparency are:</p> <p>Part 8 – An enabling provision for the development of a to facilitate the creation of a portal to make it easier for members of the public to exercise their access rights under the GDPR to see what information public bodies hold about them and the purposes for which the information is collected and processed.</p> <p>Part 9, Chapter 1 – Provides for the Minister to appoint a Data Governance Board (“the Board”) to</p>

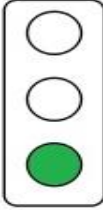
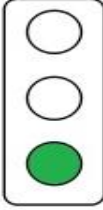
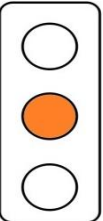
No.	Recommendation as per Joint Committee Report	Response from DPER on whether addressed (either in whole or in part) in the Bill	
			<p>advise on the operation of this Bill. The Board's functions will include:</p> <ul style="list-style-type: none"> • advising the Minister on the making of and monitoring compliance with data management rules, procedures, standards and guidelines; • advising the Minister on the designation of base registries; and • a governance role for the Board in terms of scrutinising draft Data Sharing Agreements. <p>Part 9, Chapter 2 – Sets out the process for enhancing transparency regarding data sharing and for advance scrutiny of any proposals for data sharing between public bodies as follows:</p> <ul style="list-style-type: none"> • Public bodies will be required to publish an advance draft of any proposed data-sharing agreement and invite the public to comment on the proposal; • The draft data-sharing agreement, along with a summary data protection impact assessment (if carried out) and any comments received during the consultation will then be submitted to the Board for consideration; • The Board may issue a set of recommendations in respect of the draft data-sharing agreement, which the public bodies shall incorporate into the final agreement before signing. • The signed data-sharing agreement shall be submitted to the Minister and laid before the Oireachtas. • The Minister shall publish the signed data-sharing agreement along with the summary data impact assessment and any recommendations made by the Board. <p>Part 9, Chapter 3 – Gives the Minister the power to:</p> <ul style="list-style-type: none"> • prescribe binding rules, procedures and standards for the management of data across the public service; • issue guidelines for management of data across the public service; and • prepare model data-sharing agreements that public bodies shall use as the basis for any data sharing agreements they enter into."
6	<p>Guidelines for determining the legal basis for data sharing</p> <p>It is recommended that consideration be given to including an obligation that guidelines be drawn up and published, either standalone ones or as part of the Ministerial Code and Guidelines provided for under Head 4, setting out how assessments should be carried out when determining the legitimate basis for sharing data and the safeguards that should apply.</p>		<p>"The DPC has issued guidelines for public bodies to assist them in the implementation of the GDPR. These are available at: http://gdprandyou.ie/. Section 65 of the Bill provides that the Minister may issue guidelines to assist public bodies in the performance of their functions under this Bill or other enactments relating to data-sharing."</p>

No.	Recommendation as per Joint Committee Report		Response from DPER on whether addressed (either in whole or in part) in the Bill
7	Secondary legislation to underpin Data Sharing Agreements In view of the divergent expert opinion heard in evidence regarding the adequacy of the General Scheme as a legal basis for data sharing in the Public Service and the benefit of, or requirement for secondary legislation to underpin proposed 'Data Sharing Agreements' in particular, it is recommended that this issue be subject to further detailed consideration and clarification by the Department.		<p>"The Department has engaged bilaterally on this issue with the DPC, who accepted the advice the Department had received from the Office of the Attorney General that secondary legislation was not required.</p> <p>An explicit legal basis for public bodies to share data is provided under section 12 of the Bill in line with the principles of the GDPR."</p>
8	Data sharing in accordance with data protection law It is recommended that Head 4 of the General Scheme concerning the 'Regulation of Data-Sharing between Public Service Bodies and Applicable Safeguards and Conditions' be reviewed and revised, as necessary, to ensure that all data sharing is done in accordance with data protection legislation.		<p>"Section 5 of the Bill states explicitly that the Bill shall not affect the operation of data protection law. Accordingly, any sharing arrangements entered into under this legislation must comply fully with data protection law."</p>
9	Application to public service bodies It is recommended that clarity be provided on which public service bodies will fall under the scope of the proposed legislation and those public bodies which are proposed to be exempt.		<p>"Section 9 of the Bill defines which public bodies will fall under its scope. The intention is that the legislation should cover as wide a number of public bodies as possible, with the exception of the commercial state enterprises. A full list of the bodies excluded from the Bill is in the Schedule. In addition, sections 9(2) and 9(4) provide that the Minister may add or remove bodies as required."</p>
10	Clarity as to the scope of the legislation It is recommended that consideration be given to including in the proposed legislation provisions to clarify the scope of the legislation and the data sharing arrangements it will apply to.		<p>"Large scale structural processing and the processing of special categories of sensitive data are not covered by this legislation.</p> <p>The purposes and conditions under which data may be shared is provided for at section 12 of the Bill. "</p>
11	Distinguishing between criminal and non-criminal related data From May 2018 three separate regimes will apply to the processing of personal data. It is recommended that consideration be given in the proposed legislation to distinguishing between data processing for the purpose of prevention, detection, investigation and prosecution of crime (criminal related data) and more general purposes (non-criminal related data).		<p>"Section 11 of the Bill sets out the purposes that are excluded from the scope of the Bill. These exclusions include purposes relating to law enforcement, security and defence."</p>

12	Governance controls It is recommended that the proposed legislation provides the necessary governance controls to ensure that personal data will be shared in compliance with data protection law, including the forthcoming GDPR and the Data Protection Bill. This will help to ensure compliance with data protection law and the safeguarding of citizens personal data.		“Please see response to recommendation 5 for information regarding the governance controls provided for in the Bill.”
13	Advanced publication of, and consultation on, Data Sharing Agreements It is recommended that the proposed legislation provide for the advance publication of, and consultation on, draft Data Sharing Agreements and any Data Sharing Agreements that are being reviewed.		“This is provided for at section 55 of the Bill.”
14	Review of existing Data Sharing Agreements It is recommended that consideration be given to providing a transitional provision in the proposed legislation requiring the review, and where necessary updating, of existing Data Sharing Agreements between public bodies facilitating data sharing under other legislation.		“Data-sharing arrangements that are legislated for via other enactments are not subject to the requirement for creating a data-sharing agreement as set out within this Bill. These arrangements are, however, subject to section 71 of the Bill on the provision of information on data-sharing. It is a matter for individual public bodies to review their existing data-sharing arrangements to ensure they are in compliance with the GDPR.”
15	Periodic review of Data Sharing Agreements It is recommended that the proposed legislation provide for the periodic review, and where necessary updating, of all Data Sharing Agreements.		“This is provided for at section 19 of the Bill.”
16	Ministerial Code and Guidelines In Head 4(3) of the General Scheme, it is recommended to substitute “shall” for “may” thereby placing a positive obligation on the Minister to draw up and publish a Code of Practice (‘Code’) and Guidelines.		“The Minister is committed to issuing standards, codes and model agreements in accordance with the provisions on the Bill.”
17	Consultation when preparing the Ministerial Code and Guidelines It is recommended that the proposed legislation would provide an obligation on the Minister to consult with stakeholders, in particular the Data Protection Commissioner and/or the proposed Data Governance Board (if approved by Government) when preparing the Code and Guidelines to ensure that the rights of individuals are protected.		“Section 46 provides, <i>inter alia</i> , that the Data Governance Board shall: <ul style="list-style-type: none"> advise the Minister in relation to the prescribing of rules, procedures and standards under section 64; and advise the Minister in relation to the preparation of guidelines under section 65.”

18	Advanced publication of, and consultation on, draft Ministerial Code and Guidelines It is recommended that consideration be given to the advance publication of, and public consultation on, draft Ministerial Code and Guidelines.		“Sections 65 and 66 provide that the Minister may consult with such, if any, Ministers as the Minister considers appropriate in preparing guidelines and model data-sharing agreements.”
19	Standardised and scalable infrastructure It is recommended that, in implementing the proposed legislation, there is a “standardised and scalable” ICT infrastructure with a set of rules that allow public bodies to connect to, once they have adopted those rules. This will help to minimise cost over-runs in the implementation of any e-infrastructure created as a result of the proposed legislation.		“The implementation of ICT infrastructures within the Public Service are guided by the Public Service ICT Strategy, including the Build to Share, and Data as an Enabler pillars therein. Any ICT infrastructure supports developed as part of the implementation of the legislation will take into account this recommendation in line with the aforementioned strategy.”
20	Data protection implementation principles It is recommended that in the implementation of any shared State-citizen e-infrastructure, consideration should be given to the feasibility of incorporating ‘data protection implementation principles’ validated by the DPC to ensure compliance with data protection law and the safeguarding of citizens’ personal data.		“This recommendation will be considered during the implementation of any resultant systems from the Bill via the introduction of data management standards and guidelines provided for in sections 64 and 65.”
21	Data protection implementation principles - Identity and opt-in It is recommended that the e-infrastructure underpinning the proposed legislation be implemented in a manner that complies with data protection law and that existing and new identity mechanisms also comply in this regard.		“All systems implemented to underpin the Bill will be implemented in a manner that complies with data protection law.”
22	Data protection implementation principles – Data access, not sharing In view of the evidence heard that the focus of the proposed legislation should be on data access and not data sharing, it is recommended that consideration should be given to exploring this alternative option in the context of revisions to the General Scheme.		“Part 7 of the Bill is designed to focus on the introduction of authoritative data sets that oblige data access over the storage of independent copies of data. The introduction of base registries will reduce the amount of data held by public bodies, where data access is used to satisfy service delivery needs.”
23	Data protection implementation principles - Authentication and access It is recommended that consideration be given to including in the proposed legislation the requirement for rigorous authorisation and authentication of every person in the public service with access to data. This will restrict access to those who are legally authorised to access personal data and help to ensure compliance with data protection law.		“It is envisaged that this recommendation will be addressed via the introduction of data management standards and guidelines provided for in sections 64 and 65.”

24	Data protection implementation principles - Data access logging It is recommended that consideration be given to including in the proposed legislation the requirement to automatically log access to data. This will enable audits to be carried out on who, why and when personal data was accessed and enable citizens to track who, why and when their personal data was accessed.		<p>“It is envisaged that this recommendation will be addressed via the introduction of data management standards and guidelines provided for in sections 64 and 65.”</p>
25	Data protection implementation principles - Secure online portal for individuals In view of the evidence heard highlighting the importance of a secure online portal for individuals, it is recommended that consideration be given to creating a secure online portal for citizens. This will help to ensure the citizens’ right to data access as required under the GDPR. It will also allow citizens to track State services provided to them and access details of use of, and access to, their data. Such consideration should take into account significant issues that may arise with such a portal, such as security and costs issues.		<p>“This is provided for in Part 8 of the Bill.”</p>
26	Improvement, standardisation and professionalisation of data governance functions It is recommended that the legislation provide for the improvement, standardisation and professionalisation of data governance functions and data protection officer functions in public bodies. In addition that clear and common data definitions are developed to ensure interoperability between public bodies when data sharing.		<p>“It is envisaged that this recommendation will be addressed via the introduction of data management standards and guidelines provided for in sections 64 and 65. Furthermore, Part 7, provides for the standardisation of key data types within the Public Service.”</p>
27	Sanctions It is recommended that consideration be given to creating an offence for illegally/wrongfully accessing personal data that has been processed by the State.		<p>“The Data Protection Act 2018 provides for offences for illegal/wrongful accessing of personal data as follows:</p> <ul style="list-style-type: none"> • Section 144: Unauthorised disclosure by a processor • Section 145: Disclosure of personal data obtained without authority • Section 146: Offences by directors of bodies corporate <p>Since these provisions apply to the public sector, it is not necessary for this Bill to duplicate these provisions.”</p>

28	Publication of Data Sharing Agreements It is recommended that the proposed legislation provide for the publication of Data Sharing Agreements (in their entirety as distinct to a list of Data Sharing Agreements). This will enable citizens to view the content of such Data Sharing Agreements, including the purpose for the collection and processing of personal data.		“This is provided for in section 60 of the Bill.”
29	Publication Screening Assessments and Privacy Impact Assessments It is recommended that consideration be given to including in the proposed legislation a provision requiring the publication of any screening assessments or Privacy Impact Assessments that have been carried out.		“This is provided for in sections 55 and 60 of the Bill.”
30	Exception under Head 8(6)(a) to the publication of certain Data Sharing Agreements or Privacy Impact Assessments It is recommended that consideration be given to qualifying the exception in Head 8(6)(a) that Data Sharing Agreements or Privacy Impact Assessments relating to certain justice or criminal matters be published. The Committee is of the opinion that there is merit in publishing the existence of such Data Sharing Agreements or Privacy Impact Assessment and any parts that do not contain sensitive information.		“Since section 11 excludes matters relating to law enforcement, security and defence from the scope of the Bill, the qualifying exception that was provided at Head 8(6) of the draft general scheme is not required and therefore has not been included in the Bill.”

Source: L&RS, based on PLS Report of the Joint Committee and communication from the Department to the L&RS on 12 June 2018.

Principal provisions

The *Data Sharing and Governance Bill 2018* consists of 72 sections divided over ten parts. Given the short time between publication of the Bill (12 June 2018) and its Second Stage debate (19 June 2018), this section of the Digest will focus on the following core themes identified in the Bill:

- Application of the Act;
- Regulation of Data-sharing;
- Data-sharing agreements;
- Base registries;
- Personal data access portal;
- Data governance.

It will not look at the provisions on Public Service information (Part 5) and Business Information (Part 6) however a brief description of all sections in the Bill is set out in Table 1 in the Summary Section at the start of this Digest.

Application of the Act (Part 2: sections 5-11)

Interaction with the Data Protection Acts and GDPR

Section 5 of the Bill provides for the relationship between the proposed Act and existing data protection laws. Subsections (2) and (3) provide that [section 38](#) of the *Data Protection Act 2018* (Processing for a task carried out in the public interest or in the exercise of official authority) and any regulations made thereunder will not apply to the disclosure of information by one public body to another. The effect is that such disclosures will not be deemed lawful simply because they are made in the performance of a public body's statutory functions: disclosures must meet the requirements set down in the proposed Act.

Interaction with the Social Welfare Consolidation Act 2005

Section 6 provides, among other things, for the sharing of “public service identity” information between specified bodies (as defined in the [Social Welfare Consolidation Act 2005](#)) provided that disclosure is made in accordance with the provisions of the proposed Act. However disclosure of public service identity information is not permitted for the purpose of facilitating “an analysis of the structure, functions, resources or service delivery methods” of public service bodies.

Public service identity information includes information such as a person's name, date of birth and Personal Public Service Number (PPSN).

Interaction with other enactments

Section 7 provides (subject to limited exceptions) that the proposed Act will not affect the sharing of information provided for under a number of specified Acts. This includes the sharing of information gathered for statistical purposes under the [Statistics Act 1993](#).

Data-sharing: meaning

Section 8 of the Bill defines “data-sharing” for the purposes of the proposed Act as **the disclosure of information, including personal data, by one public body to another**.

Where a change or addition to the information held on the information system of one public body results automatically from a change or addition to the information system of another public body it is deemed to be a disclosure and thus data-sharing under the proposed Act.

Section 10 provides that the proposed Act will apply to information concerning **deceased persons** as well as living persons.

The Bill specifically **excludes data sharing for the following purposes** from the provisions of the proposed Act:

- criminal investigation, prosecutions or detention;
- the functions of the Criminal Assets Bureau;
- State defence, security and intelligence activities, and
- international relations of the State.

Public body: meaning

Section 9 defines a public body for the purposes of the proposed Act as follows:

- (a) a Minister of the Government,
- (b) the Attorney General,
- (c) the Comptroller and Auditor General,
- (d) the Revenue Commissioners,
- (e) the Commissioners of Public Works in Ireland,
- (f) the Commissioner of Valuation,
- (g) the Garda Síochána,
- (h) the Defence Forces,
- (i) a local authority for the purposes of the *Local Government Act 2001*,
- (j) the Health Service Executive,
- (k) an education and training board,
- (l) a school, and the board of a school under the auspices of an education and training board
- (m) corporate bodies (other than those exempted) established under legislation. Also included are companies financed wholly or partly by public funds, where a public service pensions scheme exists or applies or may be made;
- (n) bodies (other than those exempted) that are wholly or partly funded by public funds (either directly or indirectly) where a public service pensions scheme exists or applies or may be made;

- (o) a subsidiary or company controlled by any of the bodies listed at i), j) k) m) or n) above where a public service pensions scheme exists or applies or may be made;
- (p) any other body specified by the Minister.

Section 9(2) of the Bill provides that the Minister (i.e. the Minister for Public Expenditure and Reform) may exempt a body from the definition of a public body. Before doing so the Minister must have regard to whether the body is engaged for gain in the production, supply or distribution of goods or the provision of a service and whether the sharing of data with that body could lead to commercial advantage and a distortion of competition.

Conversely, section 9(4) provides that the Minister may designate a body as a public body following consultation with any other Minister as appropriate. The Minister may do this where:

- a body is financed wholly or partly, either directly or indirectly by public funds; and
- the Minister is satisfied that the body's principal activity is the delivery of a public service on behalf of a public body.

The Schedule to the Bill lists those bodies to which the Bill's definition of "public body" does not apply. These include:

- any body corporate established by Act of Parliament before 6 December 1922 that upon its establishment, was of a commercial character;
- An Post;
- Central Bank of Ireland;
- CIE;
- The Irish National Stud Designated Activity Company;
- Electricity Supply Board;
- Ervia;
- Horse Racing Ireland;
- Irish Aviation Authority;
- Raidió Teilifís Éireann;;
- Shannon Foynes Port Company;
- Voluntary Health Insurance Board and
- A subsidiary of a body named in the Schedule, including a subsidiary of such a subsidiary.

Regulation of data-sharing (Part 3: sections 12 and 13)

Data-sharing: requirements

Section 12 provides for the disclosure of personal data (other than special categories of personal data⁹¹) by one public body to another public body in circumstances where no other legislation (either domestic or EU) permits or requires such disclosure.

⁹¹ Special categories of personal data are defined by reference to the GDPR. They include information about characteristics such as a person's genetic properties, health, ethnicity, political opinions or sexuality.

A disclosure of personal data under section 12 can only be made to facilitate the performance of a function by one or other of the public bodies concerned for one or more of following purposes:

- to verify the identity of a person where a public body is providing or proposes providing a service to that person;
- to identify and correct erroneous information held by a public body;
- to support the “once only” principle that persons should not have to provide or public bodies collect the same information multiple times;
- to establish the entitlement of a person to the provision of a public service;
- to facilitate the administration, supervision and control of a service, programme or policy;
- to facilitate the improvement or targeting of a service, programme or policy;
- to enable the evaluation, oversight or review of a service, programme or policy; or,
- to facilitate an organisational study of a public body.

Disclosure of personal data under section 12 must be made in accordance with a data-sharing agreement (see Part 4), and any data disclosed must have been lawfully obtained and stored. Section 12 also provides that public bodies that are party to a data sharing agreement must comply with any rules, procedures, standards and guidelines that may be prescribed under Part 9 (Data Governance).

Directions

Section 13 of the Bill gives the Minister power to direct a public body to disclose information, including personal data (other than special categories of personal data), to another public body. Before issuing a direction the Minister must have regard to a number of factors (listed in subsection 9). These include whether the disclosure would assist a public body in carrying out one or more of its functions:

- by reducing the duplication of tasks carried out;
- increasing the efficiency of a public body; or
- facilitating an improvement in the quality of services being offered.

A public body must comply with any direction issued by the Minister. However, the Minister may not direct the disclosure of information if the disclosure is prohibited by law (either domestic or EU) or if compliance would cause the public body to breach of any law. Before issuing a direction the Minister must consult with the public body concerned and any other Ministers considered appropriate.

Data-sharing agreements (Part 4: sections 14-21)

Part 4 of the Bill provides a legislative basis for the sharing of personal data (other than special categories of personal data) between public bodies where no other law (either

domestic or EU) permits or requires them to share such data. Public bodies proposing to share information on this basis must enter into a data-sharing agreement.

It is worth noting that section 14(2) excludes disclosures of personal data made under Part 5 of the Bill (which relates to disclosure of information concerning public service pensions) from the requirement to enter of data-sharing agreements.

Disclosure of special categories of personal data (such as information about a person's health, political opinions or sexuality), are specifically excluded from the application of Part 4 of the Bill. It is notable however that section 23 of the Bill provides for disclosure of special categories of personal data under Part 5 (Public Service Information) where such information is processed for the administration or valuation of a public service pension scheme.

Obligation to enter into data-sharing agreements

Section 15 of the Bill provides that public bodies intending to disclose personal data on the basis of Part 4 must enter into data-sharing agreements before doing so. Section 16 requires data-sharing agreements be in writing.

Accession to data-sharing agreement

Section 17 provides that a public body who was not a party to the original data-sharing agreement may accede to that data-sharing agreement with the agreement of the other parties. An accession agreement must be executed by the lead agency (specified in the original data sharing agreement) on behalf of all the other public body parties to the original agreement. The lead agency must notify the Data Governance Board (to be established under section 45 of the Bill) prior to executing an accession agreement.

Content of data-sharing agreement

Section 18 specifies the minimum content of a data-sharing agreement. This includes:

- the parties to the agreement;
- the information to be disclosed;
- the purpose and legal basis for the data sharing;
- how the information is to be processed;
- any applicable security measures; and
- provisions concerning the retention and deletion of the information disclosed.

Section 18(2) gives the Minister power to prescribe additional information that must be included in a data-sharing agreement where satisfied that the inclusion would:

- be consistent with the data processing principles set out in Article 5(1) of GDPR (see Textbox 1 above); and

- improve transparency regarding the sharing of information by public bodies or facilitate good governance in the sharing of information by public bodies.

Review of operation of data-sharing agreement

Section 19 requires the parties to a data-sharing agreement to review its terms and operation at intervals of no more than 5 years. Section 19(2) provides that any review must consider the technical, policy and legislative changes that have occurred since the date of the previous review or the agreements commencement date.

Lead agency

Section 20 of the Bill requires every data-sharing agreement to specify a party as the lead agency. The lead agency is responsible for carrying out functions specified in section 20 and elsewhere in the Bill. These functions include:

- keeping the identities of the parties to the agreement up to date;
- publishing details of reviews of the agreement, and
- receiving data access requests concerning information disclosed under the agreement and (where appropriate) forwarding them to the relevant data controller.

Cessation

Section 21 of the Bill provides that a lead agency must notify the Minister of the expiry or termination of a data-sharing agreement. Once notified the Minister must publish on a website maintained by him or her a notice of the cessation. The Minister must ensure that it is clear to any person accessing information on the website that the agreement has expired.

Base registries (Part 7: sections 36-42)

Section 2 of the Bill defines certain terms used throughout the Bill. In particular, base registry means a database which is designated as such by Ministerial order under section 37 and base registry owner means a public body specified as such in respect of a base registry in an order made under section 37(1).

Section 36 provides that Part 7 will not apply to special categories of personal data (such as data concerning a person's health, political opinions or sexuality), or to databases containing such data.

Designation of base registry

Section 37 provides that the Minister (with the consent of other Ministers as appropriate) may designate as a base registry any database of which the copyright is owned by a public body.

An order under section 37 must specify, among other things:

- the name of the base registry;
- the public body that is to be the base registry owner;

- the purpose for which the information in the base registry may be processed by a public body accessing it;
- the information to be contained in the base registry; and
- the name and associated description of each field in the database.

The Minister may only make an order designating a database as a base registry where he or she is satisfied that it is necessary for the purposes of:

- ensuring the consistency and accuracy of information frequently used by public bodies in the performance of their functions;
- avoiding administrative burdens on public bodies and persons if the information was to be collected directly; and
- avoiding the duplication of databases held by public bodies.

The Minister must also have regard to whether such a designation would, among other things:

- reduce duplication of tasks carried out by public bodies;
- increase the efficiency of public bodies in carrying out their functions;
- improve the quality of services provided by public bodies;
- assist in the verification of persons receiving a service from a public body;
- reduce the need for a person to provide the same information to different public bodies; and
- assist a public body in establishing the identity of a person receiving to service being delivered by a public body.

Base registry owner

Section 38 of the Bill provides that the base registry owner must ensure that the information in the registry is accurate, up to date, complete and accessible to authorised users. The base registry owner must also put in place measures to control and monitor access to the registry. If the base registry contains personal data, the base registry owner must be the lead agency specified in the data-sharing agreement relating to the disclosure of such information to public bodies.

Section 41 authorises a base registry owner, for the purpose of ensuring that information is accurate, up to date and complete, to modify information in a base registry and to access relevant information held by other public bodies relating to the base registry.

Processing of information

Section 39 provides that a base registry owner will have the power to process information in order to comply with its obligations under section 38, even if no other domestic or EU law authorises such processing.

Terms of service

Section 40 provides that a base registry owner must prepare terms of service for access by other public bodies to the base registry. These must be published by the Minister on a

website controlled by the Minister. The base registry owner and any public bodies accessing a base registry must comply with the terms of service relating to that base registry.

Obligation to use base registry

Section 42 will oblige public bodies to use base registries (rather than other sources) where the information in such registries meets the qualitative requirements of the public body in respect of the purpose for which it intends to use the information. Public bodies that access information in a base registry or that provide information to one must put in place the necessary administrative and technical measures required to do so.

A base registry owner may appoint a public body to collect information on its behalf to ensure compliance with its obligations to keep the registry accurate, up to date, and complete.

Personal data access portal (Part 8: sections 43 and 44)

Section 43 of the Bill provides that Part 8 will apply to personal data **including** special categories of personal data.

Establishment of personal data access portal

Section 44 provides that the Minister **may**, with the approval of the Government, develop an information system to allow data subjects to exercise their rights under the GDPR. The rights expressly mentioned include viewing personal data held by a public body, and exercising rights set out in:

- Article 15 (right of access),
- Article 16 (rights of rectification)
- Article 17 (right to be forgotten)
- Article 18 (right to restrict processing),
- Article 20 (right to data portability)
- Article 21 (right to object to processing)

The information system, if developed, must incorporate a website to be known as the “Personal Data Access Portal”. This portal may include facilities by which a data subject can exercise his or her rights as set out above.

It is worth noting that the Bill does not specifically provide for instances where there has been a breach of a data-sharing agreement. However, section 5 provides that the proposed Act will not affect the provisions of data protection law, defined in the Bill are:

- the Data Protections Acts 1988 to 2018;
- the General Data Protection Regulation;
- all law of the State giving further effect to the General Data Protection Regulation; and,
- all law of the State giving affect or further effect to the Directive 2016/680.

Data governance (Part 9: sections 45-46 and 53-67)

Data Governance Board

Part 9 of the Bill provides for the establishment of a Data Governance Board. Its details, among other things, membership and the functions of the Board, some of which are examined in more detail below.

Appointment of Board

Section 45 of the Bill provides that the Minister must appoint a Data Governance Board which is to be independent in the performance of its functions.

Functions of Board

Section 46 of the Bill describes the general functions and purposes of the Board. These include:

- advising the Minister in relation to the prescribing of rules, procedures and standards;
- advising the Minister in relation to the preparation of guidelines;
- promoting compliance by public bodies with the guidelines;
- advising the Minister in relation to monitoring of compliance with rules, procedures and standards prescribed under section 64 and guidelines under section 65; and,
- reviewing data-sharing agreements.

Section 46(4) obliges the Minister to provide the administrative and support services necessary for the Board to perform its functions.

Reporting

Section 52 of the Bill provides that the Board must prepare an annual report for the Minister not later than the 30 June each year. A copy of the report must be laid before the Houses and made available on a publicly accessible website.

Review of data-sharing agreements

As mentioned above one of the functions of the Data Governance Board will be to review data-sharing agreements. Chapter 2 of Part 9 (sections 53-62) of the Bill sets out in detail how the review process will operate, including what will be excluded from the review, the public consultation process, and the factors that the Data Governance Board must take into account when carrying out a review.

Exclusions

Section 54 excludes from the Board's review less significant changes to data-sharing agreements, such as accession of a public body to an existing agreement or a change of lead agency.

Public consultation

Section 55 requires public bodies to undertake a public consultation before entering into a data-sharing agreement. Section 55(1) requires each of the parties to a proposed data-sharing agreement to publish on a public facing website the following:

- a copy of the proposed agreement;
- a summary of the data protection impact assessment, if completed;
- a statement from the data protection officer of each of the parties that he or she has reviewed the proposed agreement and that compliance with the agreement by the parties will not contravene the data protection law; and,
- a notice inviting submissions, in a period specified by the Board, in relation to the proposed agreement to the lead agency.

Section 55(4) provides that the parties to the proposed agreement must consider any submissions made and may, where they consider it appropriate, amend the proposed agreement to reflect the submissions.

Review of data-sharing agreement

Section 56 of the Bill requires a lead agency to submit for review by the Board the proposed data-sharing agreement and related documentation within a specified time-frame. The related documentation must include statements from the parties' data protection officers that each of them is satisfied that compliance with the proposed agreement will not result in a breach in data protection laws. The Board may seek additional information which the lead agency must provide.

Section 57 of the Bill provides that Board must review the submitted documentation having regard to the following criteria:

- compliance of the agreement with the proposed Act;
- compliance with any model data-sharing agreement produced by the Minister under section 66;
- compatibility with data protection law;
- security measures applicable to the transmission, storage and accessing of personal data;
- where a data protection impact assessment has been carried out a summary of the matters set out in Article 35(7) of GDPR⁹²;
- submissions made in response to the public consultation, and
- whether the agreement is in the public interest.

The parties to the agreement must take account of any recommendations made by the Board and amend the data-sharing agreement accordingly. Section 58 provides that where the

⁹² These include an assessment of the necessity and proportionality of the data processing and an assessment of the risks to the rights and freedoms of data subjects. The text of the GDPR is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Board recommends changes dealing with 'substantial issues', the proposed data-sharing agreement must be amended and re-submitted for review.

The Board may consult with relevant Government Ministers and other relevant persons when carrying out a review. Section 62 provides that the Board may set the time-frame for public consultations and for the submission of documents to it.

Execution and publication of agreement

Section 59 of the Bill provides that where the Board makes no recommendations or the proposed agreement has been amended to reflect any recommendations made the parties may execute the agreement.

Section 60 provides for the publication of data-sharing agreements. The lead agency must forward a copy of the agreement to the Minister within 10 days of execution and must notify the Minister of any accession or withdrawal from the agreement, again within 10 days.

Section 60 also provides that these documents must be sent to the Board, laid before the Houses of the Oireachtas and published on a website maintained by the Minister. The Board must also publish the signed data-sharing agreement as well as related documents on its website.

Section 61 of the Bill provides that a date of a data-sharing agreement comes into effect on the date on which it is published on the website of the lead agency.

Governance

Section 63 of the Bill provides that the governance provisions set out in Chapter 3 of Part 9 and examined below will apply to personal data - **including special categories of personal data** as well as information that is not personal data.

Rules and Guidelines

Section 64 of the Bill provides that the Minister **may** prescribe rules, procedures and standards for the processing and management of data by public bodies. These relate to:

- the operation and use of base registries including the accessing of personal data by persons in or acting on behalf of public bodies;
- the recording of information relating to the accessing of personal data;
- the management of information for re-use by persons other than public bodies; and
- the conduct of data protection impact assessments.

Section 65 provides that the Minister **may** (after consultation with other Ministers as appropriate) prepare and issue guidelines to public bodies concerning their functions under the proposed Act and other legislation concerning data-sharing. Section 65 also requires

public bodies to have regard to the guidelines issued under this section and also the provisions of Acts relating to data-sharing.

Section 67 requires the Minister to publish any rules, procedures and standards prescribed under section 64 and any guidelines issued under section 65.

Model agreements

Section 66 of the Bill provides that the Minister **may** (after consultation with other Ministers as appropriate) prepare or revise model agreements concerning data-sharing for the purpose of the proposed Act or other relevant legislation. The Minister may request advice from the Board in relation to the preparation or revision of model data-sharing agreements. Where a model agreement has been prepared, public bodies **must** use it as the basis for any data-sharing agreement they enter into.

Compliance reports

Section 68 of the Bill provides that the Board **may** request a public body to issue a report on that body's compliance with the proposed Act and any orders or regulations made under it. A compliance report under this section is a statement signed by the public body's accounting officer (or in the absence of an accounting officer, the chief executive officer or person holding such a position within the public body).

Costs and implications

The Explanatory Memorandum for the Bill outlines a number of financial implications associated with the Bill. It states that “[a] certain level of direct cost can be expected to arise for the Exchequer for the establishment of the base registries, which has yet to be quantified”.⁹³

Such costs, it goes on to state, can be expected in respect of “incremental staffing and other administrative costs” from the Bill’s requirements to put in place data sharing agreements and undertake privacy impact assessments between public bodies. The Explanatory Memorandum states that “[t]hese costs will be met from within existing agree Ministerial expenditure ceilings”.⁹⁴ In other words, it is not envisaged that the costs associated with enactment of the Bill will require additional financial resourcing.

The Department’s Explanatory Memorandum for the Bill also observes that “an incremental positive impact” on the Exchequer can be expected through reductions “in the future administrative burden on public bodies seeing to put individual data sharing arrangements on a statutory footing”.⁹⁵ In addition, the Department state that a decrease in the duplication on the part of public bodies is likely to give rise to incremental savings.

It should be noted that in the case of costs and savings associated with the Bill, there are no formal quantifications available at the time of writing.

The Regulatory Impact Assessment (RIA) of the Bill was published at the time of drafting the General scheme in April 2015.⁹⁶ The RIA provides the following assessment (Table 5 below) of the proposals and their likely impact. This in large part mirrors the financial implications as set out in the Bills’s Explanatory Memorandum.

Table 5: Summary of DPER’s RIA for the Bill.

Headings	Relevant text from the RIA
Costs	“A certain level of direct cost can be expected to arise for the Exchequer from the establishment of base registers, which has yet to be quantified. Direct staffing and other administrative costs can also be expected to arise from the legislative process and on an on-going basis from requirements under the Bill to put data sharing agreements in place and to undertake privacy impact assessments as part of all data sharing arrangements between public bodies. On the other hand, a positive impact on the Exchequer can be expected in terms of reducing the future administrative burden on Public Bodies seeking to put individual data sharing arrangements on a statutory footing as they arise which would otherwise have been covered by a general

⁹³ Department of Public Expenditure and Reform, 2018. Explanatory Memorandum, Data Sharing and Governance Bill 2018”. Available [here](#).

⁹⁴ *ibid.*

⁹⁵ *ibid.*

⁹⁶ Department of Jobs, Enterprise and Innovation, 2017. Regulatory Impact Assessment of the General Scheme of the Terms of Employment (Information) (Amendment) and Organisation of Working Time (Amendment) Bill 2017. Available [here](#).

	legislative basis. A decrease in the duplication of efforts by public bodies is also likely to give rise to incremental cost savings.”
Benefits	<p>“This option would result in a more streamlined and transparent statutory basis for data-sharing between public bodies accompanied by enhanced governance and better data management arrangements to apply to all data sharing arrangements between public bodies, whether they occur under this or any other statutory basis.</p> <p>This legislation would also further the public service reform agenda by providing for the establishment of base registers and the prohibition of the use of physical documents by public bodies in certain cases.”</p>
Impact	<p><i>National Competitiveness</i></p> <p>Widespread data-sharing between public bodies avoids the need to provide the same information multiple times to different bodies. The implementation of an “ask-once, use-many” approach can help to significantly reduce the administrative burden on citizens and businesses and allow them to avail of higher-quality, more efficient and seamless public services on a cross-sectoral basis.</p> <p><i>The Socially Excluded and Vulnerable Groups</i></p> <p>In so far as these groups may be more likely to have increased interaction with Public Bodies in accessing public services, the implementation of an “ask-once, use-many” approach may help to reduce the administrative burden that these groups experience in dealing with public bodies and allow them to avail of public services more easily.</p> <p><i>The Environment</i></p> <p>There are no impacts for the environment.</p> <p><i>Economic Market, including Consumer and Competition Impacts</i></p> <p>International experience highlights potential for transformation in the provision of services through a comprehensive and proactive approach to data-sharing. For example, the 2013 Shakespeare Review of Public Sector Information in the UK lists the potential benefits as ‘transparency, accountability, improved efficiency, increased data quality, creation of social value, increased participation, increased economic value, improved communication, open innovation, and data linkage’</p> <p><i>The Rights of Citizens</i></p> <p>Currently, Public Service Bodies request physical documents for the purposes of identification or validation of individuals or organisations during the course of a number of administrative transactions. The proposed Bill includes provisions whereby specific uses of physical documents could be proscribed if the intended outcome could be more efficiently brought about through data-sharing instead.</p> <p>The proposed legislation will also increase safeguards for citizens’ personal data held by public bodies by providing for enhanced governance and better data management arrangements to apply to all data sharing arrangements between public bodies, whether they occur under this statute or on any other basis. For example, Privacy Impact Assessments and Data Sharing Agreements recorded in Memorandums of Agreement available for public consultation will be required as part of all data sharing arrangements between public bodies.</p>

Source: DPER, 2015. Data Sharing and Governance Bill, Regulatory Impact Analysis.

Appendix 1

Table 6: Timeline of policy developments concerning the sharing of public sector data in Ireland

Year	Summary
2002	<p>Government Action Plan, New Connections A strategy to realise the potential of the Information Society</p> <p>The New Connections strategy identified ‘e-enabling the public service’ as a key issue going forward. The strategy stated that (at p. 21):</p> <p>“there is growing acceptance of the need for a greater internal e-government focus on streamlining background processes, facilitating cross-organisational collaboration, continuing to develop an organisational culture with a user-centric focus, and achieving the full benefits from the substantial investments in technology across the public service.”</p> <p>A stated objective of the New Connections strategy was to have all government services, that were capable of being delivered on-line, to be delivered on-line through one single point of contact by 2005 (at p.17). On-line services were to be delivered through a portal referred to as “Reach”.</p>
2003	<p>National Statistics Board (NSB), Strategy for Statistics 2003 - 2008</p> <p>The NSB Strategy for 2003 to 2008 proposed the creation of a network to link the Central Statistics Office (CSO) with all relevant government and agencies “to maximise the effective use of administrative data to generate useful, quality statistics” (at p. 7).</p>
2008	<p>OECD, Ireland Towards an Integrated Public Service</p> <p>The OECD Public Management Review stated, in the context of using eGovernment to deliver integrated and citizen-focused services, that (at p.14):</p> <p>“E-Government, and the development of a more integrated ICT interface, provides a major opportunity to deliver faster, more readily accessible services and secure internal data sharing to simplify contact with the Public Service.”</p> <p>The OECD review noted that (at p. 84):</p> <p>“[m]echanisms to improve or streamline systems so that the appropriate data can be better shared within and across the Public Service is something that should also be examined.</p>
2009	<p>National Statistics Board (NSB), Strategy for Statistics 2009 - 2014</p> <p>The NSB in the Strategy for 2009 to 2014 noted how the banking and regulatory failures raised queries concerning “the nature and quality of data available to policy-makers and the public” (at p. 5). The NSB identified seven priority actions for 2009 to 2014, one of which included strengthening institutional commitment to the continued development of the statistical infrastructure to link CSO generated statistics with administrative data holding within the public service. The Strategy stated that to achieve this (at p. 7):</p> <p>“Government departments and agencies need to take ownership of the statistical system and their role in it. This should be reflected in their data strategies and in their networking and co-operation with the CSO.”</p>
2011	<p>Department of Public Expenditure and Reform, Public Service Reform Plan</p> <p>The 2011 Public Service Reform Plan promoted, among others:</p> <ul style="list-style-type: none"> • the sharing of data across Government to reduce costs and enhance customer service delivery; • the introduction of a central system to provide a single view of customer identity based on the existing Public Service Identity dataset; • the sharing of data on businesses through the public service using Revenue’s Business

	<p>Register.</p> <p>It also committed to reviewing all relevant legislative provisions relating to data sharing between public bodies and developing principles for data sharing.</p> <p>National Statistics Board (NSB), Irish Statistical System: The Way Forward and Joined up Government needs joined up data</p> <p>The NSB report on the '<i>Irish Statistical System: The Way Forward</i>' identified data protection concerns as an obstacle to the use of administrative data for statistical purposes. The report identified the development of an Irish Statistical System (ISS) as a medium to long term objective of the NSB. The NSB stated that it believed (at p. 9):</p> <p>“that it is necessary to optimise the use of data holdings in the ISS for both statistical and practical purposes. This should lead to cost savings and greater efficiency, avoid duplication and facilitate effective analysis to inform policy decisions and assist monitoring.”</p> <p>In the section on '<i>Joined up Government needs joined up data</i>' the NSB stated that in order to inform policy through statistical analysis, it would be necessary to compile datasets – using existing administrative data – that are linked through the use of identifiers. In particular it pointed to the need for three categories of registers:</p> <ol style="list-style-type: none"> 1. all persons dataset; 2. institutions/ businesses dataset; and 3. buildings/dwellings dataset.
	<p>Government, Towards Recovery: Programme for a National Government 2011–2016</p> <p>The 2011 Programme for Government, in the context of anti-fraud, committed to the better sharing of data across government departments and agencies (at p. 23).</p>
2012	<p>Department of Public Expenditure and Reform, Supporting public service reform - eGovernment 2012–2015</p> <p>The eGovernment strategy for 2012 to 2015 identified a number of priorities for public service reform including improving data sharing across public service organisations. In particular it set out the following actions (at p. 17):</p> <ul style="list-style-type: none"> • Action 40: “Public bodies will promote practices and procedures that enable single point of data capture for cross system use, both within and across organisations”. • Action 41: “When new eGovernment services are being developed, these will, where appropriate, be designed to support cross organisational data sharing opportunities and to facilitate interoperability”. • Action 42: “Public Bodies will make data that is in high demand from other Public Bodies available across Government Networks for re-use, as appropriate and where legally permissible, to minimise duplication in data-sharing”. • Action 43: “The Department of Public Expenditure and Reform will ensure that a Federated Authentication System is put in place”. • Action 44: “The Department of Public Expenditure and Reform will chair a Data Sharing Clearing House to review relevant legislative provisions and produce and promote guidelines on best practice in the area of data sharing”.
2013	<p>Memorandum to Government for Heads of Data Sharing and Governance Bill</p> <p>In October 2013, the Department of Public Expenditure and Reform brought a Memorandum to Government setting out a series of actions to improve data-sharing in the public service, including the development of Heads of a Data Sharing and Governance Bill.</p>
2014	<p>Department of Public Expenditure and Reform, Public Service Reform Plan 2014-2016</p> <p>The 2014 Public Service Reform Plan envisions data sharing becoming a norm in the public</p>

	<p>service. It states that (at p. 18):</p> <p>“[d]ata sharing needs to be adopted as a key principle in the drive to modernise service delivery that one of the three key themes of the ICT strategy is to “build to share.”</p> <p>It also commits to the development of a “citizen authentication system” to ensure that personal data will be protected. Key actions of the 2014 Public Service Reform Plan include, among others (at p. 59):</p> <ul style="list-style-type: none"> • preparing the heads of a the Data Sharing and Governance Bill; • developing an Open Data portal; • delivering a range of new public service applications based on the Single Customer View.
	<p>Department of Public Expenditure and Reform, Data Sharing and Governance: Policy Proposals and resultant public submissions</p> <p>In August 2014, the Department of Public Expenditure and Reform published a policy paper entitled ‘Data Sharing and Governance: Policy Proposals’ setting out key elements of proposed data sharing and governance legislation and invited public submission on the proposals.</p>
	<p>Department of the Taoiseach and Department of Public Expenditure and Reform, The Civil Service Renewal Plan</p> <p>Action 24 of the Civil Service Renewal Plan is to improve how data is collected, managed and shared within the civil service. One of the ways identified as necessary for achieving this is to “develop a coordinated approach to data sharing and infrastructure as part of the forthcoming ICT Strategy” (at p. 34). Furthermore, Action 19 identifies the need to “recognise data as a corporate asset and develop a common data model and coordinated data infrastructure, underpinned by legislation” (at p. 30).</p>
	<p>Department of Public Expenditure and Reform, General Scheme of the Data Sharing and Governance Bill</p> <p>The Department of Public Expenditure and Reform published the ‘<i>General Scheme of the Data Sharing and Governance Bill</i>’ (see section 3 for outline of General Scheme).</p>
2015	<p>National Statistics Board (NSB), A World Class Statistical System for Ireland Strategic Priorities for Official Statistics 2015 – 2020</p> <p>The NSB Strategic Priorities for 2015 to 2020 states that (at p. 9):</p> <p>“[t]he public sector through the proposed Data Sharing and Governance legislation needs to establish a clear legal and ethical framework that clarifies the use of unique identifiers and sharing of administrative data for all public bodies, while ensuring that citizens’ personal privacy considerations are respected.”</p>
	<p>Central Statistics Office (CSO), Statement of Strategy 2015 – 2017</p> <p>The CSO Statement of Strategy for 2015 – 2017 states that (at p.10):</p> <p>“[a] key success factor in the exploitation of administrative data sources will be the development of a National Data Infrastructure allowing for the linking of administrative data sources from public bodies through the use of unique identifiers.”</p>
	<p>Department of Public Expenditure and Reform, Public Service ICT Strategy 2015</p> <p>The Public Service ICT Strategy identified “data as an enabler” as one of its five strategic objectives and identified the need to improve data governance and data sharing.</p>
2016	<p>Department of Public Expenditure and Reform, General Scheme of the Data Sharing and Governance Bill</p> <p>The Department of Public Expenditure and Reform referred the General Scheme of the Data Sharing and Governance Bill to the Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach for PLS.</p>
2017	<p>Department of Justice and Equality, General Scheme of the Data Protection Bill</p>

	The Department of Justice referred the General Scheme of the Data Protection Bill to the Joint Committee on Justice and Equality for PLS.
2018	Department of Justice and Equality, Data Protection Act 2018 The Data Protection Act became law on 24 May 2018.

Source: Oireachtas L&RS



Contact:

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000 or 076 1001700
Twitter: @OireachtasNews

Library & Research Service
<http://library>
Tel: +353 (0)1 6184701
Email: library.and.research@oireachtas.ie

Connect with us

