



An Roinn Caiteachais Phoiblí Bonneagair
Athchóiriúcháin Seirbhíse Poiblí agus Digitiúcháin
Department of Public Expenditure Infrastructure
Public Service Reform and Digitalisation

Data Sharing Standards Framework

Data Governance Unit



**Better Data Governance
Better Public Services**

Department of Public Expenditure Infrastructure
Public Service Reform and Digitalisation



Contents

1	Ministerial Foreword	2
2	Introduction	3
3	Glossary	4
4	Scope and Audience	6
5	The Once-Only Principle	7
6	Data Sharing and Standards Framework Layers	8
7	Data Sharing Principles	10
8	Layers and Actions	11
9	Appendix	14

1

Ministerial Foreword

The Data Sharing Standards Framework lays the foundation for best practice data sharing across the public service. As Minister for Public Expenditure, Infrastructure, Public Service Reform and Digitalisation, I remain committed to the delivering the Government's vision for an integrated public service and comprehensive, trusted data ecosystem. Achieving this vision requires leadership, consistent data governance and the adoption of best-in-class technologies.

This framework is underpinned by six core data sharing principles, applied across four layers: legal, organisational, semantic and technical. Together, these layers establish a standardised foundation upon which data sharing can be initiated, governed and sustained.

The Data Sharing Standards Framework serves as the cornerstone of a broader suite of data sharing supports, including Public Service API Standards and Guidelines, Data Sharing Agreement (DSA) and Accession Guidelines, Data Sharing Agreement Playbook, Data Sharing Agreement Template, the Accession Agreement Playbook and Accession Agreement Template.

By providing public service bodies with consistent, standardised tools, we are enabling them to address practical challenges of data sharing while adhering to best practice. The publication of this framework marks a significant shift away from fragmented data sharing approaches, aligning public bodies with a single reference point grounded in international best practices and standards. This unified approach strengthens the public service data ecosystem, unlocks greater value from the data we hold, and ultimately supports the delivery of better, more responsive public services.



Jack Chambers

Jack Chambers, T.D.,

*Minister for Public Expenditure, Infrastructure,
Public Service Reform and Digitalisation*

2

Introduction

Current public service data strategies and initiatives envisage the establishment of a public service-wide data ecosystem. It focuses on improving the re-use and sharing of data between Public Service Bodies (PSBs) in a secure, efficient, and transparent way, for the benefit of service users and PSBs. Implementing a comprehensive government-wide data sharing approach requires leadership, management, and technical skills.

Data sharing is critical for finding new ways to integrate one public service-wide approach across different public sector domains to provide better public services. The EU Once-Only Principle means that the public service should collect data once,

and only once from individuals and businesses, and re-use that data as opposed to recollecting it. Ultimately, when data re-use is increased, data recollection will be reduced. This reduces the burden on the public to resubmit information they have already provided and brings consistency of data across the public service. Additionally, it leads to the reduction in the administrative overhead on the public service to manage data recollection. With better data, comes improved evidence-based policy. These outcomes reflect the vision of the [Better Public Services Strategy](#), to deliver an inclusive, high quality and integrated public service that meets the needs and improves the lives of the people of Ireland.



3

Glossary

- ▶ **CHIEF INFORMATION OFFICER (CIO):** A senior executive responsible for managing and implementing an organisation's information technology strategy and systems.
- ▶ **CHIEF TECHNOLOGY OFFICER (CTO):** A senior executive responsible for overseeing the technological strategy and development within an organisation.
- ▶ **DATA SHARING INITIATIVE (DSI):** A push by one or more PSBs to share data across departmental borders or domains.
- ▶ **DATA SHARING TEAM:** A group of skilled individuals or staff from different functional areas tasked by the PSB to plan and execute DSI.
- ▶ **DATA OFFICER:** A Data Officer is an official from each PSB that serves as the main contact throughout the data sharing process and for the lifetime of a DSGA DSA or Accession Agreement. The Data Officer will communicate with the Other PSBs Data Officers in relation to the DSA, coordinate the DSA locally and advise their relevant stakeholders (authorised signatory and DPO) about the proposed DSA and be responsible for publishing the DSA notice on their website.
- ▶ **DATA GOVERNANCE UNIT (DGU):** The Data Governance Unit, in the Office of Government Chief Information Officer, provide a wide range of supports to both the Data Governance Board and PSBs as drafted data sharing agreements and accession agreements progress through the playbook process. The DGU consists of the DGB Secretariat and the Data Policy Team.
- ▶ **DATA PROTECTION OFFICER (DPO):** Designated individual on the basis of professional qualities and expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in [Article 39 GDPR](#).
- ▶ **DATA:** Information that is collected, organized, and used for analysis and decision-making. It can be raw or processed and comes in different forms including numbers, text, images, etc. It is essential for understanding patterns, making informed choices and gaining insights.
- ▶ **DATA GOVERNANCE:** The exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets. Data Governance guides all data management functions and ensures data is managed properly, according to an organization's policies and best practices.
- ▶ **Data Sharing and Governance Act 2019 (DSGA):** An Act to, inter alia, provide for the regulation of the sharing of information, including personal data, between public bodies.
- ▶ **EUROPEAN INTEROPERABILITY FRAMEWORK:** The European Interoperability Framework (EIF) provides specific guidance on how to set up interoperable digital public services. It was established by the EU Commission in 2017.
- ▶ **GDPR:** The GDPR, or General Data Protection Regulation, is an EU law that sets out rules for the protection of personal data and the rights and freedoms of data subjects.

- ▶ **OPEN DATA DIRECTIVE:** The Open Data Directive mandates the release of public sector data in free and open formats. It was transposed into Irish law in July 2021.
- ▶ **PUBLIC SERVICE DATA STRATEGY 2019-2023:** The strategy sets out a vision, along with a set of actions, on how the government can improve the use of data to support a more joined-up, efficient and effective Government.
- ▶ **DATA GOVERNANCE BOARD (DGB):** The [Data Governance Board](#) was established after the enactment of the Data Sharing and Governance Act. The Board has a remit that covers all areas of data management across the public service. The Board reviews all Data Sharing Agreements (DSA) submitted and may make recommendations in relation to a DSA, which must all be addressed by the PSBs involved before the agreement can be executed.
- ▶ **DATA SHARING COMMITTEE (DSC):** The Data Sharing Committee is a committee established by the DGB under the DSGA. This specialist committee will review all draft DSAs and accession agreements, and advise the DGB of the findings and observations where required.
- ▶ **DATA ARCHITECTURE & TECHNICAL COMMITTEE (DATC):** The Data Architecture & Technical committee plays a leading role in the introduction and promotion of technical guidelines and standards in the public service. The committee will also drive and support the Public Service Data Strategy actions of a technical nature in relation to Analytics, GeoSpatial and Data Standards and Architecture including Base Registries.
- ▶ **DATA SAFEGUARDING AND TRANSPARENCY COMMITTEE (DSTC):** Data Safeguarding and Transparency Committee helps ensure that any transparency, privacy, or data protection concerns that arise around the sharing or governance of data are managed in an ethical way. The DSTC is responsible for the implementation of a Data Sharing Ethics Framework for use across the public service.

- ▶ **NATIONAL DATA INFRASTRUCTURE NDI / NDI+:** The National Data Infrastructure Champions Group monitors and promotes use of unique identifiers across public sector data holdings. This group has the ambition of identifying gaps in the coverage of unique identifiers while also promoting the value of the NDI in addressing known and emerging data needs in the public service.

4

Scope and Audience

This Data Sharing Standards Framework presents a foundation for this approach by introducing a clear roadmap, actions, and standards for sharing data across the public sector under the [Data Sharing and Governance Act 2019](#) (DSGA)¹. This framework was developed to align with international best practices for data sharing and this methodology may be considered as a support in a wider data sharing context but only after compliance with appropriate data protection legislation has been satisfied, subject to exclusion under the DSGA.

This framework is aimed at all those involved in data sharing across the public service, in particular Data Officers, stakeholders and data leaders.

While the use of this framework remains optional, it is particularly relevant for the purpose of Data Sharing Agreements drawn up and adopted under the DSGA. Legislation exists outside of the DSGA, which provide PSBs the legal basis with which to share data. This framework will not apply in these cases. However there are aspects and features of the framework which may be usefully drawn upon where appropriate. The framework, therefore,

should be reviewed and applied on a case-by-case basis.

This framework document consists of four sections. It starts with outlining the purpose of the Data Sharing Standards Framework and then sets out international best practice of introducing the legal, organisational, semantic, and technical layers that form the foundation of the framework. The third section introduces the data sharing principles that underpin this framework while the fourth outlines concrete objectives, actions, roles and references for each of the framework layers.

The [Appendix](#) provides a list of relevant standards and resources that support implementation by PSB's.

¹ The Statistics Act 1993 falls out of scope of the Data Sharing Standards Framework

5

The Once-Only Principle

Purpose & Mission

The sharing of data across public service domains provides opportunities for improvement in the provision of more user-friendly and efficient services and for the implementation of the [Once-Only Principle \(OOP\)](#). This principle ensures that individuals and businesses provide data to public administrations only once and this data can be exchanged among public bodies when requested and in compliance with any relevant regulations.

This framework provides a roadmap to public sector bodies on how to initiate data sharing within

the context of their operations, outlining the legal, organisational, semantic, and technical layers and respective data sharing standards that need to be considered during the process.

It is important to note, that data collected cannot always be re-used and for this reason, a review of the legal basis and GDPR is essential before any data sharing occurrence. In some cases, the sharing with other PSBs of personal data collected or supplied for a specific purpose is strictly prohibited by law. There are numerous examples of this across the public service. Data may be supplied to PSBs on the strict understanding that it will not be shared.



6

Data Sharing Standards Framework Layers

In-line with current public service data strategies and initiatives including and the Harnessing Data Effectively section of the [Connecting Government 2030 ICT Strategy](#), the Data Sharing Standards Framework emphasises the need for the re-use of data for better public sector service delivery.

In proposing a way to facilitating the above, the Public Service Data Strategy makes clear reference to the [European Interoperability Framework](#) (EIF) and its four legal, organisational, semantic and technical layers, which allow for integrated digital services.³ These four layers are the foundation of this Data Sharing Standards Framework and their respective actions and referenced standards must be part of any data sharing initiative. Section four of this document describes the practical instruction in more detail.

“Integrated digital public services requires PSBs to cooperate and re-use data and services in an effective, structured, consistent, and transparent way. By embracing an API² approach for Government, data and services can be exposed for re-use in a secure, consistent manner, leading to the delivery of more joined-up, efficient public services for citizens and businesses”
(Public Service Data Strategy, 2023)

² An Application Programming Interface (API) is software that provides secure transmission over the internet and enables the transmission of data between them.

³ Integrated Digital Services make use of digital technologies to streamline and unify various public services. The objective is to create a seamless and interconnected experience for citizens when accessing government services through digital channels. The integration involves leveraging business process logic and technology to consolidate different services into a cohesive one, which allows citizens to access multiple public services through a single digital interface. The aim is to improve efficiency, accessibility, and user experience while reducing bureaucratic barriers.

Data Sharing Standards Framework

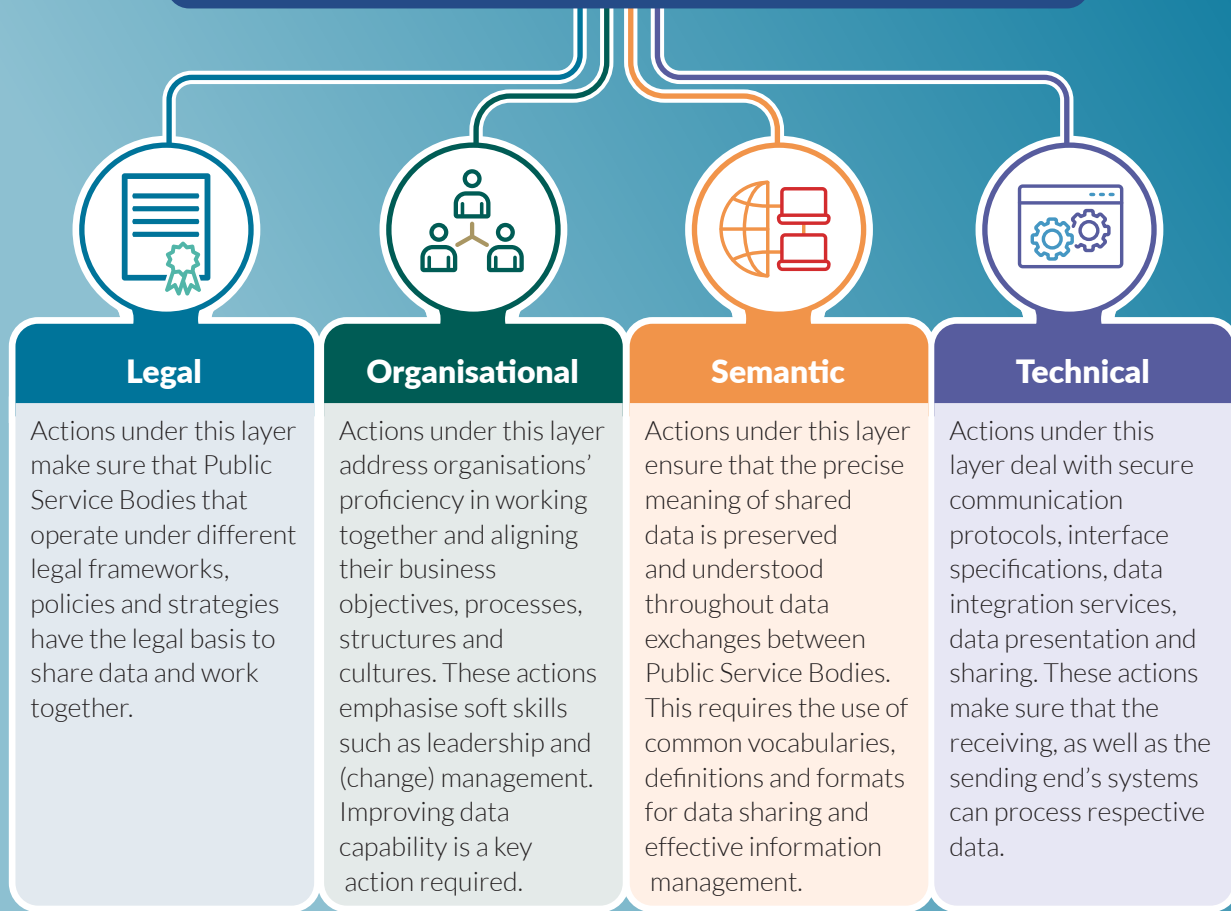


Figure 1: Data Sharing Standards Framework

7

Data Sharing Principles

The Data Sharing Standards Framework is underpinned by six principles that must be considered across all legal, organisational, semantic and technical actions associated with any data sharing initiative. Confidentiality, Integrity and Availability form the C-I-A triad, a long-established practice of cybersecurity. The triad is complemented by three further principles: Transparency (see [Art. 5, GDPR](#)), Security (see [Article 32 GDPR](#)) and Accountability (see [Art. 5, GDPR](#)).

Together, these six principles will ensure that data is processed and made available in a secure and authorised manner by making use of appropriate technical and organisational measures to protect it, prevent illegal tampering while simultaneously logging all user access for monitoring purposes. GDPR principles apply to personal data only.

The case-studies in the [Appendix](#) illustrate the sharing of personal and non-personal data and outline how these principles can be practically applied.

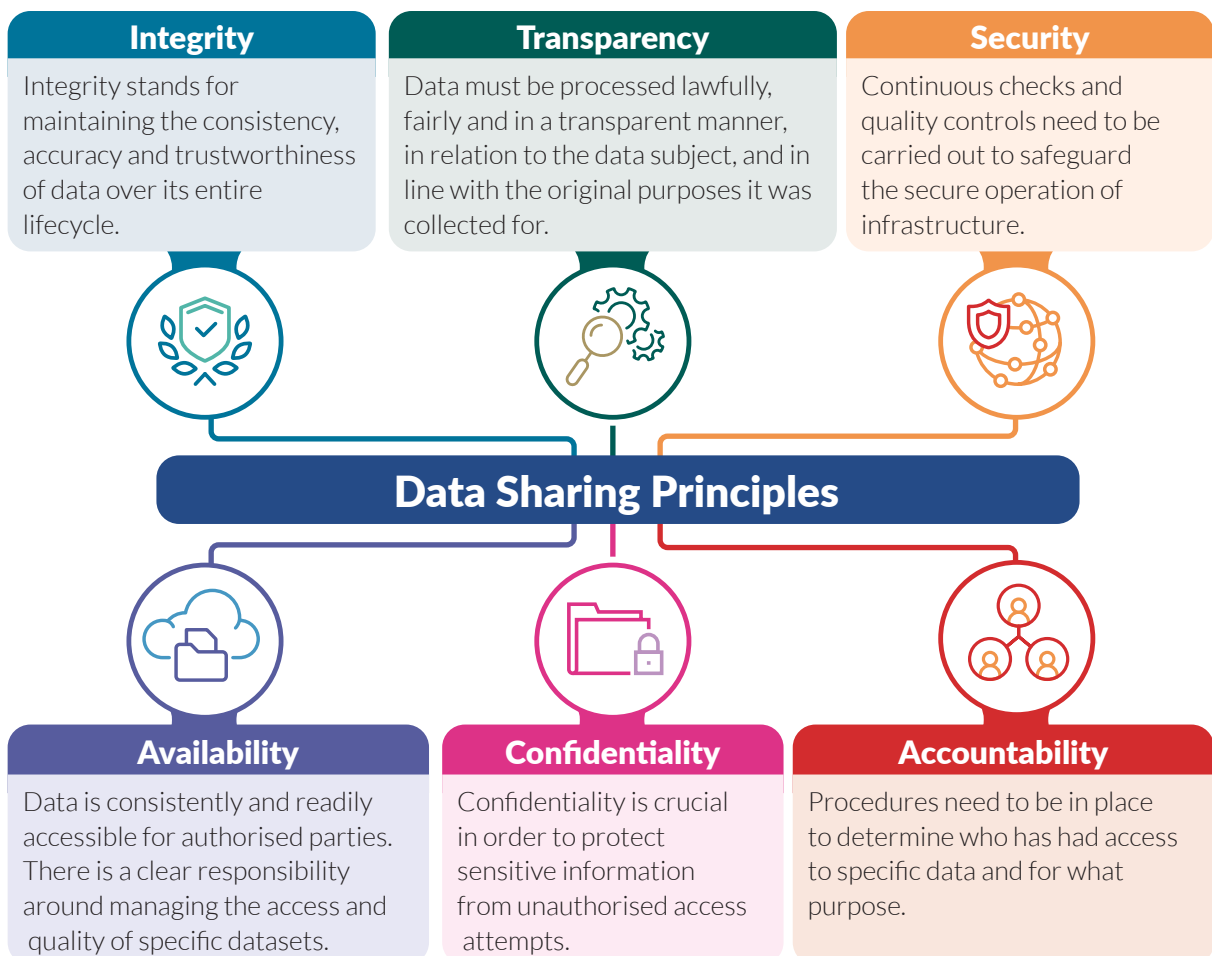


Figure 2: Data Sharing Principles

8

Layers and Actions

A data sharing initiative should be developed considering all four layers, whose actions are enhanced by a number of specific standards. The standards of layers (detailed in the [Appendix](#)) provide more practical guidance on how to carry out the actions. A data sharing initiative would typically start actions under the legal layer, but this is not mandatory. It is crucial to address all

layers, as any data sharing initiative will have legal, organisational, semantic and technical implications for both the PSB providing and the PSB receiving data. If not addressed, the data sharing initiative could fall short of its intended impact, namely re-using data for better public sector service provision.

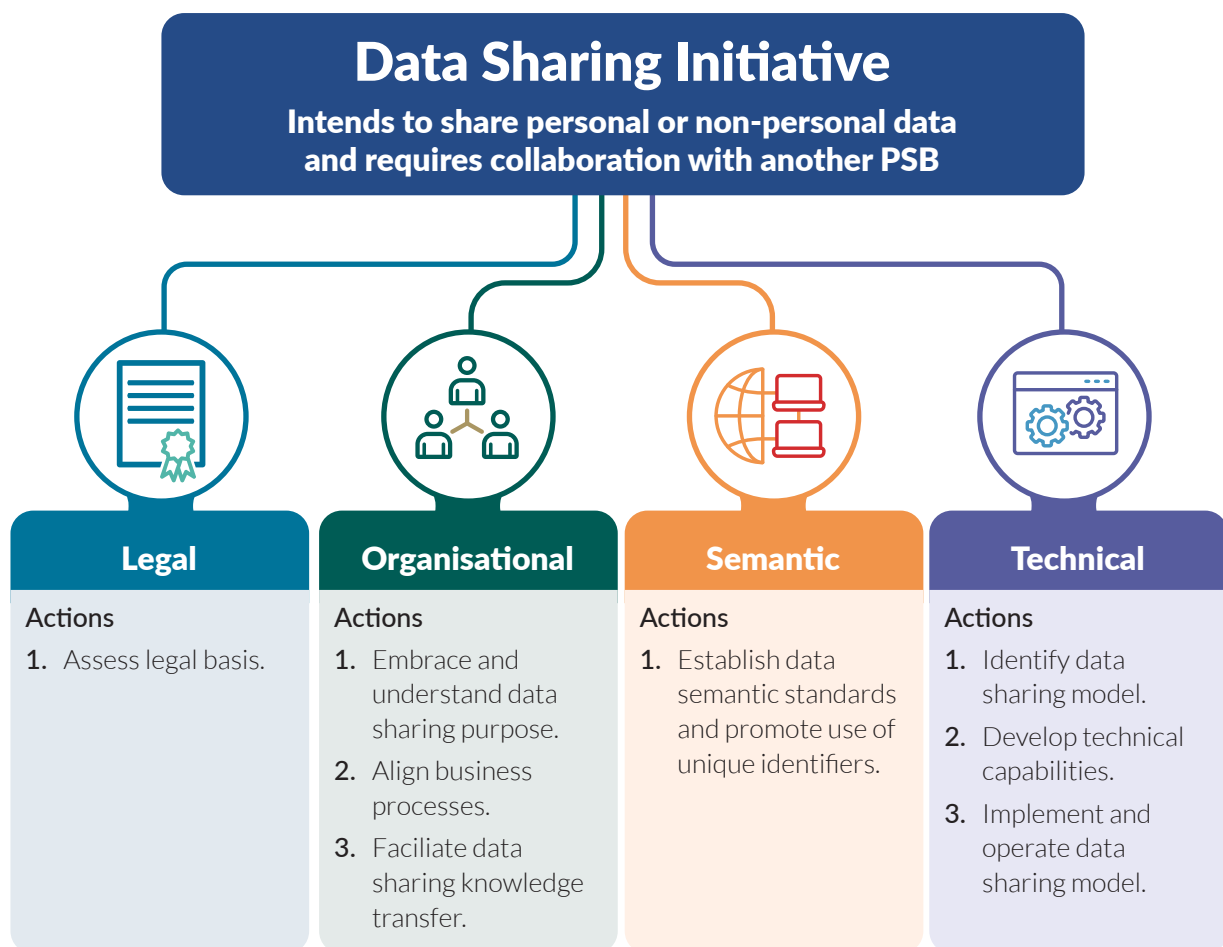


Figure 3: Data Sharing Initiative Overview

8.1 Legal



Objective

Establish a clear legal basis for any respective data sharing initiative.

Actions

1. Assess legal basis

There must be a clear legal basis for all data collected, stored and shared by any PSB. In addition to achieving a legal basis for data sharing, any data sharing initiative should be checked against the Data Sharing Ethics Framework, which guides PSBs to integrate ethics evaluations into data sharing decisions. A [Data Protection Impact Assessment](#) is an important step before any data sharing agreements are considered. Sharing personal data must also comply with the legal provisions of the [Data Sharing and Governance Act](#) or any other legislation facilitating the data sharing. GDPR and primary legislation governing the bodies involved or any other relevant EU legislation must also be considered. The [DSGA Data Sharing Agreement Playbook](#), the [DSGA Accession Agreement Playbook](#), the [DSGA Model Data Sharing Agreement Template](#) and the [DSGA Accession Agreement Template](#) are available to guide practitioners on compliance with the DSGA. Previous data sharing agreements between the parties are specific to earlier projects but may be reviewed to inform the current process and as templates for further agreement. Non personal data may be considered under the [Open Data Directive and Regulation 2018/1807: Regulation on a Framework for the free flow of non-personal data in the European Union](#). Furthermore, the [European Data Governance Act](#) provides a legal basis for sharing of protected data across the EU including data standards and data security mechanisms, that include National Single Information Points established by EU member states.

Roles

Some roles that are likely to be important at this stage of the process include:

- ▶ Data Officers

- ▶ Data Protection Officers – see more on [GDPR and the role of the DPO](#), also the [Data Protection Commission](#) provides further information.
- ▶ Legal Advisors
- ▶ [Data Governance Board](#) (DGB)
- ▶ Data Sharing Committee (DSC)

8.2 Organisational

Actions



Objective

Introduce and initiate data sharing among PSBs for more integrated public services.

1. Understand and embrace purpose of data sharing:

Management and business units within PSBs must have a clear understanding of the benefits of data sharing and fully embrace it at strategic level to fully realise its potential. This will require:

- ▶ Considering data sharing initiatives during a PSB's data strategy process and allocating respective resources.
- ▶ Assessing organisational data sharing readiness.
- ▶ Establishing concrete data sharing benchmarks and progress their reviews.
- ▶ Leadership support and international stakeholder management for data sharing initiatives throughout the process. Further information on this topic can be found in the Data Sharing Ethics Framework Toolkit on Stakeholder Mapping.
- ▶ Reviewing the [Public Service Data Catalogue](#) and [Public Service API Catalogue](#) to identify datasets which may advance business needs.
- ▶ Contributing to, promoting, and maintaining the [Public Service Data Catalogue](#) and [API Catalogue](#) to help circulate knowledge of data holdings among other PSBs.
- ▶ Having data and re-use of data as standing items within the senior management team or equivalent. It should be part of the PSB's culture to ask if sharing data with other PSBs is needed or to have data shared with them.

2. Align Business Processes:

Business processes within organisations may need to be reviewed so that they align more effectively with an enhanced public service data sharing environment. This will involve:

- ▶ Mapping, analysing and re-envisioning current business processes in a collaborative way.
- ▶ Co-operating on the creation of roadmaps for data sharing initiatives.
- ▶ Establishing strong working relationships with partner organisations and professional networks.

3. Data Sharing Knowledge Transfer:

In order to embed a data sharing ethos throughout the public service, there must be a drive to increase knowledge levels and share solutions and best practices throughout all PSBs by:

- ▶ Facilitating national and international exchange of best practices.
- ▶ Inviting external perspectives on established data sharing initiatives and their challenges.
- ▶ Implementing skills profile to assist recruitment as an effective way to increase knowledge.

Roles

Some roles that are likely to be important at this stage of the process include:

- ▶ Senior Public Sector Management.
- ▶ Data Governance Board.
- ▶ Data Safeguarding and Transparency Committee (DSTC): a committee under the DGB which champions data safeguarding and transparency across the public service.
- ▶ Central Statistics Office (CSO).
- ▶ External Advisors such as Public Private Partnerships, academia, and industry experts.

8.3 Semantic Actions



Objective

Ensure data compatibility within the public service by establishing and adhering to data standards. Data semantic standards are essential for any data sharing initiative. Standards provide a way to organise and classify data to create a structured hierarchy allowing for a meaningful and consistent data sharing experience.

1. Establish Data Standards and Promote Use of Unique Identifiers

Data standards, universally applied throughout the public service, enable data to be effectively shared among different bodies with minimum administrative overhead. The National Data Infrastructure Champions Group (NDI) chaired by the CSO, plays a key role here, encompassing PSBs with high value data holdings, with the aim of promoting data as a strategic public asset. The CSO are widely regarded as the stewards of Data Standards within the public service. This action involves:

- ▶ The CSO developing and supporting the implementation of data standards for key data concepts to further advance the coverage of the NDI / NDI+. The NDI+ will improve the potential of linking data through the use of CSO data standards for CSO data standards across public sector data holdings.
- ▶ Promoting the coverage of unique identifiers across public sector data holdings under the guidance of the NDI.
- ▶ Introducing open, widely accepted, standards governing various data types across the public sector in your data where possible.
- ▶ Facilitating exchange of best practice around data standards.
- ▶ Adopting the Data Quality Framework.
- ▶ Introducing benchmarks for adoption of data standards.
- ▶ Introducing incentives around the adoption of data standards.

Roles

Some roles that are likely to be important at this stage of the process include:

- ▶ Data Architecture & Technical Committee (DATC): a committee under the DGB that promotes the adoption of data standards within the public service.
- ▶ National Data Infrastructure Champions Group (NDI).
- ▶ Central Statistics Office (CSO).
- ▶ Senior Public Sector Management.

8.4 Technical



Objective

Ensure that data flows securely and reliably

Actions

1. Identify Data Sharing Model

There are a number of avenues open to PSBs to share data depending on the type and sensitivity of data involved. Non-personal data can be published on the national Open Data Portal data.gov.ie. This would, of course, exclude commercially sensitive or confidential data. The processing of personal data by any public service body must comply with the [GDPR](#).

An Application Programming Interface (API) is software that provides secure transmission of data over the internet between API providers and consumers. The [Public Service API Catalogue](#) provides details of non-open datasets accessible through available APIs provided by the holders of these datasets. If an API exists, it may be possible to incorporate it into existing or new business process applications. If an API does not exist, the creation of one using acceptable API standards may be considered. An API with authentication, will provide a safe and secure mechanism to share data in a repeatable manner while allowing the ability to track access to data. An API is a recommended approach for sharing data, though it must be noted it is not appropriate for all data sharing initiatives. It may depend on size of data sent or received and any technological limitations.

In addition, the NDI / NDI+ may provide structures for sharing data using unique identifiers such as PPSN, Eircode or the Unique Business Identifier (UBI).

2. Develop Technical Capabilities

Any data sharing initiative requires some level of technical capacity within the parties involved to ensure its successful implementation. The skills required may cover a range of activities from

data infrastructure to software creation and data analysis/business intelligence. A review exercise should be carried out to ascertain:

- ▶ What skills are needed?
- ▶ If they are available?
- ▶ How they may be acquired?

3. Implementation and Operation of Data Sharing Model

Once the data sharing model has been agreed between the PSBs involved and the technical capacity is available, a clear blueprint should be produced outlining the development, maintenance and operation of its service. It is recommended for the service to be monitored and evaluated as agreed with actions detailed under the organisational layer. This will ensure that the service complies with the expectations of all parties and helps identifying opportunities for improvement where necessary. [Public Service API Standards and Guidelines](#) can provide details regarding international best practices for this area. The review of this document is strongly encouraged during any technical implementation.

Roles

Some roles that are likely to be important at this stage of the process include:

- ▶ CIO / CTO
- ▶ Senior Public Management
- ▶ CSO
- ▶ NDI / NDI+
- ▶ Data Architecture and Technical Committee

9

Appendix

This work was supported by Derilinx, who provided expert input on the development of the Data Sharing Standards Framework.

9.1 Full list of referenced standards

Legal

- ▶ [Data Sharing Governance Act \(DSGA\)](#) – an Irish legal act providing for the regulation of the sharing of information, including personal data, between PSBs.
- ▶ [DSGA Data Sharing Playbook](#) – accompanies the above mentioned DSGA and outlines practically how to put together a Data Sharing Agreement between two or more PSBs.
- ▶ [EU Data Governance Act \(DGA\)](#) – the DGA regulates the re-use of protected data held by PSBs. Together with the EU Data Act and the Open Data Directive it forms the basis for data governance in the European Union.
- ▶ [General Data Protection Regulation \(GDPR\)](#) – the GDPR is an EU regulation, highly regarded internationally, to protect natural persons and the processing of personal data and govern the free movement of such data.
- ▶ [DSGA Model Data Sharing Agreement Template](#) – the DSGA Model Data Sharing Agreement template has been designed for the sharing of personal data under the Data Sharing and Governance Act 2019. This model DSA template is subject to revision in the future.
- ▶ List of published [DSGA Data Sharing Agreements](#) – this lists the current proposed or published data sharing agreements on the website of the Data Governance Board DSA Register.
- ▶ [Public Service Data Catalogue](#) – The Public Service Data Catalogue aims to promote openness and transparency around the data held by the public service by cataloguing and describing public service data.

Organisational

- ▶ [Public Service Data Strategy](#) – the strategy sets out a vision, along with a set of actions, on how the government can improve the use of data for a more joined up, efficient and effective Government.
- ▶ [European Interoperability Framework \(EIF\)](#) – the EIF provides specific guidance on how to set up interoperable digital public services. It outlines the four interoperability layers in great detail.
- ▶ European Commission [Interoperability Quick Assessment Toolkit \(IQAT\)](#) – IQAT is a useful tool that allows product / service / solution owners to quickly assess the potential interoperability of their solutions. It's freely available [here](#).
- ▶ Data Sharing Ethics Framework – this framework introduces the ethical considerations that are necessary when sharing personal data and recommends a process for how to address them.
- ▶ Data Quality Framework - this framework provides PSBs with a path for continuous improvement and monitoring of the quality of their data holdings.
- ▶ [The Public Service API Catalogue](#) - the central point for PSBs to register details of non-open data APIs, facilitating access to common datasets held within the public service. The API Catalogue does not contain any personal data collected from the public but does detail metadata regarding the purpose of APIs, datasets accessible, the organisation that holds the API and dataset, and how PSBs can access APIs.

- ▶ [Public Service Data Catalogue](#) - provides high-level information on over 1,360 key datasets across almost 100 PSBs. It catalogues the key data in these bodies, including personal data, business data, and data critical to business decisions or service delivery. This catalogue provides the public with simple descriptive information about datasets. It also includes the purpose and coverage of the dataset and if any personal or sensitive data is contained within it.
- ▶ Five views of the Business Process, [Architecture of Integrated Information Systems](#) – ARIS is a unique and internationally renowned method for optimising business processes. Its five-view architecture breaks down the complexity of an organisation's business processes and makes their modelling / mapping simpler. The ARIS Community has created a free ARIS Business Process Modelling software. The software is available [here](#).
- ▶ User Journey Mapping, [Atlassian Guide](#) – User journey mapping is a way to visualise and understand how users experience a product or service over time and across channels. It's a helpful tool for organisations to map their services. The Atlassian Guide provides a practical template process for such an exercise.
- ▶ [Business Process Model Notation v2.0](#) – A Business Process Model and Notation (BPMN) provides businesses with the capability of understanding their internal business procedures in a graphical notation and gives organizations the ability to communicate these procedures in a standard manner. BPMN 2.0 is the current standard.
- ▶ Business Analysis Body of Knowledge, [BABOK](#) – is a globally recognized standard for the practice of business analysis. The BABOK® Guide describes business analysis knowledge areas, tasks, underlying competencies, techniques and perspectives on how to approach business analysis.
- ▶ Data Management Book of Knowledge, [DMBOK](#), Chapter 17 – DMBOK is a comprehensive guide to the concepts, principles, and practices of data management. Chapter 17 accounts for all matters related to data management and organisational change management, which is required for introducing data sharing to an organisation.

- ▶ EU Commission [Digital Public Administration \(DPA\) factsheets](#) – the National Interoperability Framework Observatory DPA factsheets represent the most recent developments that the public administrations of 31 European countries have undergone.
- ▶ X-Road [Case Studies](#) – X-Road is regarded as one of the most successful public sector data sharing framework and used in multiple countries.

Semantic

- ▶ [Open Standards For Data](#) – the Open Data Institute's online guidebook helps people and organisations create, develop, identify and adopt open standards for data.
- ▶ Centre for Government Excellence, [Open Standards Directory](#) – the directory contains more than 60 Open Data standards from different domains and is a useful resource for identifying potentially applicable standards.
- ▶ Government-approved standards (UK): [Open Standards For Government](#) – this is a list of UK government approved open standards for the UK government and is also useful for identifying potentially applicable standards.
- ▶ EU Commission SEMIC Support Centre: [eGovernment Core Vocabularies Handbook](#) – acts as an enabler for reducing semantic interoperability conflicts and a resource for e-Government specific terminology.
- ▶ Domain-based standards such as Public Google Transit: [GTFS Static Overview](#) – this is a widely regarded standard that is listed here as an example of a domain-specific standard. It defines a common format for public transportation schedules and associated information.
- ▶ [Data Governance Board](#).
- ▶ Data Architecture and Technical Committee.
- ▶ Data Quality Framework – the aim of the framework is to improve the level of data quality across the public sector. It will be used to provide PSBs with a path for continuous improvement and monitoring of the quality of data holdings. It is currently being compiled and will be published by the OGCIO.

- ▶ Data Strategy Template – this template provides practical guidance on the compilation of data strategies. It will be used by PSBs across the public service. It is currently being compiled and will be published by the OGCIO.
- ▶ [OGCIO Data Maturity Assessment](#) – A data maturity assessment is a method available to public bodies to assist them in improving data, data management and its governance.

Technical

- ▶ [Public Service API Standards and Guidelines](#) - are standards that are agreed best practice for development, design, management, security and maintenance of APIs. As set out in the Connecting Government 2030 strategy and in relation to Government as a Platform, the Public Service API Standards and Guidelines are essential to support an interoperable all-of-government digital environment.
- ▶ National Data Infrastructure (NDI) - NDI concerns itself with the consistent and reliable identification of data e.g. data that relates to a particular location – through the use of an Eircode; particular person – through the use of a PPSN; particular business – through the use of a Unique Business Identifier (UBI).
- ▶ [The Connecting Europe Facility eDelivery Building Block two, three, four corner model.](#)
- ▶ Introduction to [E-Delivery Building Block](#) – provides technical specifications and standards, installable software and ancillary services to allow projects create a network of nodes for secure digital data exchange.
- ▶ Introduction to the [X-Road Project](#) – X-Road is regarded as one of the most successful public sector data sharing frameworks and used in multiple countries. X-Road started in Estonia and has since been implemented in Finland, Iceland and a wide range of other countries worldwide.
- ▶ Electronic cross-border health services ([eHDSI](#)) – The eHealth Digital Service Infrastructure (eHDSI) is an infrastructure ensuring the continuity of care for European citizens while travelling abroad in the EU. This gives EU countries the possibility to exchange health data in a secure, efficient and interoperable way.
- ▶ Introduction to the [Govstack Project](#) – aims to build a common understanding on fundamental reusable and interoperable digital components. Its [Information Mediator](#) provides a gateway for exchange of data and services among GovStack Building Blocks through open-API REST-based interfaces to ensure interoperability and implementation of standards.
- ▶ Gaia-X [Federation Services \(GXFS\)](#) – Gaia-X promotes open innovation through sovereign data sharing based on trust between all involved actors. GXFS provides a set of open-source software components that assist in operating a Gaia-X compliant federated ecosystem of infrastructure and data.
- ▶ Managing the security of Information Exchange, [NIST Standard 800-47](#) – this standard focuses on managing the protection of the information being exchanged or accessed before, during, and after the exchange and provides guidance on identifying information exchanges, considerations for protecting exchanged information, and the agreement(s) needed to help manage the risk associated with exchanging information.
- ▶ Information and documentation – Data exchange protocol for interoperability and preservation, [ISO 20614:2017 \(DEPIP\)](#) – DEPIP specifies a standardised framework for the various data (including both data and related metadata) exchange transactions between an archive and its producers and consumers.
- ▶ e-Delivery [Training and Deployment Service](#) – Freely available training material for the e-Delivery Building Block.
- ▶ eHDSI [Training Course](#) – Freely available training material for eHDSI.
- ▶ X-Road [Academy](#) – Freely available training material for X-Road Implementation.
- ▶ A Unique Identifier (UID) is a numeric or alphanumeric string that uniquely identifies a single entity.
- ▶ A data standard is a technical specification that describes best practices on how data should be stored and exchanged.

9.2 The Irish Data Sharing Landscape in 2024

The Irish data sharing landscape is shaped by two key pieces of data legislation. The Data Sharing Governance Act 2019 and the Open Data Directive should be considered in the context of the current public service data vision of improving data governance, management, and re-use of data in a secure, efficient, and transparent way.

The [Open Data Directive](#), as of 2015, has had a clear [technical framework](#) in place on how to publish respective data. The [Open Data Portal](#), [Public Service Data Catalogue](#) and [PxStat](#) are functional tools for the public sector to use for their open data publication.

Likewise, the DSGA has introduced very clear [data sharing and accession playbooks](#), which outline the legal procedure of how to share personal data based on the creation of a data sharing agreement. However, there are no current guidelines on how to address organisational, semantic, and technical considerations when introducing data sharing initiatives. The Data Sharing Standards Framework addresses this and provides actionable guidance for PSBs that intend to become more prolific in data sharing.

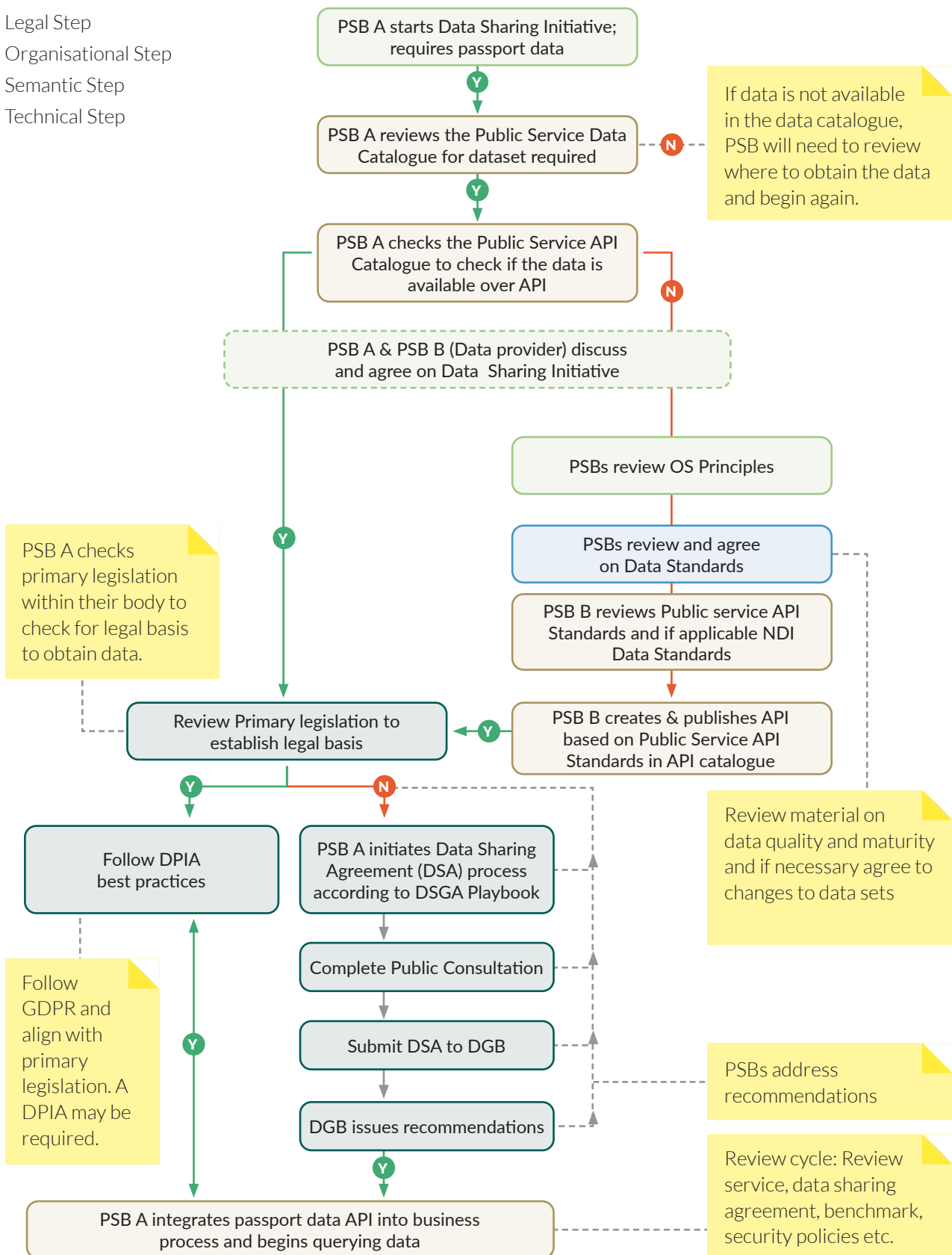
Vision	Improve Data governance, management, and re-use of data in a safe and transparent way	
Legislation	DSGA	Open Data Directive
Type of Data	Personal	Non-Personal
Prerequisites for DS	Data Sharing Agreement Base Registry Data	Open Data (OD)
Catalogues	Public Service (PS) API & National Single Information Point Catalogues	OD Portal PS Data Catalogue PxStat
Data standards	NDI EU Standards	Int. Standards CSO Standards

Figure 4: Overview over Irish Data Sharing Landscape

Case Study

Sharing Personal Data

- Legal Step
- Organisational Step
- Semantic Step
- Technical Step



Any kind of personal data, such as e.g. passport-related data, can only be processed by an authorised entity. If a public service body (PSB A, data requester) needs an individual personal data, managed by another entity (PSB B, data provider), PSB A would check the Public Service Data Catalogue to see if the data is available. If it's not, the respective source needs to be identified before being able to move ahead.

If it is listed there, PSB A would then search the Public Service API Catalogue to determine whether the data is readily available to be shared. If a dataset is listed in the API catalogue, the data provider and requester need to agree on the conditions for sharing the data. The data provider needs to be assured that the data client will protect the data and only use it for the indicated purpose. The following data sharing principles and respective statements are helpful during this process:

- ▶ Data is accessed by authorised personnel only (Confidentiality).
- ▶ Data is not changed (Integrity).
- ▶ Data is available 24/7 and there's a redundancy plan (Availability).
- ▶ Data Ownership remains with data provider (Ownership).
- ▶ Data is transmitted securely via trusted protocols (Security).
- ▶ Access to data is logged, time-stamped and signed for accountability (Accountability).

Once the two organisations have agreed terms, the next steps depend on whether data can already be accessed via an existing API or whether a new one needs to be created. If there is an existing API, legal basis needs to be established to allow the sharing of the required personal data. This can be done by first reviewing the PSB's primary legislation, and if no such basis can be established it may be possible to establish legal basis under the remit of the Data Sharing and Governance Act 2019. Once legal basis has been established, DPIA best practices and GDPR need to be considered and followed before the formal process of creating a data sharing agreement can be initiated in accordance with the Data Sharing and Governance Act and the DSGA Playbook which outlines each step in formalising a data sharing agreement.

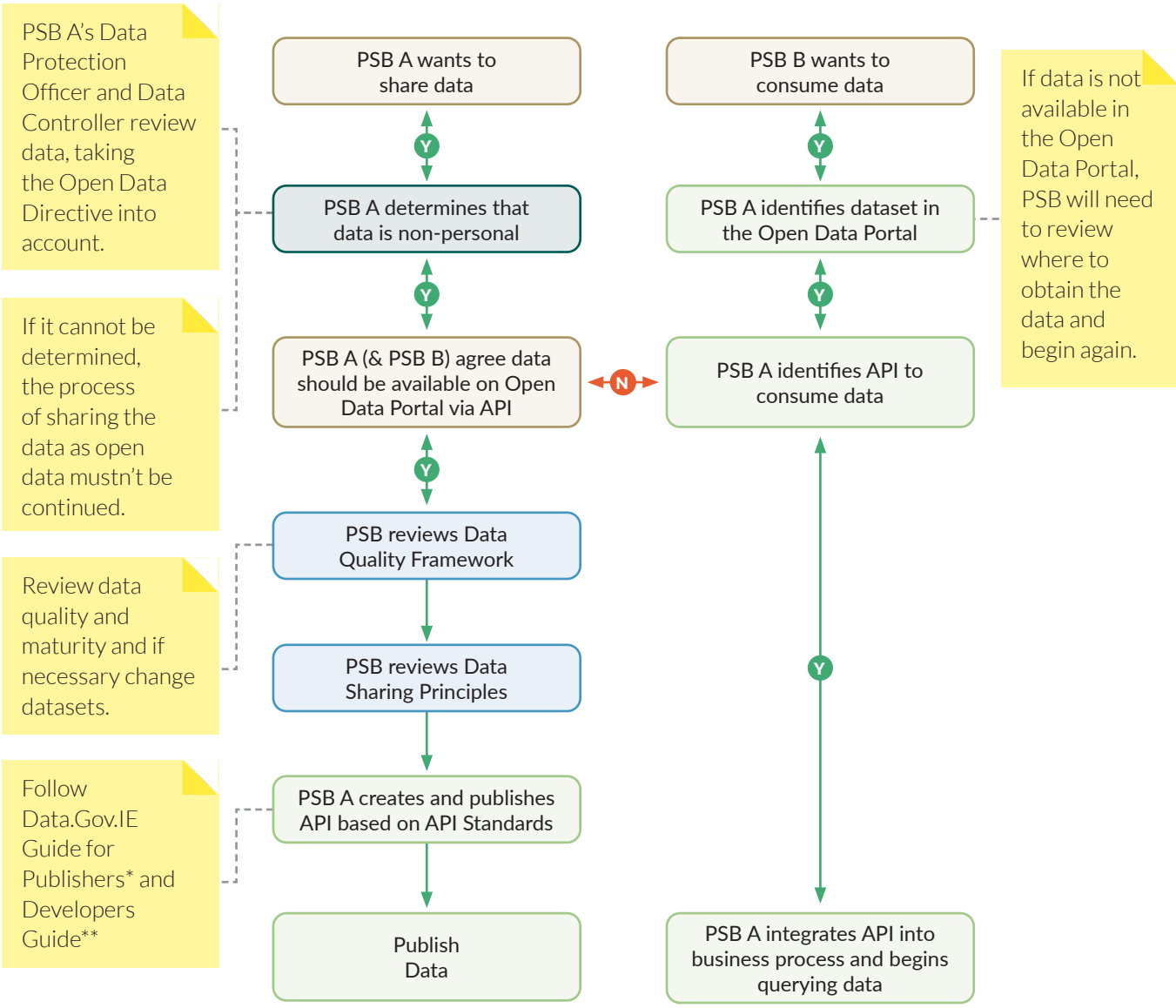
If there is no existing API, the data provider needs to create one according to the Public Service API Standards and Guidelines and consider common NDI & NDI+ Data Standards. Before reviewing these API standards and respective NDI & NDI+ Data Standards, the PSBs need to review the data sharing principles, as outlined above, and agree on a data standard that takes the Data Quality Framework into consideration. Once this is done, the API can be created and the legal review process starting with primary legislation can be initiated and followed as previously outlined.

As soon as the legal approval is provided, PSB A has all it needs to integrate API calls into its service's business process for the data sharing to begin.

Assuming PSB A would like to share non-personal data, such as data about the [Daily Irish Gas Demand](#), it would first need to determine whether the data can be considered open data according to the Open Data Directive.

If it is open data, PSB A and the requester, PSB B, agree that the data should be available on [data.gov.ie](#) via an API. To publish the data via API on the Open Data Portal, PSB A needs to review the data sharing principles and agree on a data standard that takes the Data Quality Framework into consideration. Once that is done, PSB A creates and publishes the API based on the [Public Service API Standards](#) and Guidelines document. Helpful resources are the Open Data Portal Guides for [Publishers](#) and [Developers](#). As soon as the API is published, PSB B can integrate the newly created API into its business process(es) so the non-personal data sharing can begin.

Sharing Non-Personal Data



* <https://data.gov.ie/pages/guideforpublishers>

** <https://data.gov.ie/pages/developers>

9.3 Further Reading

An introduction to the two, three and four-corner model may be useful for facilitation of Data Sharing.

The Connecting Europe Facility [eDelivery Building Block](#) introduces three message exchange topologies, the so-called two-, three-, and four-corner models. They are characterised by the following advantages and disadvantages:

2-corner model: Direct back-end communication

Pro:

- ▶ Simple integrations

Con:

- ▶ Difficult to scale
- ▶ Heavy impact on backends

3-corner model: Back-end communication via central hub (Enterprise Service Bus)

Pro:

- ▶ No need to set up bilateral channels between participants
- ▶ Central management and control of all processes
- ▶ Central monitoring processes

Con:

- ▶ Central Access Point may become a bottleneck/ single point of failure
- ▶ Risk of service provider lock-in
- ▶ Scalability

4-corner model: Back-end communication via standardised gateways

Pro:

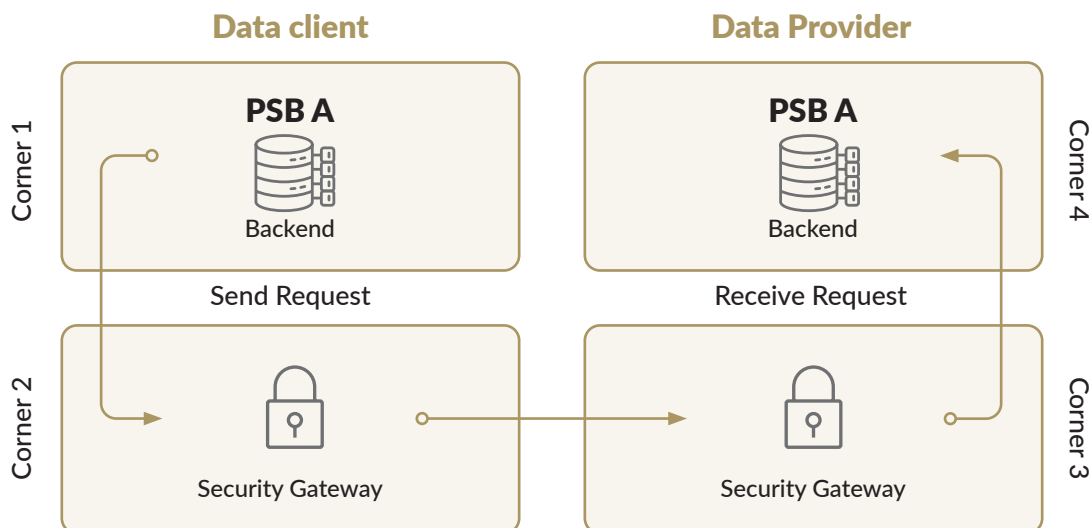
- ▶ Eliminates risk of single point of failure
- ▶ Eliminates risk of service provider lock-in

Con:

- ▶ Need to enhance security between security gateways
- ▶ Need to conform to common message exchange protocol

In comparison to the two- and three-corner models the four-corner model allows users to easily and safely exchange data even if their IT systems were developed independently from each other. Hence the four-corner model has become a proven model for the sharing of personal data across domains, e.g. as the reference model for the EU CEF eDelivery Building Block. If the 4-corner model is built on open standards, there is no risk for vendor lock-in (e.g. Govstack, X-Road, AS4, Peppol etc.) and thrives as a trust-enabled network of PSBs.

In a four-corner model, there are access points or security gateways, managed by a PSB, that manage access to their own backends. Sharing data is based on data sharing agreements and respective Service Level Agreements between a data provider and a data client. The security and regulations around the security gateways would be enforced by a central entity managing the data sharing infrastructure, hence creating a trusted



- Ministerial Foreword
- Introduction
- Glossary
- Scope and Audience
- The Once-Only Principle
- Data Sharing and Standards Framework Layers
- Data Sharing Principles
- Layers and Actions
- Appendix

data sharing framework, where any member of the infrastructure can rely on the truthfulness and authenticity of any other security gateway.

Security Gateways would also:

- ▶ Make sure transactions are digitally signed.
- ▶ Check trustworthiness of source.
- ▶ Check if there’s an agreement in place between provider and client.
- ▶ Make use of verified trust service providers for time-stamping.
- ▶ Create access logs for both requests and received data.
- ▶ Be designated to specific PSBs.

Document History

Version	Date	Summary of Revision
v1.0 - Final Draft	04/11/2025	▶ As advised by the DGB and approved by MPER.





An Roinn Caiteachais Phoiblí Bonneagair
Athchóiriúcháin Seirbhíse Poiblí agus Dígitiúcháin
Department of Public Expenditure Infrastructure
Public Service Reform and Digitalisation

Tithe an Rialtas. Sráid Mhuirfean Uacht,
Baile Átha Cliath 2, D02 R583, Éire
Government Buildings, Upper Merrion Street,
Dublin 2, D02 R583, Ireland

T:+353 1 676 7571
@IRLDeptPer
www.gov.ie/per