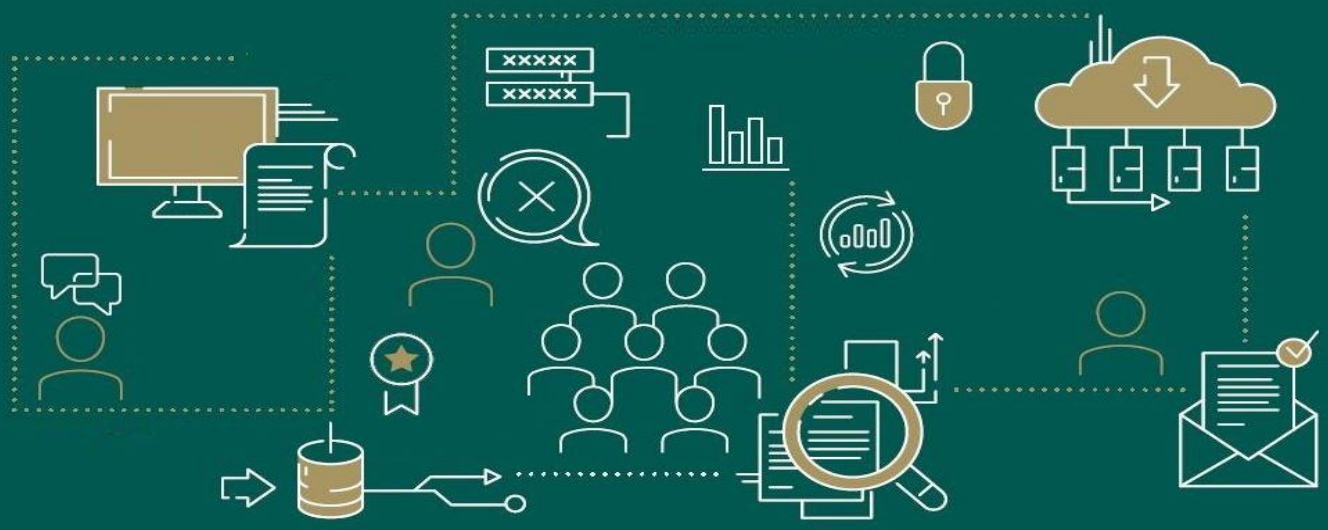
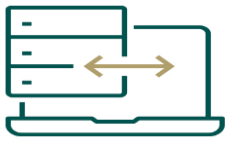
An Roinn Caiteachais
Phoiblí agus Athchóirithe
Department of Public
Expenditure and Reform

DSGA Data Sharing Guidelines

June 2022



Public Service Data Principles



Contents

1. Foreword

1.1 Ministerial Foreword

Data lies at the heart of Government - it informs decision making, shapes public policy, and is central to the delivery of public services. As our society evolves so too does the demand for better and more efficient use of data in the delivery of public policies and public services. In order to optimise the use of our data to meet this demand, Government has recently put in place a number of measures to improve public service data and its use;

- The Data Sharing and Governance Act
- The Public Service Data Strategy

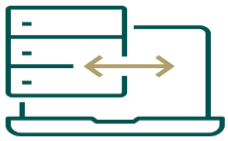
The Data Sharing and Governance Act (DSGA) is an enabling piece of legislation which will allow us to make advances in improving data management and data sharing in the Public Service. To complement this, the Public Service Data Strategy outlines a broad-based plan for data, including the implementation of the Act, and when put into practice, together, they will create a strong and supportive data ecosystem for the Public Service.

This Data Sharing Guideline builds upon the Data Sharing and Governance Act by setting out a common set of practices for all Public Bodies to follow when they wish to use the Act as their legal basis for sharing data.

This first step is one of many that are required to transform how data is accessed, collected, stored and transferred across all Public Bodies. Collectively we can improve how organisations engage with each other and how the general public perceive the Government's handling of their data. This work is not only highly anticipated but will be valued for generations to come.

Public Bodies must share the responsibilities to improve how we use data in the services we provide.

Michael McGrath TD
Minister for Public Expenditure and Reform



2. Introduction

The Data Sharing and Governance Act 2019 (DSGA) provides for the regulation of information sharing, including personal data, between Public Service Bodies (PSBs); the management of information by PSBs; the establishment of base registries; the collection of public service information; and the establishment of the Data Governance Board.

The DSGA provides a statutory basis on which public bodies can share personal data in the context of providing public services. It will ensure the safe handling of that data through an appropriate governance framework and gives transparency to the data sharing agreements in place.

These Guidelines set out the new governance framework for data sharing under the DSGA. An infographic of these guidelines, the **DSGA Data Sharing Playbook** (the Playbook), has been developed and can be viewed online. The Playbook is essentially a flowchart that navigates the stages of personal data sharing. The stages are sequential and must be followed in order to adhere to the DSGA and the processes of the data sharing governance framework. Each stage is mapped out in these guidelines to ensure organisations understand the process along with their roles and responsibilities.

These guidelines should be used where Public Service Bodies want to leverage the DSGA as their legal basis for sharing personal data.

The new data sharing governance framework, alongside good communications between PSBs, will ensure consistent, transparent and trusted data sharing across the public service.

2.1 What information should I consider before following these guidelines?

Before a Data Sharing Agreement (DSA) can be put in place there are a number of prerequisites that must be considered and met. Knowing these upfront and assessing if a PSB meets the requirements are essential - see **Section 3.1** of this document for details.

TABLE OF USEFUL TERMS

To ensure the terminology used through this document is clear, a list of commonly used terms is provided for users of this guide to familiarise themselves with.

Term	Explanation
Authorised Signatory	A senior official who signs the DSA and who is accountable for the data sharing within a PSB.
Business Unit	An area of the organisation that is involved in the disclosing or receiving of the data.
Data Governance Board ("The Board")	The Data Governance Board was established after the enactment of **S.9** 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 will review every DSA submitted and may make recommendations in relation to a DSA. All recommendations must be addressed by the PSBs involved before the agreement can be executed. More information on the Board can be found at; **Data Governance Board**.
Data Governance Unit (DGU)	The Data Governance Unit (DGU) in The Office of Government Chief Information Officer (OGCIO) has a range of responsibilities in relation to the Act. These include publishing the essential content (e.g. DSA & DPO Statements) at public consultation stage and collating public comments; publishing the essential content (e.g. DSA, DPO Statements & the Board's recommendations) online once the DSA has been executed; and, acting as the secretariat for the Board and the Data Sharing Committee. Contact details: datagovernance@per.gov.ie
Data Officer	The Data Officers are the officials from each PSB that serve as the main contacts throughout the data sharing process and for the lifetime of the DSA. It is the Lead PSB's Data Officer's responsibility to prepare and submit the DSA to the Other PSB's Data Officer and the Data Governance Unit.
Data Sharing	Data sharing is defined in the DSGA as the disclosure of information, including personal data, by a public body to another public body but only when the data concerned has been lawfully obtained and held by the disclosing public body. Personal data sharing must only be carried out in accordance with the provision of the Act.
Data Sharing Committee ("DS Committee")	The Data Sharing Committee is a committee that has been established by the Board. This specialist committee will review all DSA's and advise the Board of their findings.

Disclosing PSB	PSB sharing data with the recipient PSB. The data in question must be data that is legally obtained by the disclosing PSB.
DPER	**Department of Public Expenditure and Reform**
DPO	Data Protection Officer. The DPO is required to review the data sharing agreement for their organisation and sign a DPO Statement, before public consultation and at execution stage. They must ensure they are satisfied that they have reviewed the agreement, that it is compliant with Data Protection law and that the DSA is consistent with the principles of GDPR.
DSA	**Data Sharing Agreement**. This is a document that must be completed when following the process outlined in this guide.
Lead PSB	The PSB who prepares the DSA. The Lead PSB is the Lead Agency. The functions of the 'Lead Agency' are set out in subsections.18(2), 18(3), 21(3), 21(5), 22(1), 55(3), 56(1), 56(2), 57(4), 58, 60(1) and 60(4) of the Act**.**
Minister	For the purpose of this document Minister refers to the Minister for Public Expenditure and Reform.
OGCIO	**Office of the Government Chief Information Officer**
Other PSB	The PSB which is the other party/parties to the DSA agreement. An agreement can have more than two parties.
PSB	Public Service Body. The definition of a Public Body in this context can be found in **S.10** of the Data Sharing and Governance Act.
Recipient PSB	PSB wishing to obtain data from another PSB. The recipient PSB is the party or parties receiving data.
The Data Sharing and Governance Act ("The Act") DSGA	**The Data Sharing and Governance Act 2019** was enacted on 4 March 2019. The Act comes on foot of the **GDPR** and **Data Protection Act 2018** in order to clarify the legality of data sharing between public bodies and to introduce data governance within the Public Service on a statutory footing.

3. What are the data sharing stages?

3.1 Stage One – Data Sharing Preparation

Summary of stage One

- PSB identifies the need for data to be shared. In the majority of cases the Recipient PSB will identify the data required.
- In order for a Data Sharing Agreement to be considered in line with the DSGA there are 3 prerequisites that must be adhered to:
    - Can the data be sourced?
    - Ensure its only PSB-PSB sharing
    - Ensure the disclosing PSB has a legal basis to collect the personal data

PREREQUISITES

IDENTIFYING THE DATA

The PSB first identifies a need to have data shared with their organisation. In order to identify the data they can:

- Confirm if the data is held by another PSB; this can be facilitated by contacting the PSB directly or consulting the **Public Service Data Catalogue**.
- Check if an existing Data Sharing Agreement is in place by reviewing published Data sharing Agreements on the Data Governance Board website.

PSB- PSB SHARING

The data must be shared only between Public Bodies as defined in the **DSGA**.

LEGAL BASIS FOR COLLECTION

There must be a legal basis for the disclosing PSB to collect the personal data.

EXAMINING THE PREREQUISITES

In order for a Data Sharing Agreement to be considered in line with the Data Sharing and Governance Act the following prerequisites must be adhered to:

Pre-Requisite	Pre-Req Met
Does the data exist?	✓
Will the sharing of this data align with the definition of data sharing in the Act? • Data sharing is defined as the disclosure of information, including personal data, by a public service body to another public service body.	✓
Will the data sharing be from PSB to PSB?	✓
Is there a legal basis for the Disclosing PSB to collect this data in its own right?	✓
Confirm there is no other specific legal provision that allows for the sharing of this data outside of the Data Sharing and Governance Act? Note: s38 of the Data Protection Act 2018 will no longer provide a legal basis for personal data sharing data after 31st March 2022.	✓

Note: ***All*** pre-requisites ***must*** be met for a Data Sharing Agreement to proceed any further.

FINAL REVIEW AT STAGE ONE

Check whether a specific legal provision other than the Data Sharing and Governance Act provides for the sharing of that data e.g. Social Welfare and Consolidation Act 2005 (ss265-270). Check that the data can be lawfully shared using the Data Sharing and Governance Act 2019. Validate that the data is required for the purpose of a function. Ensure that the personal data being processed is proportionate, relevant but limited[1].

Public bodies have a duty to act in accordance with the law. Sharing personal data without a lawful basis is contrary to GDPR and could result in enforcement action by the Data Protection Commissioner, or in legal action by persons affected[2]. Consideration should be given if the data sharing arrangement "is likely to result in a high risk to the rights and freedoms of natural persons" then a Data Protection Impact Assessment (DPIA)[3] must be completed to support the data sharing arrangement. For further information please consult **www.dataprotection.ie**

[1] GDPR principle for data minimisation – only ask for what you need. https://gdpr-info.eu/art-5-gdpr/

[2] https://www.dataprotection.ie/en/dpc-guidance/blogs/right-compensation-and-liability

[3] DPIA - https://gdpr.eu/data-protection-impact-assessment-template/
https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

3.2 Stage Two – Data Officers' Review (All PSBs)

Summary of stage two

Communication

- The Data Officers from the PSBs involved should agree that the requested data is data that can be shared. Communication between the Data Officers of the PSBs is essential.

Consensus

- Once a consensus has been reached the Data Officers from PSBs involved inform their relevant stakeholders (authorised signatory and DPO) about the proposed DSA, who is involved and who will take on the role of Lead PSB.
  The Lead PSB Data Officer informs the Board of the same, along with any special public consultation requirements using the **Notification Template** available for download from the OGCIO website.

DATA OFFICERS DECISION

The Data Officers from the PSB's meet to review and agree:

- What data can be shared?
- What data cannot be shared?

The Data Officers from each PSB should agree that the requested data is data that, in accordance with the Data Sharing and Governance Act (DSGA), can be shared.

At this time, the Data Officer should consult with the Data Protection Officer to be advised if a Data Protection Impact Assessment (DPIA) is required. This will allow you to consider if the introduction of this data sharing process will pose a sufficiently high risk to the rights and freedoms of the individuals.

HOW DOES THE DSGA DEFINE DATA SHARING?

Data sharing is defined in the DSGA as the disclosure of information, including personal data, by a public body to another public body but only when the data concerned has been lawfully obtained and held by the disclosing public body. In order to have the legal protection of the DSGA, data sharing must only be carried out in accordance with the provisions of the Act.

Under the DSGA a reference to the key word "person" includes a deceased person and a reference to personal data also includes personal data of a deceased person.

ARE THERE ANY CATEGORIES OF DATA EXCLUDED?

Yes. The Act does not apply to the sharing of special categories of data defined as:

- racial or ethnic origin data
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data
- sexual orientation

This definition relates to Article 9 of GDPR[4].

Section 5 of the Act does not apply to special categories of personal data, except in relation to the Personal Data Access Portal and administration of a Public Service Pension scheme or actuarial valuation of Public Service Pension Scheme (see sections 5, 8 and chapter 3 of part 9). Chapter 2 of the Data Protection Act 2018 also provides a legal basis for sharing special categories of personal data in certain circumstances.

WHEN CAN PERSONAL DATA BE SHARED UNDER THE DSGA?

A public body may disclose personal data (including personal data of deceased persons) other than special categories of personal data (as referred to Article 9(1) of the GDPR) to another public body in the following circumstances, see table 2.0 below.

Circumstances	Share
Where required to do so by a direction of the Minister of Public Expenditure and Reform under s.14 of the DSGA;	✓
Where it is necessary and proportionate to do so for the purpose of performing a function of either public body, <u>and for at least one of the following purposes</u>: • to verify the identity of a person, in connection with the provision of services to that person • to identify and correct erroneous information held by either public body	✓

[4]GDPR Processing of special categories of personal data https://gdpr-info.eu/art-9-gdpr/

- to avoid a financial or administrative burden that would otherwise be imposed on a person in connection with the provision of services to that person
- to establish a person's entitlement to the provision of a service
- to facilitate the administration, supervision and control of a service, programme or policy being delivered by or on behalf of either public body
- to facilitate the improvement or targeting of such a service, programme or policy
- to enable to evaluation, oversight or review of such a service, programme or policy
- to facilitate analysis of the structure, functions, resources and service delivery methods of either public body

Table 2.0

Importantly, personal data may only be shared in the manner set out above, if:

a) the provisions of the General Data Protection Regulation ("GDPR") are respected; and
b) a data sharing agreement is put in place between the public bodies. This agreement is subject to public consultation and review and approval by the Board, which will be outlined later in this document.

The Minister may also direct a public body to disclose certain information to another public body and request personal and non-personal data from public bodies for public pension-related purposes.

WHEN CAN PERSONAL DATA NOT BE SHARED UNDER THE DSGA?

A Data Sharing Agreement between public bodies under the DSGA is not an appropriate legal basis for sharing data for the following purposes, see table 2.1 below.

Purpose	Share
Where a legal basis for sharing the data exists in other legislation, as for example in the Social Welfare Consolidation Act 2005, sections 265-270.	✘
The internal administration of either public body, including that relating to the employment of the data subject.	✘
The prevention, detection or investigation of offences.	✘
The apprehension or prosecution of offenders.	✘
The imposition or execution of a fine or sentence of imprisonment.	✘
The exercise of the functions of the Criminal Assets Bureau.	✘
Protecting the security of the State, including, but not limited to, the following: i. preventing, detecting and investigating offences under the Offences against the State Acts 1939 to 1998, the Criminal Law Act 1976 , the Criminal Justice (Terrorist Offences) Act 2005 and the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 ; ii. protecting the State from— a. espionage, b. sabotage, c. unlawful acts that subvert or undermine, or are intended to subvert or undermine, parliamentary democracy or the institutions of the State, and d. acts of foreign interference that are, or are intended to be, detrimental to the interests of the State and are clandestine or deceptive or involve a threat to any person, whether directed from, or committed or intended to be committed within, the State or not,	✘
Identifying foreign capabilities, intentions or activities that impact the international or economic well-being of the State.	✘
Co-operating with authorities in other states and international organisations aimed at preserving international peace, public order and security.	✘
The defence of the State, or	✘
The international relations of the State.	✘

Table 2.1

CONSENSUS REACHED AT DATA OFFICERS REVIEW

Once a consensus has been reached the Data Officers from the PSBs involved inform their relevant stakeholders about the proposed DSA, who is involved and who will take on the role of Lead PSB. This includes the authorised signatory, the security specialist and the DPO. The Lead PSB informs the Board of same, by emailing dgbsecretariat@per.gov.ie along with any special public consultation requirements. A **Notification Template** has been prepared that includes sections that must be completed and sent to the Data Governance Board secretariat as part of this process.

The Secretariat will confirm receipt of the DSA notification by email to the Lead PSB Data Officer. They will advise all Board members of the proposed DSA and any specific public consultation requirements.

The Lead PSB will have responsibility for managing communications and engagement for the data sharing arrangement that each DSA relates to. This includes managing stakeholder or interest groups where they have special public consultation requirements.

3.3 Stage Three – Preparing the Data Sharing Agreement (Lead PSB)

Summary of stage three

- A DSA is prepared by the Lead PSB's Data Officer (see "**Completing the DSA**" for more information on this).
- It is then reviewed by the Lead PSB's DPO.
- The DSA is then sent to the Other PSB's Data Officer(s) for completion.
- A security specialist from the Lead PSB and Other PSBs involved should review the DSA and their advice should be taken into consideration.
- The Other PSB's DPO will then review it and if they are happy with the DSA they will sign a DPO Statement. The Data Protection Officer (DPO) from each PSB is required to review the DSA for compliance and to sign a DPO Statement. The Data Officer will then formally issue the completed DSA back to the Lead PSB Data Officer.
- The Lead PSB Data Officer will send the DSA to their DPO for a final review before signing their DPO statement. The DSA is now ready for public consultation.
- The Lead PSB Data Officer will then send the DSA, which includes all relevant DPO Statements, to the Data Governance Unit in the OGCIO, consultations.dsa@per.gov.ie, who will publish online at for public consultation.

DEVELOPING THE DSA FOR PUBLIC CONSULTATION

Once the PSB Data Officer's review is complete and there is agreement in principle that data sharing could take place, the Lead PSB prepares the DSA by filling in the **DSGA Data Sharing Agreement template** available on the **OGCIO** website. See "**Completing the DSA**" section of this chapter for more information on this.

The Lead PSB's Data Officer prepares the DSA and their DPO will review it before sending to the Other PSBs for completion. All sections of the DSA must be completed.

Once the DSA is complete, including the signed DPO statements and the completed Admin section (which will not be published), the Lead PSB Data Officer will send a copy of the DSA (including DPO Statements and DPIA summary where one was carried out) to the Data Governance Unit (DGU) at consultations.dsa@per.gov.ie. The DGU will assist with the public consultation process. The DGU will acknowledge receipt of the email and do a preliminary quality check to ensure all sections are completed, and ready for public consultation.

WHAT INFORMATION WILL BE REQUIRED IN THE DSA?

The DSA sets out the information that PSBs need to know to ensure that data sharing is possible and that it will be executed and governed in a secure manner together with any conditions that specifically relate to the arrangement. The topics covered should include:

DSA Content	
Names of PSBs involved (Lead PSB and Other PSBs involved)	☑
The data to be shared	☑
The functions of the PSBs	☑
The purpose of the data sharing agreement	☑
The legal basis for the data sharing and for any further processing	☑
The motivation(impetus) of the data sharing – data subject or a public body	☑
The frequency e.g. once off or ongoing basis	☑
Defining the categories of data subject - individual or classes of data subjects	☑
The security measures – transmission, storage and accessibility	☑
Retention of the data shared and data resulting from the processing of the data sharing agreement	☑
Methods used to destroy the data shared and the data resulting from the processing of the data sharing agreement	☑
Subsequent use of the data - how the information will be processed	☑
Any restrictions on sharing information after processing	☑
An undertaking by the PSBs for compliance with data sharing and Article 5 of the GDPR	☑
DPIA – Checklist to ensure understanding for the requirement of a DPIA. A Summary of DPIA carried out or reasons why there is no DPIA	☑
Withdrawal procedure	☑
Schedules summarising the necessity for performance of the PSB and a schedule summarising the appropriate safeguards.	☑
Other additional information that is unique to that DSA	☑
Administration section for the Data Governance Board (this section will not be published online)	☑

The **DSA template**, when published and available to all PSBs, ensures that compliance with all relevant data protection legislation is addressed. No sections of the DSA template may be removed; however, new sections can be added.

All parts of the **DSA template**, along with DPO Statements and the DPIA section, must be completed before submission for public consultation.

Refer to Part 3 **S.13** Subsection 2 (C) and Part 4 **S.16** of the DSGA for further information.

WILL A DATA PROTECTION IMPACT ASSESSMENT HAVE TO BE COMPLETED?

If the data sharing arrangement "is likely to result in a high risk to the rights and freedoms of natural persons" then a Data Protection Impact Assessment (DPIA)[5] must be completed to support the data sharing arrangement. Note also the DPIA may inform several sections of the Data Sharing Agreement.

Section 1 of the DSA template comprises of an evaluation process for a DPIA. It includes a checklist to help identify whether a DPIA is required. The questions must be answered in relation to the entire project that the data share corresponds to.

Where a DPIA has been carried out in relation to the data sharing proposed, a summary of the matters referred to in Article 35(7) of the GDPR must be included in section 16 of the DSA template. This summary should contain:

DSA Content	
A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;	✓
An assessment of the necessity and proportionality of the processing operations in relation to the purposes;	✓
An assessment of the risks to the rights and freedoms of data subjects;	✓
The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	✓

[5] DPIA - https://gdpr.eu/data-protection-impact-assessment-template/
https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

Where no DPIA has been carried out in relation to the processing proposed to be undertaken under the proposed agreement, a summary of the reasons why no data protection impact assessment has been carried out must be included in the DSA.

Note: If the DSA is amended to reflect a change in the scope, form or content of the data processing, then there is an obligation on the data controllers to consider whether the changes give rise to a high risk to the rights and freedoms of natural persons, such that a DPIA should be carried out. Under S.20 (4) of Data Sharing and Governance Act, a draft amendment agreement must be submitted for review to the Data Governance Board in accordance with Part 9, Chapter 2 of the Data Sharing and Governance Act.

Further information in relation to DPIAs please consult **www.dataprotection.ie**

COMPLETING THE DSGA DATA SHARING AGREEMENT(DSA) TEMPLATE

INTERPRETATION

The definition and meaning for terms used throughout the **DSA template** are called out in this table. This table gives the user an understanding of specific terms that are used in the DSA to ensure there is no ambiguity and to ensure, for those that are not familiar with the terms, there is a plain English definition.

DSA PARTIES

The role of Lead Agency for the purpose of the Data Sharing Agreement is recorded here. The name and registered address of the Lead Agency (PSB) and the name(s) and registered addresses of the Other Parties (PSBs) are filled out on this section.

At stage 2 of the Playbook process you will have determined who takes on the role of the Lead PSB and what Other PSBs (in DSA terms the PSBs are the “Other Parties”) are involved. It is important to provide clarity about who is taking on the role of the Lead PSB and who else is involved, this section informs us of the relevant factual information regarding parties involved.

The Lead PSB is either the controller or in a joint processor arrangement they must be a nominated controller.

PERFORMANCE OF A FUNCTION

Where a PSB discloses personal data to another PSB under the DSA, it should be for the purpose of the performance of a function of the PSBs, and for one or more of the eight purposes called out in a table that you will need to select.

This table includes eight purposes that are taken straight from the Act and you must choose at least one.

DETAILS ABOUT THE PURPOSE

This section is where you will give sufficient background information to demonstrate how the sharing of data meets one or more the purposes that you have already identified in the performance of a function section.

The DSGA does not specify the scope or the level of detail you are required to fill in here but what is required is that you provide enough information to assure the Board that you have a legitimate purpose for data sharing. It should be understandable to the Data Governance Board and have a meaningful connection to the data being shared. In this way the Data Governance Board can deliver in its governance capacity.

DETAIL OF THE INFORMATION TO BE DISCLOSED

This section is where you will provide details of the personal data set to be disclosed and the detail of any non-personal data. This is the exact data set that will be disclosed and only information filled into this field will be allowed to be disclosed as part of this agreement. It is advised that you set out the minimum needed for the purposes of the agreement. The detail of information to be disclosed should be good quality data, accurate and kept up-to-date.

Non-personal data is data that originally did not relate to an identified or identifiable natural person. Anonymised personal data is not personal data in GDPR terms. If you have anonymised data that the person can be identified then its personal data. If you require clarification on personal data/non-personal data it is a matter of GDPR and we advise you to consult with your Data Protection Officer (DPO).

Note: If the non-personal data and personal data are linked together to the extent that the non-personal data becomes capable of identifying a data subject then the data protection rights and obligations arising under the GDPR will apply fully to the whole mixed dataset, even if the personal data represents a small part of the set. Therefore the whole dataset in this case is personal data.

FUNCTIONS OF THE PARTIES

This section is where you will specify the functions of the disclosing PSB and the receiving PSBs to which the purpose (identified in section 2.3 of the DSA) relates. For multiple PSBs involved you should insert new rows below and insert the name and the function for all PSBs involved.

LEGAL GROUNDS

This section is broken up into two parts, the legal grounds or the legal basis for the data sharing and for any further processing of the information shared. Legal basis will always be in the GDPR but the domestic legislative provisions giving you (the PSBs) your legal obligation (task in the public interest) will also need to be set out.

The first part asks you to define the legislative provisions for the sharing of the data and the second part asks you to specify the legislative provisions for further processing.

Legal grounds are highlighted and you will have to choose one of these and delete the one not relevant to the DSA.

i. processing is necessary for compliance with a legal obligation to which the controller is subject; (GDPR Art 6. 1 (c))
ii. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e))

Where the legal basis lies in the exercise of official authority vested in the controller (GDPR Art. 6(1)(c)(e)), include reference to relevant legislative provisions as appropriate.

Legal Provisions means all statutes, laws, ordinances, rules, regulations, judgments, orders and decrees of any Governmental Entity. A provision of an Act or instrument is any words or anything else that forms part of the Act or instrument for example provisions consisting of groups of words like sections, subsections, paragraphs, subparagraphs, sub-subparagraphs along with chapters, parts, divisions, subdivisions, schedules.

IMPETUS FOR DATA SHARING

The term impetus means "something that makes a process or activity happen" which in terms of the DSA is the motivation. This section requires you to specify the primary motivation for the data sharing agreement, where the benefits can be realised in relation to the data shared under this agreement. Is it for the 'Data Subject' or for the 'Public Body' or both? Tick which is most appropriate to the data sharing agreement.

CATEGORIES FOR DATA SHARED

The personal data shared may be in relation to individual data subjects and/or classes of data subjects. The term 'data subject' refers to any living individual whose personal data is collected, held or processed by an organisation. The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons.

Examples of classes of data subject are customers, employees, vendors, suppliers, visitors. Using customers as an example, your organisation is likely to have internal and external customers and hold personal data on each customer e.g. Personal Email Address, Work Email Address, etc. Social Network Information – Facebook Identifier, Twitter Address, LinkedIn identifier, etc. Account Information – Details of your customer's account ids or user ids. Job Information – Company Name, Department Name, Job Title, etc. As it is likely that you process the personal data of your customers in a similar way, i.e. using similar types of personal data for similar purposes. If such is the case, it makes sense to group them together in one category called customers.

The DSA includes a tick box where you can choose between individual and classes of data subject. There is a comment section where you can provide details of either.

Note: **Aggregated data** is information gathered and expressed in a summary form for purposes such as statistical analysis and is not the same as classes of data subject.

DURATION

This section of the DSA allows you to define the start and end dates (if required) for the disclosure of the information in the agreement. Fill in the most appropriate for your agreement and delete all other options available.

FREQUENCY

This section of the DSA allows you to indicate the type of transfer whether it is once off, an ongoing or regular or another type of frequency and it includes a description section where you can explain briefly what this frequency will entail. It is used to determine how often the transfer will be made.

DESCRIPTION OF PROCESSING

Each PSB should ensure that it processes the shared personal data fairly and lawfully. Each will comply with the requirements of the Data Protection Act 2018, GDPR and any legislation amending or extending same, in relation to the data exchanged.

Processing means using personal data in any way, including; collecting, storing, retrieving, consulting, disclosing or sharing with someone else, erasing, or destroying personal data. Each PSB undertakes to comply with the principles relating to the processing of personal data as set out in Article 5 GDPR, in the disclosing of information under the DSA.

Include a description of how the disclosed information will be processed by each receiving party.

FURTHER PROCESSING

Further processing of personal data means the processing of personal data for a purpose other than that for which they were initially collected. Although the principle of 'purpose limitation', set out in Article 5(1)(b) GDPR, does require that personal data is collected for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes', there are limited cases in which '**further processing**' of personal data for purposes other than those for which the personal data were initially collected should be allowed. This is only possible where the processing is 'compatible' with the purposes for which the personal data were initially collected. A **Guidance Note** has been published by the Data Protection Commissioner that goes into more detail on further processing.

RESTRICTIONS

This section of the DSA asks you to identify or state any restrictions the disclosing PSB places on the disclosure of information after the processing by the receiving PSBs. Once you have specified the restrictions if any, which apply to the further disclosure of the information, you should provide a description of them.

SECURITY MEASURES

Under this section of the DSA a number of key security measures of the DSA are explained before the parties starts to fill in the table provided. The PSBs receiving the data agree, in accordance Article 32 of the GDPR, to implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data transmitted, stored or otherwise processed.

All PSBs involved will need to ensure that the security standards appropriate to the transfer of personal data under the agreement are adhered to. The PSBs receiving data will need to ensure that all persons who have access to and who process the personal data are obliged to keep the personal data confidential and that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data. All

PSBs will keep the data secure and ensure that it is transferred securely in accordance with the procedures of the agreement.

There is a responsibility on the Lead PSB/disclosing PSB and the Other PSBs involved to fill in their appropriate table and particular regard should be given to the data safeguards outlined.

The Lead PSB/disclosing PSB is required to declare if they comply or do not comply with a statement regarding the encryptions services used in the transmission of the data and to give details. They then have to outline the security measures in place for the transmission of this data without compromising those security measures. To complete their part of this section they must answer 'Yes/No' to whether their security specialist has reviewed and the advice they have given has been considered when completing this section ensuring the security expert opinion has been giving before proceeding.

The Other PSBs are required to declare if they comply with a number of security statements regarding the storage and accessing of the data that is being shared and to provide details that do not compromise those measures in place. They too are required to answer whether their security specialist has reviewed the DSA and the advice has been considered. This table must be replicated and completed by each PSB receiving the data.

Note: If a personal data breach occurs after the data is transmitted to the PSBs receiving data, the PSBs receiving data will act in accordance with the **Data Protection Commission's Breach Notification Process** and in accordance with **GDPR requirements**.

RETENTION

Data retention is the continued storage of an organisation's data for compliance or business reasons. The GDPR does not specify time limits for retention. However, the general principle is that data should only be kept for as long as it is needed.

In the **DSA template** you are required to define the retention requirements for the disclosed information for the duration of the Data Sharing Agreement and in the event the agreement is terminated, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

METHODS USED TO DESTROY/DELETE DATA

Deletion methods are not prescribed under the DSGA or even under the GDPR. A safe deletion mechanism should be used, due to the requirements outlined under security measures and safeguarding of data by design and by default.

Detail how information will be destroyed or deleted at the end of the retention period as defined in the DSA, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

WITHDRAWAL

Each Party commits to giving a minimum of 90 days' notice of its intention to withdraw from or terminate this Data Sharing Agreement. As this is a template agreement the number of days can be decided upon by the PSBs involved, it is editable for that purpose.

OTHER MATTERS

Any other relevant matters to the DSA can be included in this area of the DSA. An editable section is created, if this is not required you can delete this section.

SCHEDULE A

Data Protection Impact Assessments (DPIA) can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect your organisation or the individuals it engages with. Under the GDPR, DPIAs will be mandatory for any new high risk processing projects.

If a data protection impact assessment (DPIA) has been conducted in respect of the data sharing to which this Data Sharing Agreement relates, a summary of the matters referred to in Article 35(7) of the GDPR is required to be filled in the table provided.

OR

If a data protection impact assessment has not been conducted as it is not mandatory where processing is not "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35 of the GDPR), outline the reasons for that decision in the table provided.

SCHEDULE B

Outline the reasons why the disclosure of information under the DSA is necessary for the performance of the relevant function and explain why it is proportionate in that context.

Summarise the extent to which the safeguards applicable to the data shared under this agreement are proportionate, having regard to the performance of functions by the PSBs involved and the effects of the disclosure on the rights of the data subjects concerned.

SCHEDULE C

Set out the names of all the Parties to the agreement.

As required under **s.21**(3)(a), (b) and (c) of the Data Sharing and Governance Act 2019, this Schedule must be updated by the Lead PSB to include any PSBs who have joined the agreement by way of an Accession Agreement, and to remove any PSB that has withdrawn from the agreement. The Lead PSB must notify the other PSBs of any amendments to this Schedule and the Data Governance Board.

AUTHORISED SIGNATORY

An authorised signatory is required to sign this Data Sharing Agreement after all recommendations made by the Data Governance Board have been addressed and before the Data Sharing Agreement can be executed.
This signatory has the role of accountability for the data sharing defined in the DSA and holds the post of Principal Officer (equivalent) or above.
The PSBs agree to their obligations pursuant to the DSA for the transfer of personal data as described in the Data Sharing Agreement.

DATA PROTECTION OFFICERS STATEMENT

This Statement is separate to the Data Sharing Agreement. It is required by law under **S.55**(1)(d) of the Data Sharing and Governance Act 2019. The Data Protection Officers in each PSB must sign and complete this statement before the Data Sharing Agreement is submitted to the Data Governance Unit for Public Consultation and again at execution stage. This statement will be published, as part of the DSA, on a public website.

The Data Protection Officers in each PSB must ensure that they:

i. have reviewed the proposed agreement, and
ii. are satisfied that compliance by the proposed PSBs with the terms of the proposed agreement would not result in a contravention of data protection law,
iii. are satisfied that the agreement is consistent with Article 5(1) of the GDPR

DATA GOVERNANCE BOARD ADMINISTRATION SECTION

The Admin section will be used for administrative purposes by the Data Governance Unit, the Data Governance Board and its committees.

Note: This section is not published.

ACCESSION AGREEMENT

Ideally, all PSBs involved in the data sharing agreement should sign up to the DSA on the date of its execution (the effective date). If it is not possible to do so on this date, an Accession Agreement can be created but will only be to the DSA in its original form. If different terms are required, a creation of a separate DSA will be necessary.

The **DSGA Accession Agreement template** is available for download from the **OGCIO** website.

3.4 Stage Four – Public Consultation (28 Days)

Summary of stage four

- The Lead PSB Data Officer is responsible for sending the essential content (including DPO Statements and DPIA summary where one was carried out) to the Data Governance Unit (DGU) who will format the document and issue back a PDF version ready for publication. The Lead PSB will then publish the PDF version of the DSA online on the consultations hub **https://www.gov.ie/consultations/DSA/**
- The Data Governance Board has defined the Public Consultation period as **28 days**, therefore once published it will expire after 28 days.
- All PSBs must communicate with any special interest groups they have outlined in their stage 2 notification. This may direct them to the public consultation hub or provide more information on the data share.
- All PSBs must publish, on the same date as the consultation, a notice on their website that they are intending to enter into the proposed DSA. They should state where the relevant public consultations is available online and publish a copy of the DSA on their website. This notice should invite submissions and include the date of publication of the notice.
- The Lead PSB Data Officer will notify the Board about these publications by emailing the secretariat.
- The DGU will be checking if any submissions are made, on a regular basis, if there are submissions they will compile them all and feed them back to the relevant Data Officers from the PSBs involved. If there are no submissions the DGU will notify the relevant Data Officers about this and send the DSA to the Board for review.

WHAT HAPPENS AT PUBLIC CONSULTATION STAGE?

Once the DSA and DPO Statements progress to stage four they must be made available for public consultation. The DGU will ensure all Data Officers have a copy of the **Public Consultation Notice template** for their Notice to include on their website. The Lead PSB will confirm that the DSA has been published on the gov.ie consultations page. The Lead PSB will confirm publication and advise the DGU and all relevant Other PSB Data Officers by email that consultation is 'live' on a specified date. The DGU will update their **master list of public consultations** with a link to the newly published consultation. The DSA will be open for public feedback for a period of 28 days as specified by the Data Governance Board.

The DGU will monitor consultation submissions received into consultations.dsa@per.gov.ie. The DGU will collate submissions regularly and send them to the Lead PSB Data Officer. Once the consultation period expires (after 28 days) the DGU will send the final collated

submissions to the Lead PSB Data Officer. If there are no submissions the DGU will notify the Lead PSB about this and send the DSA to the Board for review.

All PSBs Data Officers will publish a notice on their website (on the same date as the consultation) that they are proposing to enter into the DSA. A **Public Consultation Notice template** has been created which lists details of all information that must be provided. They should state where the relevant public consultation is available online and state the documents that are accessible to the public and publish a copy of the DSA (including DPO statements & DPIA section) on their website. This notice should invite submissions and include the date of publication of the notice.

The Lead PSB Data Officer will publish a notice on their website as described above and notify the Board once everything has been published by all PSBs involved, by emailing dgbsecretariat@per.gov.ie.

EXAMINING PUBLIC CONSULTATION REQUIREMENTS FOR PSBS

Public Consultation	Checklist
Has the DSA been completed and sent to DGU?	☑
Has the DGU notified all PSBs involved that the consultation is live and provided the relevant link?	☑
Have all PSBs published a Notice, as per the **Public Consultation Notice template** (provided above) on their website?	☑
Have all PSBs published a copy of the DSA on their website?	☑
Has the Lead PSB notified the Board that the DSA is live and all Notices are published?	☑

3.5 Stage Five – PSBs Review (21 Days)

Summary of stage five

- The Data Governance Unit will compile submissions and issue them to the Data Officers in each PSB.
- Following receipt of any submissions made, the Data Officers can then coordinate with relevant stakeholders in the PSBs. They must review the feedback and decide if the DSA should be amended.
- Data Officers may be required to update the DSA based on the decision made.
- The Lead PSB has a maximum of 21days (from the date of public consultation closing) to submit the following to the Board:
    - Copy of the DSA (with amendments, where applicable)
    - Relevant DPO statements (included in the DSA)
    - DPIA summary, where one has been carried out (included in the DSA)
    - Any information that the Board may require regarding submissions made through the public consultation process

WHAT SHOULD PSBS DO WHEN THEY RECEIVE SUBMISSIONS?

Once the public consultation period has closed all submissions will be compiled by the DGU and issued to each PSB's Data Officer. PSBs will review and consult for any amendments that may be required.

The Lead PSB has 21days (from the date of public consultation closing) to submit the following to the Board:

- Copy of the DSA (with amendments, where applicable)
- Relevant DPO statements (included in the DSA)
- DPIA summary, where one has been carried out (included in the DSA)
- Any information that the Board may require regarding submissions made through the public consultation process

It is recommended that the Lead PSB creates a summary of any changes made to the DSA on foot of public consultation and include this summary with the relevant documentation for the Board.

- If the PSBs decide that no amendments are required, based on the submissions made, then the DSA is sent directly to the Board for review by emailing dgbsecretariat@per.gov.ie.
- In the event of no public feedback to Public Consultation the DSA is sent directly to the Board by the DGU for review

Note: Only submissions recieved to the public consultation published email address consultations.dsa@per.gov.ie will be accepted ie. if submissions go directly to any PSB they cannot be included.

Table 3.5.1 below outlines the possible scenarios and actions required.

Public Consultation Feedback	Amendments Requested	Amendments Required	Action
Submissions	*N*	*N*	DGU sends DSA (including DPO Statements) directly to the Board for review
Submissions	*Y*	*N*	Lead PSB Data Officer sends all relevant information to the Board for review and includes reasons why DSA was not amended. – within 21 days
Submissions	*Y*	*Y*	Lead PSB amends the DSA; Lead PSB sends amended DSA, a summary of the changes made and all relevant information to the Board for review within the specified timeframe – 21 days

Table 3.5.1

3.6 Stage Six – Data Governance Board Review

Summary of stage six

- The Board's review may involve seeking information from the Lead PSB Data Officer and they may also consult with relevant Ministers.
- The Board will seek appropriate advice from their Data Sharing Committee and may seek further advice from other established Committees.
- The DS Committee will review all DSAs and advise the Board of their findings.
- Other relevant Committees will advise the Board on any aspect of the DSA as requested.
- Once the Board has completed their review and if substantive issues arise in their recommendations, a further review will be requested by the Board.
- If no further review is required by the Board, they will issue their recommendations to the Lead PSB Data Officer to be addressed.

The Data Governance Board may request information regarding the public consultation feedback from the Lead PSB. The Data Governance Board may consult with Ministers of Government when reviewing the DSA.

The Data Sharing Committee is a committee formed by the Data Governance Board to undertake the review process of all DSA's. The Data Sharing Committee will advise the Data Governance Board on compliance in all aspects of best practice, ethics, standards and guidelines for data sharing. The Board may seek further advice from other established Committees. Other relevant Committees will advise the Board on any aspect of the DSA as requested.

The Data Sharing Committee will report their findings to the Data Governance Board.

Once the Board has completed their review, they may make recommendations, all of which must be addressed by the PSBs before the DSA can be executed.

Where the Data Governance Board is of the view that its recommendations concern substantive issues, a further review is necessary. In this case the recommendations for amendment will be issued back to the Lead PSB Data Officer and, once amended, the DSA will be sent back to the Board for further review.

If no further review is required by the Data Governance Board, they will issue their recommendations to the Lead PSB to be addressed.

3.7 Stage Seven – PSBs Address Recommendations & Sign

Summary of stage seven

- The PSBs address the Data Governance Board's recommendations;
- PSBs DPO's sign DPO statement once they have completed their review and they are satisfied with compliance to Data Protection law and that the DSA is consistent with GDPR.
- The DSA is completed on signing by Authorised Signatories (PSBs);
- If there are amendments that contain substantive issues the amendments will be made and sent back to the Board for further review.
- PSBs may seek clarification from the Board on their recommendations.
- The PSBs must ensure that all recommendations made by the Board are addressed, only then can the DSA be executed.
- Once all recommendations have been addressed the DSA will then be signed by the each PSB's authorised signatories and the DPO will update their DPO Statement by signing and dating it.

DPO is required to review the Data Sharing Agreement for their organisation and sign and date an updated DPO Statement before it can be executed. They must ensure they are satisfied with compliance to Data Protection law and that the DSA is consistent with GDPR. When this and all other necessary steps are completed, a senior official (Authorised Signatory) who is accountable for the data sharing within each PSB involved, will review and complete this stage by signing the DSA.

Note: The DSA will be deemed to be executable once:

a. The Data Governance Board does not specify any recommendations.
or
b. The recommendations from the Data Governance Board do not contain substantive issues.
c. The PSBs involved are satisfied that all recommendations have been addressed and the authorised signatories will then sign the DSA.
d. DPOs update and sign DPO Statement ensuring they are satisfied that the DSA is compliant with Data Protection law and GDPR.

3.8 Stage Eight – Publication

Summary of stage eight

- The Lead PSB's Data Officer will be responsible for sending the final executed DSA to the Minister (DGU) within the specified time (10 days).
- The DGU, on behalf of the Minister, will publish a list of documents the Minister has received.
- The Lead PSB will be responsible for publishing the final executed DSA on their website.
- The Board will publish the executed DSA and their recommendations on their website.

The Lead PSB's Data Officer will be responsible for sending the final executed DSA to the Minister. This must be done within 10 days of the date of execution. The Lead PSB will be responsible for publishing the final executed DSA on their website.

The Data Governance Unit, on behalf of the Minister, will publish a list of documents the Minister has received.

The Data Governance Board is responsible for publishing a copy of the DSA and their recommendations on their website.

Note: **S.61 of the DSGA.** The effective date of the DSA is the date of its publication (by the Lead PSB).

3.9 Stage Nine – DSA Implementation

Summary of stage nine

- The Lead PSB's Data Officer will be responsible for informing the Data Governance Board of any changes to the Data Sharing Agreement during the lifetime of the agreement.

The Lead PSB's Data Officer will be responsible for informing the Data Governance Board of any changes to the Data Sharing Agreement during the lifetime of the agreement. This includes any new PSBs joining the DSA by way of Accession Agreement or any changes in the terms of the DSA.

The PSBs involved in the Data Sharing Agreement will review the operation of the agreement on a regular basis that is not more than 5 years from the effective date. The Lead PSB will publish a copy of the conclusions of the review on a website maintained by it or on its behalf.

Revision History

Version	Date	Revision Summary
DRAFT	02/08/2021	Substantial DRAFT prepared for ratification
v.1.0	28/10/2021	Adding section “Completing DSA”
V2.0	22/12/2021	Version complete and ready for publishing
V2.1	20/06/2021	Updates to Stage 2, Stage3, Stage 4 and Stage 8