Rialtas na hÉireann
Government of Ireland

PUBLIC SERVICE DATA STRATEGY 2019 – 2023

Office of the Government Chief Information Officer
Department of Public Expenditure and Reform

Contents

Foreword

I am delighted to publish the first Data Strategy for the Public Service. Data lies at the heart of Government, it drives decision making, shapes public policy, and is central to the delivery of public services. As our society evolves so too does the demand for improved public services. The strategy sets out a vision, along with a set of actions, on how we can improve our use of data to support a more joined-up, efficient and effective Government. It aims to put in place a series of measures to improve how data is governed, managed and re-used in a secure, efficient and transparent manner across the whole of Government for the benefit of citizens and businesses.

The strategy's implementation will put Government in a better place to respond to service demands, providing joined-up and integrated services, reducing administrative burdens, better protection of personal data, and improving the process of policy formulation and evaluation.

The strategy builds upon the forthcoming Data Sharing and Governance Bill. In order to improve Government data, its treatment, and its reuse, the Data Sharing and Governance Bill will put in place a legal framework for the safe and secure sharing of data across Government. This is complimented by a wide range of governance and transparency measures to ensure that all data sharing is done in an appropriate manner.

In order to deliver efficient and effective public services, the same data should not have to be collected over and over again, this is costly and cumbersome for citizens, businesses and public bodies alike. Public Service bodies should be able to work together for the benefit of citizens and businesses.

In October 2017 Ireland signed up to the Tallinn Declaration on eGovernment, which contains the once-only principle. The once-only principle outlines that public bodies should collect data once, and only once from citizens and businesses, and reuse that data as opposed to recollecting it. The benefits of adopting this approach are numerous, and both the Data Sharing and Governance Bill and this strategy drive Ireland further along this path.

I am excited about the direction and ambitious nature of this strategy. It aims to bring about real change and improvements in how we deliver public services. I look forward to seeing the benefits and positive outcomes that its implementation will deliver.

Patrick O'Donovan T.D.
Minister of State at the Department of Finance and the Department of Public Expenditure and Reform with special responsibility for Public Procurement, Open Government and eGovernment

1

Executive Summary

Data lies at the heart of Government, informs and drives public policy, is collected and consumed by Public Service bodies (PSBs) and is central to the delivery of public services. In order to optimise the use of our data throughout its lifecycle, and ensure it is appropriately protected, a Public Service data strategy is required.

While there are many examples of good data management practice throughout the Public Service, data is frequently collected and managed in an independent manner. This approach has commonly been adopted in order to serve specific needs and to comply with legislative obligations, though has resulted in a somewhat fragmented whole-of-Government data ecosystem. These practices can result in increased administrative burdens, reduced data driven policy making, difficulties in introducing joined-up digital services, and reduced Government agility in responding to today's challenges.

By building on the good data management practices already employed by some PSBs, adopting a more consistent and uniform approach to data across Government, and enabling the secure reuse of data and services, a well-functioning whole-of-Government data ecosystem can emerge to better serve its citizens and businesses.

This strategy describes a data ecosystem, including associated governance, for the optimisation of data management within Government. It sets out a single narrative paving the way to an integrated approach to the improved use of data, particularly across PSB boundaries. This approach will result in benefits across both the strategic and operational use of data. Such benefits include:

- More joined-up end-to-end digital services
- Better analytics driven data insights leading to improved policy formulation
- Reduced administration by cutting the need to provide the same data over and over again
- Improved agility by securely and efficiently reusing data
- Improved protection and transparency of the way data is used throughout its lifecycle
- Better services and policy through improved data quality

The strategy builds upon existing data initiatives

such as the National Data Infrastructure (NDI), which primarily concerns the identification of people, businesses and location; and the Data Sharing and Governance Bill (DSGB), which sets out a legal framework for the sharing and governance of data across Government. The strategy illustrates how these work together, along with appropriate governance, processes and systems, to create a cohesive ecosystem.

This strategy first sets out a vision for data management within Government and includes a set of guiding principles to assist PSBs in aligning with the vision. The strategy proceeds to detail a set of strategic themes and supporting actions that will build incrementally to a target state data ecosystem. The ecosystem is comprised of the following primary characteristics.

- A strong emphasis on supporting data controllers in meeting their obligations under the GDPR and other legislation while safely allowing citizens, businesses and PSBs to get appropriate access to the data that Government holds
- Standards and good governance processes will ensure that data is managed appropriately and consistently across all PSBs, maintaining trust with Government
- Security and data protection measures to identify and protect citizen and business data, for example, privacy-by-design and privacy-by-default, will be adopted
- Co-ordinated approach, including shared systems and processes, moving us to a consistent method of publishing and collecting data digitally
- Shared platform to support the secure, transparent and controlled reuse of data across PSBs will be introduced. These technologies will focus on APIs as the primary enabler for data reuse. APIs (Application Programming Interface) are a modern best-practice machine-to-machine mechanism to facilitate technical interoperability, supporting controlled service and data access
- Base registries (single authoritative sources of data) will enable data to be reused, and reduce the need for citizens and businesses to provide the same information to PSBs again and again
- Privacy, security and transparency systems and processes empowering people to see what data Government holds on them and how they are being processed. These will be instrumental in fostering trust between the various actors in the ecosystem
- A structured approach to open data and cross-departmental analytics is central to the promoting the value of data, the generation of data-driven insights and delivery of evidence based decision making

Informed by exemplar implementations in Europe, such as Estonia and Denmark, and aligning with best-practice recommendations from the EU, OECD and the World Bank, the target state data ecosystem envisioned by this strategy requires a whole-of-government approach, where PSBs will cooperate and reuse data and services in an effective, secure and consistent way using API-led technologies.

The Public Service Data Strategy is a comprehensive multi-year, multi-department strategy that sets out a series of ambitious goals and actions to deliver on a target state data ecosystem for Government. It sets our "North Star" to start moving towards incrementally. Although covering four years, this strategy sets out some long-term actions which will take well beyond the lifetime of this strategy to fully realise.

Delivery of the strategy will be modular and incremental, with each action delivering its own value and progressively adding to the data ecosystem. Many of these actions are already underway in some form and this strategy seeks to build upon what is already in place within PSBs. Delivery of the strategy will require a sustained investment and commitment across Government.

2

Introduction

2.1 Context and relevant strategies

Public Service data, as a service-wide cross cutting concern, would benefit from being examined and dealt with in a unified and consistent manner. Across PSB boundaries, data sources are often independent and lack harmonisation and consistency, frequently making it diffi cult to accurately and reliably reuse data for new administrative and statistical purposes.

Better treatment of data, through standardised data management practices, advocating data reuse over data collection, promotion of cross-agency data-sharing underpinned by a clear legal basis and driven by improved effi ciencies for citizens and businesses is central to the solution of these challenges.

A number of recently published Government strategies call for improvements in the management of data as a key enabler to delivering effi cient and effective public services and policy making. These strategies include:

- The Public Service ICT Strategy includes a Data as an Enable strategic pillar calling for the improved management of data across the Public Service supporting better administration and decision making.
- The eGovernment Strategy 2017-2020 sets out a vision that utilises technology to improve citizen and business interactions with Government through better digital and data usage, improved capabilities, and enhanced governance.
- The National Statistics Board's Strategy 2015-2020 outlines the importance of joined-up data for joined-up Government. It describes how the ability to make successful national policy decisions and to be accountable to citizens can be enhanced by the increased availability, breadth and quality of information, evidence and insight.
- Our Public Service 2020 includes an action to "Optimise the use of data" – outlining how data will support better service delivery, better decision making, increase the ease of access to services and drive efficiencies.

The cohesive approach to Public Service data as outlined in this Strategy aligns well with the forthcoming National Digital Strategy, which is currently in development. The National Digital Strategy will set out a clear long-term vision and high-level ambition for how Ireland can best respond to digitisation, which will rely heavily on the effective management of data.

The move towards better data management practices and regulated data-sharing is also prevalent amongst EU bodies and global organisations advocating a whole-of-Government approach:

- Principle 7 of the OECD's 12 principles of digital Government strategies states that Governments should develop common policies and standards and drive the adoption of national interoperability frameworks for data exchange.
- The EU's Tallinn declaration of Oct 2017 states that we should take steps to create a culture of re-use, including responsible and transparent re-use of data within our administrations.
- The EU's European Interoperability Framework (EIF) outlines the objective of "Promoting seamless services and data flows for European public administrations". The aim of the EIF is to inspire European public administrations in their efforts to design and deliver seamless European Public Services to other public administrations, citizens and businesses.
- The European Commission's Digital Agenda, in pursuit of a Digital Single Market, lists 2 key pillars - enhancing interoperability and standards, and strengthening online trust and security.
- The UN advocates that Governments can contribute to policy integration and integrated service delivery by regulating data sharing and promoting data standards that make sharing more effective.

European exemplars like Denmark, Norway and Estonia have prioritised data initiatives such as adherence to "Once only" and "Privacy by design" principles; focusing on good governance and effective legislation enforcing inter-agency data-sharing; and implementation of key enablers such as base registries, e-Identifi ers, and a core interoperability platform.

This strategy recognises the signifi cant opportunities to be gained by improving the treatment of data held by the Public Service in a holistic manner. It sets out a detailed vision, and complementary action points, for developing an improved and coherent data management ecosystem within Government.

2.2 Data Management Landscape in the Public Service Today

Across the Public Service, there are many examples of good data management practices being employed in individual PSBs. However, as a whole-of-Government cross cutting concern, data is not being examined and dealt with in a unifi ed and consistent manner. Data, in order to comply with legislation, is often maintained in silos, where it is collected and stored for the needs of the individual PSBs. There are benefi ts to these practices, as is evident by the safe, secure delivery of specifi c public services – but it also results in ineffi ciencies such as the potential duplication of data being stored and collected by different PSBs, bespoke bi-lateral data-sharing agreements between PSBs, and a reduction in data quality.

The overall result is a sub-optimal whole-of-Government ecosystem where data is governed and managed by the policies of individual PSBs, and not easily reused to deliver joined up services or assist policy making and evaluation. In order to improve the various forms of data reuse, a greater degree of standardisation in terms of systems, policies and practices is required. The good practices being employed by PSBs should serve as the foundation for building a more co-ordinated, consistent approach to data management in a whole-of-Government manner.

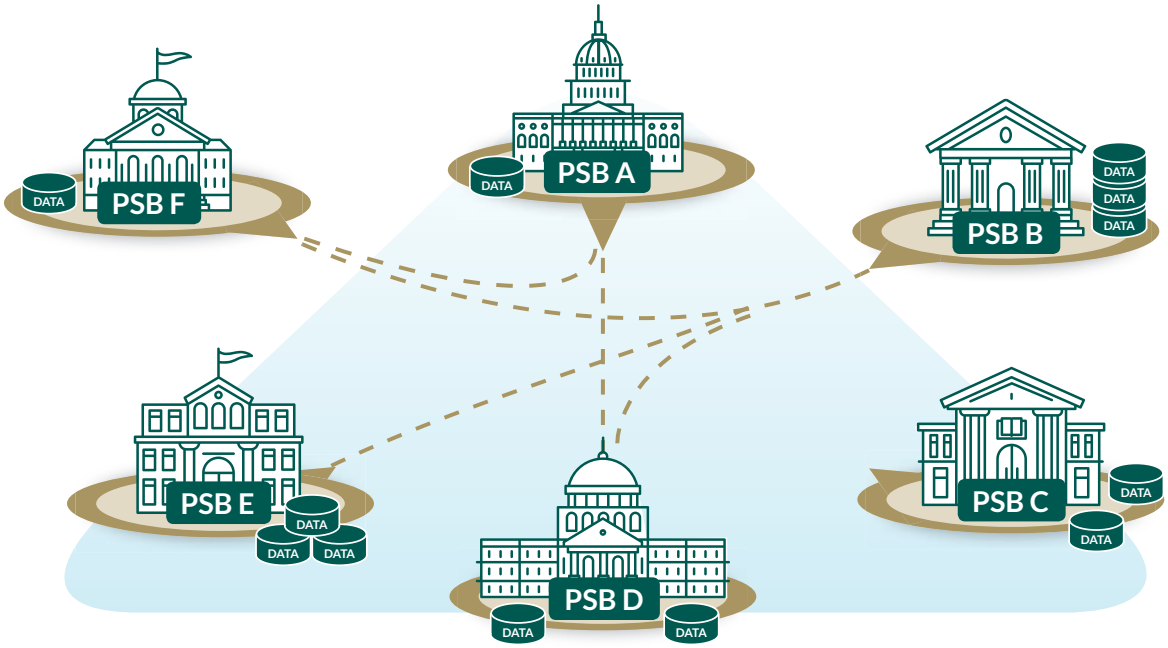


Figure 1: As-Is Data Management Landscape in the Public Service Today

While the above may paint a challenging picture of a largely un-coordinated data management landscape in existence today, there are many good examples of outcome driven sharing of data and services between PSBs such as:

	MyGovID, the Government's citizen identity verification service, being used by many PSBs to access and deliver a growing number of services online
	The Local Property Tax register reusing data from various internal and external sources
	Real-time data sharing between a number of PSBs supporting SUSI in efficiently processing student grant applications
	Education reports providing insight into graduate destinations and earnings using data from the HEA, Revenue and DEASP
	The Job Seeker Longitudinal Dataset combines income, claims and training data to produce a uniquely detailed view of the Irish labour market for policy creation and evaluation
	Companies Registration Office providing controlled access to its data via APIs to various PSBs
	The HSE Healthlink project facilitating the secure transmission of clinical patient information between Hospitals, Health Care Agencies and GPs

Equally, there are many examples today where challenges exist for citizens, businesses, and PSBs alike due to inconsistent treatment of data and the lack of systems integration and a pan-agency interoperability platform. Such examples include:

- Separate online customer registration systems and processes that are at odds with the once-only principle
- Cross-agency customer data matching issues
- Manual processes due to the lack of real-time interfaces
- Re-collection of data already captured by separate agencies slowing down service delivery.

Government have taken steps to address some of these challenges by embarking on the National Data Infrastructure (NDI), which concerns itself with the consistent and reliable identification of data that relates to a particular location – through the use of an Eircode; person – through the use of a PPSN; business – through the use of a Unique Business Identifier (UBI). The consistent identification of these core data assets is crucial to successfully linking data, joining up government, and delivering integrated services.

To further assist in resolving these challenges, the Data Sharing and Governance Bill (DSGB) seeks to provide a legal basis to enable PSBs - where they already have a legal basis to collect data from the citizen or business directly, to collect that data from another PSB. This aligns with the once-only principle of collecting data once from citizens and businesses, and reusing data as opposed to recollecting.

This Data Strategy sets the NDI and the DSGB in the wider context of building a coherent data management ecosystem for the Public Service. It seeks to remedy the aforementioned challenges with current data initiatives in the Public Service today by bringing about a unified approach to how such data initiatives are devised and implemented. To support this cohesion, this data strategy sets out an overarching vision and provides a set of principles, themes and actions guiding the management, governance, architecture, and re-use of data in a secure, open and transparent way.

3

Vision

"To establish a data ecosystem that will improve how we govern, manage and re-use data in a secure, efficient, and transparent way, for the benefit of citizens, businesses and policy makers".

Informed by the context already laid out and a strong belief that data is the lifeblood of digital transformation and decision making, the vision presented in this strategy seeks to improve the treatment of data held by the Public Service in a secure, open and transparent way for the benefit of citizens, businesses, and PSBs.

By taking a whole-of-system approach to data management within the Public Service the vision is to create a coherent ecosystem where PSBs can confidently exchange data to support improved service delivery and policy creation. The target data ecosystem described in this strategy ensures that data exchange is performed in a legal, transparent and effective manner.

3.1 Data Ecosystem

Delivering on this vision requires PSBs to adopt a holistic and cohesive approach to a target state data ecosystem replacing the largely un-coordinated data landscape in existence today.

Figure 2 illustrates a high level view of the target state data ecosystem supporting the once-only-principle. Key to achieving this target state is reducing the number of independent copies of data being collected and maintained by PSBs. Through the establishment of base registries, managed by the appropriate PSBs, authoritative sources of data will be created, facilitating efficient and legal reuse of data across the Public Service.

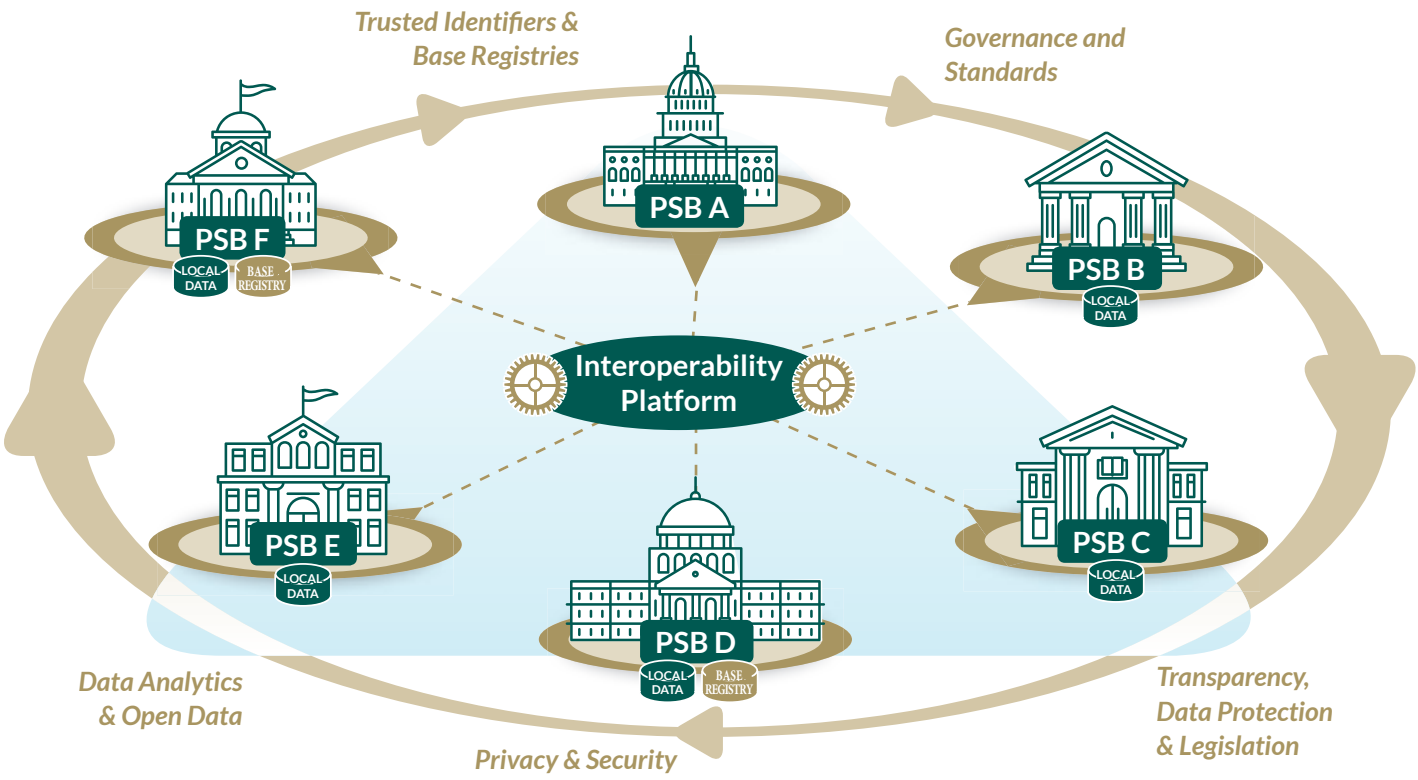


Figure 2: Target State Data Ecosystem for the Public Service

The implementation of base registries will reduce the need for citizens and businesses to provide the same information to PSBs again and again, and create the opportunity for PSBs to reuse data where appropriate. The reuse of data in this manner will assist PSBs in adopting end to end digital approaches to delivering joined-up services for the benefit of citizens and businesses.

To achieve this data ecosystem, and to facilitate the technical interoperability of PSBs, an interoperability platform will be established, providing a secure, reliable and consistent way for PSBs to reuse both data and services. The interoperability platform will form the backbone of machine to machine inter-Government communications – allowing PSBs to discover, manage, and deliver data and services for service delivery.

It is important to note that data and base registries will remain with PSBs, while the interoperability platform will be used to discover what data is available and facilitate its reuse, preventing duplication of effort, across PSBs.

By making the data available and reusable in this manner, complimented with good governance and strict controls, the interoperability platform will facilitate a structured approach to data access, which can be used for cross-departmental data analysis. This facility is central to the generation of data-driven insights, qualification of outcomes, and delivery of evidence based decision making across Government.

Data privacy and transparency are core components of our target state data ecosystem, whereby personal data processing follows a common set of standards and guidelines. Through the implementation of this strategy people will be able to find out what personal data Government holds on them, for what reason is it being held, and information as to how that data is processed.

This data ecosystem will be supported by legislation in conjunction with the necessary governance and controls, ensuring a whole-of-Government approach to data. Components, features and capabilities of the target ecosystem are summarised below.

- Sharing of personal data will be underpinned by clear and explicit legislation and governance to help foster trust between citizens and businesses, and Government

- Designated authoritative data stores, called base registries, will be established to promote the once-only principle and reduce PSB data holdings
- Transparency will be delivered through citizen accessible data-sharing agreements, a Data Portal for citizens to view personal data that Government holds, well-architected logging solutions, and the publication of open datasets
- An API-led Interoperability Platform based on a Service Oriented Architecture (SOA) will be developed to enable PSBs to cooperate, share and reuse data and services in an effective, secure and consistent way
- Driven by a privacy-by-design mind-set, robust data security solutions and processes will be implemented to help foster trust between the various actors in the ecosystem
- A structured approach to data analytics will be encouraged to promote the value of data to support evidence-based policy-making
- Trusted identifiers will enable data to be linked across data holdings
- Standards and good governance processes will be implemented to ensure that data is accessed, collected, stored, and transferred in a consistent and uniform manner by all PSBs

3.2 Benefits

As evidenced by the vision statement, while the primary beneficiaries of initiatives proposed in this strategy are citizens and businesses, there are also benefits to be realised for individual PSBs and for Government as a whole. The graphic below summarises the benefits that this strategy sets out to achieve through both data analytics, delivering insight and foresight, and through operational use of data.

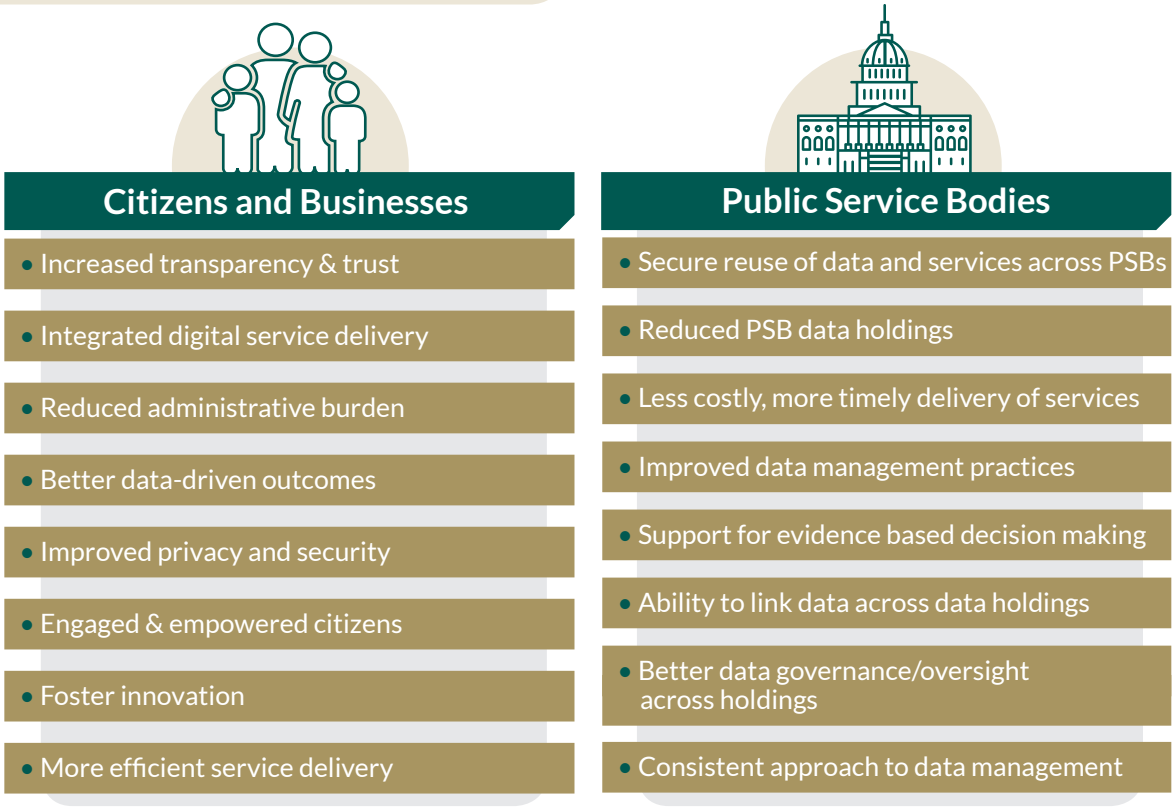


Figure 3: Benefits of the target data ecosystem for Citizens, Businesses and Government

4

Principles

The principles set forth below will help shape the evolution of a target state data ecosystem based on transparency, accessibility, and reusability, driven by the application of standards, trusted identifiers and secure interoperable solutions enabled by effective governance, and dealing with data protection as a cross cutting concern.

4.1 Data Transparency

Principle 1: Data is discoverable by citizens, businesses and the Public Service

Governments are increasingly collecting, storing and processing large volumes of data across the public sector through the provision of public services. In order for citizens, businesses and PSBs to leverage the benefits of data, it must be made discoverable, identifiable and understandable.

Making data and services more easily discoverable will increase knowledge of data and services held, and in turn facilitate reuse. To support this, where appropriate, Government must build and publish catalogues that enable interested parties to locate, understand and use the data and associated services.

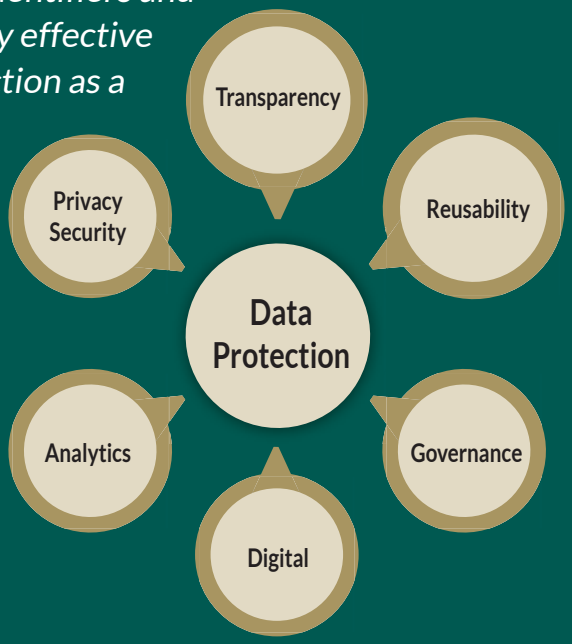


Figure 4: Data principles at a glance

Principle 2: Data is processed in a transparent manner

In order to provide the type of joined-up services and information/insight expected, Government not only requires data to be collected from citizens and businesses but

should where permitted share this data amongst PSBs in a secure and effi cient manner. While most users of Government services would welcome the introduction of such improved integration, it raises the question of trust with respect to processing of personal data.

To ensure data is processed in an appropriate manner throughout Government, personal data must be processed in a way that is transparent to citizens, providing a window into what data is held, shared and processed across the Public Service.

Principle 3: Data that can be made public should be made public

Openness and transparency is a key Government priority and the Open Data Strategy[1] contends that opening up Government data will empower citizens and businesses, foster innovation and reform Public Services.

In the spirit of openness and transparency, PSBs should catalogue and publish appropriate datasets where legally permissible, whilst taking into consideration Government's obligations to protect the confidentiality of citizens and businesses.

4.2 Data Reuse

Principle 4: Data is reusable

Data must be reusable by all actors in the ecosystem, in line with legislation, in order to deliver integrated services and insight with efficiency to businesses, citizens and policy makers.

Data reuse must respect data minimisation. Such reuse must adhere to a policy of "*assertion over access*", where reuse is in the form of making checks or queries on the status of data, only returning true or false responses. Where data access is required, the minimum amount of data is shared and held for the minimum amount of time required.

Implementing the Once-Only principle, by ensuring that citizens and businesses supply the same information only once, and reducing the number of independent copies of data held in the Public Service, will promote sharing and reuse of data and common services to improve service provision and decision making.

Through adherence to the once-only principle, use of base registries and removal of redundant or duplicate data sets, PSBs will only capture data that has not already been collected by the Public Service. This data will be reused as opposed to recollected where there is a legal basis to reuse it.

Principle 5: Data is accessed and maintained via base registries

The European Interoperability Framework describes base registries as "reliable sources of basic information on items such as persons, companies, vehicles... that are authentic and authoritative".

Implementing base registries of data that are reliable, transparent, timely, and of high quality, will establish authoritative single sources of truth, promote minimisation and facilitate reuse across PSBs and make it easier to audit data and its usage due to reduced data holdings.

Data that is already collected and stored in a base registry must be accessed and maintained by PSBs via that base registry. This will help reduce administrative burden on businesses and citizens having to resupply data and to reduce independent copies of data being held among PSBs.

Principle 6: Data is accessible through APIs to support interoperability

In order to deliver a joined-up Public Service, IT systems must facilitate technical interoperability - having the ability to connect to each other and speak the same language. APIs should be used to facilitate this interoperability. An API (Application Programming Interface) is a modern best-

1 https://www.per.gov.ie/wp-content/uploads/Draft-Open-Data-Strategy-2017-2022.pdf

practice machine-to-machine mechanism to facilitate technical interoperability, supporting service and data access.

The use of APIs enables PSBs to expose data and related services in a controlled and structured manner, supporting inter and intra PSB interoperability. This facilitates the delivery of joined up Public Services, and underpins the principles of reusability, transparency and discoverability. APIs will act as a key building block, upon which, the envisaged whole-of-Government ecosystem is built.

4.3 Data Governance and Controls

Principle 7: Data is demonstrably processed in line with legislation

Citizens and businesses must be confident that their interactions with Government are secure and in compliance with all relevant regulations. PSBs must ensure privacy and respect the confidentiality and integrity of the data by demonstrably processing data in line with legislation.

Personal data must be collected for specific, explicit and legitimate purposes only, and must not be further processed in way that is incompatible with those purposes. In order to demonstrate compliance, PSBs must make relevant audit data available to citizens and businesses to view.

The proposed Data-Sharing and Governance Bill is designed to protect citizen's privacy by establishing a prescriptive framework in legislation for governance, oversight and transparency of data processing within the Public Service. PSBs will process data in line with this Bill once enacted.

Principle 8: Data is effectively governed
Data must be effectively governed through a formal system of accountability, designed to enforce proper management of data assets and the performance of data-related functions.

Good data governance will be delivered through a whole-of-Government set of rules, standards, guides, tools, policies, procedures, roles and responsibilities that guide the overall management of Government data.

A Data Governance Board will be established to direct, oversee and drive data governance across the Public Service. Through good data governance, PSBs will ensure that their data are accurate, consistent, complete, available, discoverable and secure.

4.4 Digital

Principle 9: Data is collected and processed digitally
The benefits of a digital-first approach to Government services are well documented but much data is still collected and processed on handwritten and paper based forms or standalone electronic systems that do not improve downstream processes. PSBs need to adopt a digital-by-default strategy to realise improvements in data quality, timeliness, privacy controls, consistency and reduced citizen overhead.

PSBs must by default, collect data digitally at the first point of citizen and business engagement, not only with respect to transactional Government services but also for survey responses, statistical analysis, etc. Introduction of a modernised and extensible digital data collection platform for surveys by Government will assist PSBs in realising these benefits sooner.

4.5 Data Analytics

Principle 10: Data is used to support evidence-based decision making
Data is the foundation of decision making and the basis for accountability. In order to effect good policies and provide useful statistical insights, data must be used to support evidence based or informed decision making. Evidence-based decision making, whether by Government, business or the general public, is reliant on directly available quality data or insights derived through research.

The vision espoused in this strategy promotes better treatment of data through

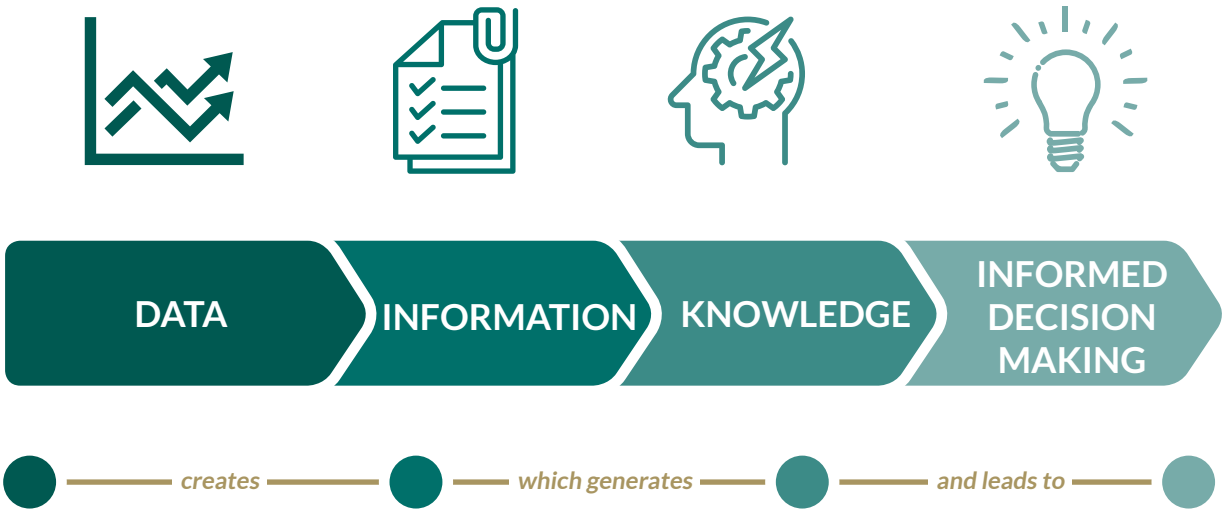


Figure 5: Data used to support evidence-based decision making

improved data management, governance and architecture, where quality data improves and feeds into evidence based decision making for the benefit of citizens, businesses and PSBs.

4.6 Data Privacy and Security

Principle 11: Data is processed in a secure and private manner

It is imperative that appropriate security measures are implemented to ensure data is protected to greatest extent possible. Personal data must be secured and protected from unauthorized internal or external access, modification or deletion, regardless of the intent and a clear approach defined for secure handling of this data.

By adopting a privacy-by-design mind set, robust data security solutions and processes will be implemented to help foster trust between the various actors in the ecosystem. By treating privacy as a design concern, rather than a regulatory or compliance burden, this will ensure that privacy is considered up-front and built into these solutions at design stage, to help alleviate privacy concerns and promote data protection compliance.

5 Strategic Themes

Realisation of the stated vision will be guided by the principles outlined above and a set of strategic themes that illustrates how Government will go about achieving this vision.

Each of the themes described have a strategic focus and include a set of defined actions to signal how we intend to manage, govern, architect, share and re-use data in a secure, efficient and transparent way.

5.1 Protection and Legislation

The protection of data is a pervasive theme and a cross-cutting concern throughout the Public Service. All processing of personal data, is subject to the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act of 2018. PSBs must adhere to these obligations, which spring from the core principles of data protection as listed in Article 5 of GDPR, summarised below.

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

In line with these principles and obligations, the proposed Data Sharing and Governance Bill makes the following strategic decisions in regards the introduction of national legislation to include the following:

- The sharing of personal data between PSBs is provided for with a clear and explicit legislative basis
- Strategic data management infrastructures and standards applying to the Public Service will be underpinned by legislation

- Governance controls and processes in relation to data management within the Public Service are to be put on a legislative footing.
- Transparency processes and obligations relating to personal data processing within the Public Service to be put on a legislative footing

Actions

- Complete the Data Sharing and Governance Bill and bring it into law
- Create a framework to support PSBs in sharing data in line with the Data Sharing and Governance Bill
- Each PSB that processes personal data will work with their Data Protection Officer to ensure their data processing practices are demonstrably in line with data protection legislation, including the assessment of risk associated with such processing as appropriate

5.2 Governance and Standards

Data governance with the appropriate standards and guidelines is necessary to build a system of accountability combined with proper management of data assets. Such governance and standards include rules, policies, procedures, roles, and guidelines, which combine to create an environment promoting data accuracy, consistency, completeness, availability, transparency and security.

It encompasses the people, processes, and technology used to ensure that key information delivered throughout the Public Service is appropriately defined, used and maintained in order to deliver integrated digital services for citizens and businesses. Effective governance and standards also underpins the right data being processed in the right way – a cornerstone of maintaining trust with Government.

Underlining its importance, the Public Service ICT strategy encourages PSBs to "recognise that the governance and management of data is critical to ensuring data quality, as is the implementation of the necessary infrastructure to allow sharing of data between PSBs".

Implementation of this strategy across the Public Service will include the introduction of a set of standards and guidelines, in line with GDPR Article 40, helping to drive a uniformity of approach to data management for all PSBs. Adoption and implementation of appropriate standards and guidelines will support the reuse of data, in line with legislation, in order to deliver joined up services, and support analysis for policy formation and evaluation.

A Data Governance Board will be established to formalise a long-term governance structure for the Public Service, through which the development and implementation of data management standards, guidelines and activities can be overseen. The board will also be responsible for promoting the compliance of PSBs with the introduced standards and guidelines.

Actions

- Establish a Data Governance Board to oversee and monitor data management practice within the Public Service with appropriate supports
- Define and publish a set of standards and guidelines, in line with GDPR Article 40, addressing areas of data management

5.3 Privacy and Security

The Data landscape is rapidly evolving with the proliferation of new and different kinds of threats emerging. Now, more than ever, governments must take actions to identify and protect the citizen and business data which they process.

By adopting a privacy-by-design mind-set, PSBs will implement robust data security solutions and processes that will help

foster trust between the various actors in the ecosystem. By treating privacy as a design concern, rather than a regulatory or compliance burden, we will ensure that privacy is considered up-front and built into systems at design stage.

GDPR establishes "privacy by design" and "privacy by default" in law and requires that systems take account of privacy and security considerations from the outset. While GDPR doesn't apply to all types of data, all citizen and business data of a sensitive or confidential nature, should also be subject to such considerations. Examples of these considerations are listed below.

- Policies, guidelines and procedures governing information security, both physical and electronic
- Privacy-by-design controls, e.g. least privileges basis.
- Data breach procedures
- Risk assessments
- Data protection roles
- User Access and Authentication Controls
- Appropriate virus-checking software and firewalls
- Backup and recovery policies to counter data loss, data corruption and data encryption
- Intrusion detection systems and procedures
- Logging and audit procedures

Implementing the appropriate controls which govern who can access data is at the heart of data security and privacy. A consistent and robust method for Identity and Access Management (IAM), authenticating users, should be employed across Government for access to data. PSBs should use the MyGovID service to protect online access to citizen data.

A planned initiative under this strategic theme is the implementation of Digital Postbox, a mechanism for secure delivery and storage of data. The Digital Postbox will over time support citizen access to all Government

communications in a single, safe and secure digital platform, and is designed to serve as an alternative to paper post for reasons of cost and efficiency. It is expected that PSBs will adopt the Digital Postbox as the default communication channel between Government and citizens, similar to EU exemplars like Denmark.

Actions

- Publish privacy-by-design and security guidelines for which PSBs must have regard, and apply in the context of public tenders
- PSBs to implement appropriate security and privacy measures to comply with Data Protection obligations
- PSBs should ensure that personal data is protected online at point of access and collection via the use of MyGovID
- Implement a secure cross-agency Digital Postbox solution

5.4 Digital Collection

As we strive to advance both the Government's digital agenda and introduce initiatives to improve the overall treatment of data, we must consider strategies to improve data collection and storage. In response, this strategy proposes the introduction of a modernised and extensible data collection platform, along with a concerted move to a digital-by-default data collection strategy.

A data collection platform will be established for use by PSBs for electronic and online surveys. The goal is to reduce respondent overhead for citizens and businesses in surveys suitable for online collection while providing a consistent approach to security and user interface. The platform must be designed for scalability, incorporating implementation of the Online Census.

PSBs will continue the move towards digital through online interactions with citizens and business. The development of self-service forms should be progressed by PSBs ensuring that data is collected from citizens and businesses in a digital manner. Such forms should support pre-population of data where appropriate. Opportunities for a shared service approach to the provision of online self-service forms should be considered.

UI/UX plays an important role in ensuring effective quality data collection at source, as does the adoption of a more consistent look and feel across Government services. To aid PSBs in access to UI/UX skills and resources, we will seek to establish a UI/UX procurement framework. To assist in building a more consistent look and feel for Government online, a UI/UX style guide will be considered.

Actions

- PSBs to adopt digital data collection as the default method of collection where appropriate, while exploring opportunities for a shared service approach
- Develop a secure platform for online surveys that has general applicability to multiple surveys and is capable of scaling to accommodate very large surveys, including the Census
- Establish a UI/UX procurement framework to assist PSBs in accessing UI/UX skills and consider establishing a Government UI/UX style guide for online content. This will help build a more consistent look and feel to Government online, including data collection and input forms
- Develop a platform for online self-service forms that meets the needs of PSBs seeking to collect non-complex data as part of an administrative process

5.5 Interoperability

Delivery of integrated digital Public Services requires PSBs to cooperate and reuse data and services in an effective, structured, consistent and transparent way. By embracing an API approach for Government, data and services can be exposed for reuse in a secure, consistent manner, leading to the delivery of more joined-up, efficient public services for citizens and businesses.

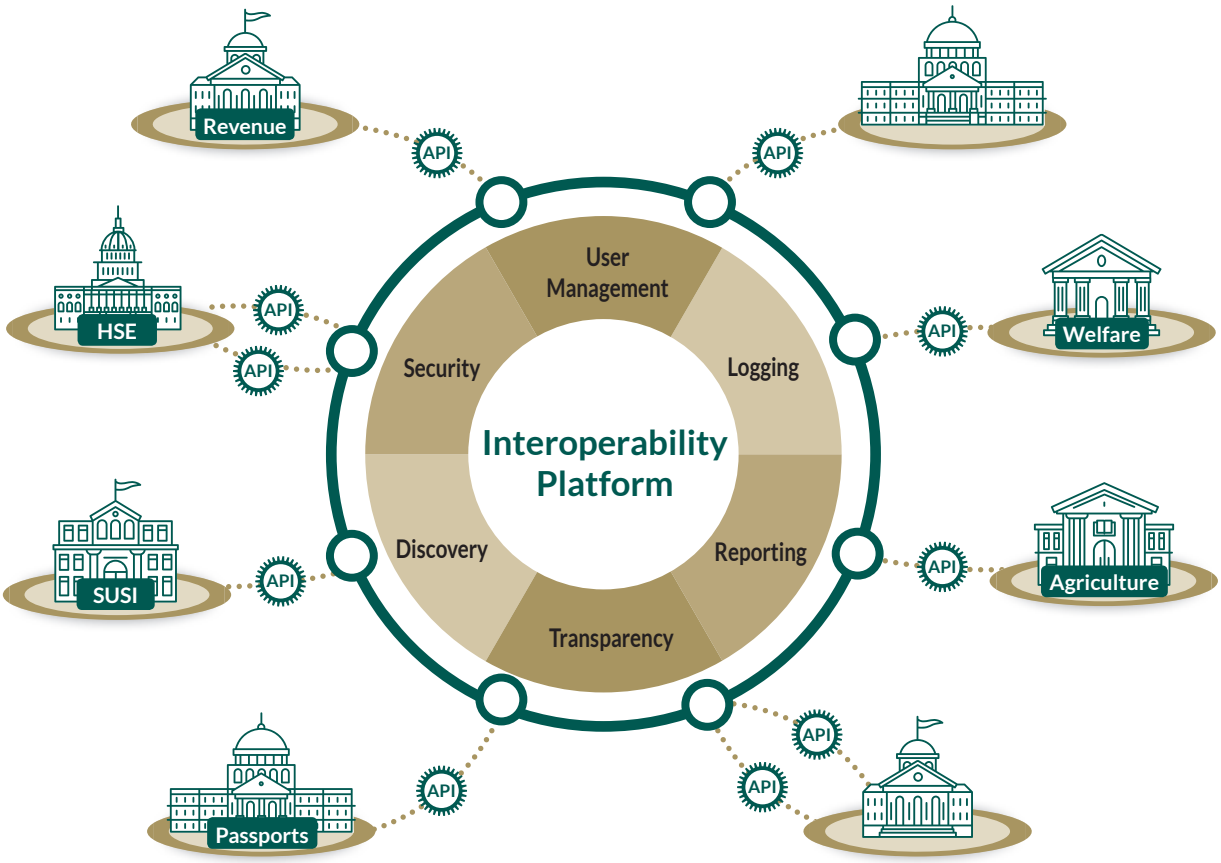


Figure 6: Interoperability Platform

The European Interoperability Framework (EIF) is defined as "an agreed approach to interoperability for organizations that wish to work together towards the joint delivery of Public Services…". The EIF promotes reusability as a driver for interoperability and includes elements such as integrated service delivery; reuse of data and services; catalogues describing reusable services; Governance; security and privacy.

Aligned with the EIF interoperability levels (legal, organisational, semantic and technical), we propose developing a Data Interoperability Platform that will be architected to promote reuse, where PSBs will share common data and services in a consistent and uniform manner. It will be designed as an API-led Service Oriented Architecture with APIs published to expose data and services within the Government ecosystem. The Interoperability Platform aims to achieve at least the following and will be guided by the success and learnings from similar platforms such as Estonia's X-Road and Altinn in Norway.

- Consistency of approach to technical measures employed to reuse data between PSBs
- Supports secure transport and authorised access to data for reuse
- Promote awareness and facilitate the discovery of data and services available for reuse via an API discovery portal
- Provide appropriate management plane to allow PSBs to monitor and control how their data is being used and manage the life cycle of their associated interface end-points
- Support API led service design for PSB data reuse, and become the default method of exposing APIs for PSB data and service exchange

The diagram above demonstrates how data and services will remain with PSBs, the interoperability platform, via the use of APIs, will be used to discover what data is available and facilitate its reuse, preventing duplication of effort across PSBs.

While there may be limited merit in implementing APIs for some legacy systems, all new systems should implement APIs by default. Furthermore, existing APIs should be considered for incorporation into the interoperability platform.

Actions

- Incrementally develop an Interoperability Platform and supporting guidelines and processes to support interoperability

5.6 Analytics

Analysis of data has enormous potential to improve the precision and outcome of policy formulation and decision making for Government. The opportunities for data analytics are growing both on the supply side (doing more with the growing volume of data) and the demand side (policy and operational questions and issues that data can help inform).

The availability of accurate and timely Government data, combined with a developed capability to analyse it, controlled by well-defined governance processes are central to the generation of data-driven insights, qualification of outcomes and delivery of evidence based decision making.

The supply side is driven by other aspects of this strategy document such as the Data Interoperability Platform, the establishment of Base Registers, Data Catalogues, and so on. The best practice architecture approach to facilitating the demand for analytics is a data warehouse (or data lake) which allows data to be processed without compromising operational systems. However, this type of approach is likely to result in concerns from citizens and data controllers regarding large amounts of data being held in a single location for potential rather than specific processing purposes.

Government proposes to take a more granular approach to establishing a platform for data analytics that balances better facilitation of analytics with the obligations of data controllers by implementing secure virtual "Data Rooms", based on similar CSO practices, as outlined below.

The Public Service Data Strategy is a comprehensive multi-year, multi-department strategy that sets out a series of ambitious goals and actions to deliver on a target state data ecosystem for Government.

- A requesting PSB obtains agreement from one or more PSBs to access and link their data for a specific and legitimate purpose
- A governance process reviews, and approves (or not) each of these data analysis projects, taking account of GDPR, Article 22.
- A dedicated virtual environment ("Data Room") will be created that contains the specific data requested and approved tools for its analysis. Data can be viewed and analysed, but data cannot be removed from the virtual data room.
- Access to the data room is strictly limited to authorised project personnel with all access logged for audit purposes. All data is read-only.
- A further governance process is needed to allow the Data Processor to obtain an actionable copy of the results of the analytics
- The contents of the data room and any physical copies of data in it are destroyed after the project concludes. The methodology (and associated code) used to create the data sets should be retained for future re-use.

The separation of data analytics from data engineering means that analysts are insulated from data security and access considerations and can focus on getting value from the data. This will make data analytics more accessible to smaller Departments and provide a better platform for services such as IGEES and statisticians seconded to Government Departments. The use of standard tooling will improve skill levels and make the quality of analytical outputs more consistent. It is anticipated that as this service grows there may be a requirement for a dedicated data engineering team.

Secure virtual Data Rooms require well-defined assets and processes governing their use including:

- Data catalogues to publish the data that is available with metadata
- Data Sharing Agreements to provide transparency over the use of the data
- A process to review and approve the output of the analysis executed on the data
- Output logs showing an audit of what data was accessed and by whom

It is also important for PSBs to embrace data visualisation tools and techniques as a means of analysing and presenting complex information in a way that is easier to visualise, grasp and understand. By presenting data as engaging, meaningful images, data visualisation can unearth 'stories' behind the information, to help drive policy development and citizen engagement. There are enormous opportunities for data visualisation techniques to provide cross-sectoral insights, highlight trends and patterns and derive additional value from the wealth of Public Sector data to be made available through the target state data ecosystem.

Actions

- Develop an analytics platform supporting secure virtual data rooms with a standard analytics and visualisation toolset, and governance process to facilitate cross-agency data analysis
- PSBs to adopt analytics and visualisation tools to ensure policy development can engage with available data in a meaningful and intuitive manner

5.7 Discovery

One of this strategy's objectives is to increase reuse of data for the benefit of citizens, businesses and policy makers. However basic it may seem, in order to reuse this data, one must have knowledge of that data in the first place. As the proliferation of Public Service data increases, so too does the challenge of discoverability, which determines the ability of a piece of content, information, or data to be found and accessed.

A data catalogue, which can be considered

a repository containing information on data holdings within an organisation, is a mechanism for making data discoverable. Catalogues are designed to help people find data and understand how such data can be used, typically including capabilities to register, classify, and detail the metadata describing the data holdings.

We will develop a Government data catalogue that will enable PSBs to list and describe their data holdings. This catalogue will contain a list of key data holdings for each PSB, in particular those pertaining to personal data and those critical for business decisions or service delivery, where appropriate. For each data holding, metadata will be detailed allowing people to ascertain the contents of the data holding, its purpose, scope, contact details, etc.

Such a catalogue is expected to not only be used to stimulate cross Government data awareness and reuse, but also for internal awareness and reuse within PSBs. Furthermore, a citizen view of the catalogue will support the measures outlined within the Transparency strategic theme of this strategy.

To compliment the catalogue we will also develop a pan-Government API portal that allows for the discovery of data and services that are available for use via a machine to machine mechanism. This API discovery portal is a key component of the Interoperability Platform, promoting an ecosystem where API interfaces are published, discovered and used.

Actions

- Develop a Government data catalogue, for internal and public use, cataloguing key data holdings within PSBs, supporting reuse and transparency
- Develop a Government API portal, as part of the Interoperability Platform, supporting the discovery of data and services that are available for reuse via a machine to machine mechanism

5.8 Trusted Identifiers

PSBs have adopted a National Data Infrastructure, which seeks to establish the consistent use of unique trusted identifiers in Public Service administrative data focusing on citizen, business and address identification. Trusted identifiers are critical to unlocking the potential of PSB data holdings as they enable the linking of data across these holdings. Trusted identifiers that have already been implemented in Ireland or are under active consideration include:

- *Personal Public Service Number (PPSN):* A unique individual identifier that is used by individuals to engage with and access Public Services in Ireland.
- *Individual Health Identifier (IHI):* Provides for the introduction of unique Individual Health Identifiers for individuals, healthcare professionals and healthcare organisations, which is only accessible in a health context.
- *Eircode:* The National Postcode System for Ireland, Eircode benefits businesses and PSBs who can use it to plan delivery logistics or services to communities and to help drive geospatial analysis for policy formation and assessment.
- *Unique Business Identifier (UBI):* Government started an initiative in 2017 to assess the introduction of a UBI across the Public Service to act as a single standard identifier for business.
- *Unique Geographic Identifiers (UGIs):* Ordnance Survey Ireland maintains a common set of unique geographic identifiers (UGIs) for over 50 million geographic objects in Ireland (including land parcels, buildings, road segments, etc.), which is available for use by all PSBs.

Countries that have successfully implemented unique trusted identifiers across the Public Service have experienced quantifiable benefits including improved efficiencies through data sharing across Government agencies, simplified interactions with Government,

consistent registration and access methods, a reduction in administrative burden on citizens / businesses, implementation of a range of integrated Government services as well as facilitating better statistical and analytical insights.

Unique identifi ers are also key enablers for Identity and Access Management (IAM) solutions – a set of processes and technologies required to manage users' digital identities, their relationship to real-world identity, and access to systems and information. This is critical for data protection and the provision of secure services online for citizens and businesses.

An example of the use of trusted identifiers in an IAM solution is the MyGovID, which provides citizens with a safe secure online identity for accessing Irish Government services. It is built on the Public Services Card and an individual's PPSN, linking a 'real world' identity to an online identity and gives citizens a secure identity for accessing online Government services. The implementation of a UBI is fundamental to the establishment of a similar such service for businesses.

In the context of the use of trusted identifiers, core data protection considerations related to data, governance, risks, the legal basis, and user rights and freedoms must be considered by PSBs.

Actions

- Promote rollout and adoption across the Public Service of the PSC, MyGovId and Eircode
- Progress the UBI initiative to assess the introduction of a unique identifier for business

5.9 Base Registries

The European Interoperability Framework describes base registries as 'reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, geographic locations and roads…' that are 'authentic and authoritative, and form the cornerstone of Public Services'.

Base registries provide a single source of truth, are underpinned by legislation and promote adherence to the once-only principle by advocating data reuse over data collection, where PSBs only capture data that has not

already been collected and where they have a legal basis to reuse this data.

Verified sources of trusted and authoritative data, and the associated governing PSB of that data, will be developed and made accessible via formal base registries. Implementation of these registries will provide a mechanism through which PSBs access reliable data, in a standardised format using defined APIs, thus removing the need for those PSBs to request, persist and duplicate this same data from citizens and businesses.

Key principles associated with base registries include;

- Trustworthiness – Based on accurate, timely and quality data
- Single authoritative source – A master data repository
- Legal Certainty – A valid source of information
- Reusable – Advocates data reuse over data collection

In October 2017 Ireland signed up to the Tallinn Declaration on eGovernment, which contains the once-only principle as a central tenet and commits the signatories to "take steps to identify redundant administrative burden in Public Services and introduce once only options for citizens and businesses in digital Public Services by collaboration and data exchange across our administrations…".

Implementation of base registries is central to meeting these obligations, will help reduce administrative burden on citizen and businesses having to resupply data, will increase collaboration and data re-use among PSBs, and will promote minimisation and reduce duplication of data across the Public Service.

Exemplars like the Netherlands, Norway, and Estonia have developed base registries as a core building block of their data ecosystems and implemented strict governance processes around the establishment and update of the data within the registry. Based on their experience it is acknowledged that developing a formal system of base registries is a significant undertaking and should be done in an incremental manner.

Actions

- Develop base registries and the processes required to govern their operation

5.10 Transparency

Today's citizens expect seamless digital solutions from all service providers including Government, and demand a high level of transparency and openness, ensuring their privacy is respected. People must be confident in the knowledge that they can find out what personal data Government holds, which

PSBs use that data and for what reason, who accessed that data and when it was accessed.

To help achieve openness and transparency with respect to data management, we will develop a Personal Data Portal, accessible through MyGovID, which will:

- Enable people to see what personal data Government holds on them, which PSBs use that data and for what reason
- Allow people to see how their data is and has been processed
- Facilitate the exercise of the rights of the individual under the GDPR
- Help PSBs meet their Data Protection obligations, such as carrying out Subject Access Requests

To facilitate this, we will introduce data standards to be adopted by PSBs, ensuring personal data and how it is processed is available in a uniform manner to support the functioning of the personal data portal.

We will also make data sharing agreements between PSBs available to citizens, highlighting the legal basis and reasoning behind why personal data is being shared. The Personal Data Portal and the publication of data sharing agreements are complementary to the Government data catalogue commitment detailed in the Discovery section of this strategy. We will work to ensure that the output of these initiatives function in a harmonised and symbiotic manner.

Governments are increasingly embracing openness and transparency by publishing open datasets, which helps improve public accountability and drive innovation and entrepreneurship. Ireland, foremost in this regard, is ranked No.1 in the European Commission's Open Data Maturity assessment for 2017 . Building on this achievement, a well-developed, interoperable, data-sharing ecosystem, with an emphasis on and willingness to open up Government data, where possible, will enable the potential of Open Data to be exploited. This release of any data needs to be in line with legislation such as the requirements to maintain confidentiality (through anonymization or aggregation for example).

High quality and well-governed data, accessible by third parties through an API-first, interoperable architecture, will further drive increases in the availability and value of open data in Ireland.

Actions

- Develop a secure Personal Data Portal for citizens, underpinned with appropriate legislation
- PSBs to publish data sharing agreements on a Government portal, complementing the Government data catalogue
- PSBs to catalogue and release open datasets in line with the Open Data Strategy 2017-2022

5.11 Capability

Best practice data management across the Public Service requires the development of a capability, both in terms of driving standards and monitoring adherence, as well as resources responsible for adoption and implementation.

Developing a PSB's data management capability starts with an assessment of the as-is using a maturity framework that enables data holders to assess their current level of maturity and define a desired target state through a focus on potential benefits. Each PSB, with significant data holdings, should carry out such an assessment and create a data strategy to define a target state data management capability in line with their business objectives.

Each PSB with significant volumes of, or reliance on, data holdings should appoint an officer with overall responsibility for the safe, transparent and optimised use of data. This officer would have the following primary responsibilities:

1. Capability assessment for their organisation in relation to data
2. Creation and implementation of a data strategy
3. Alignment of their organisation with the Public Service Data Strategy
4. Work with the organisation's Data Protection Officer to ensure compliance with data management governance processes, policies, standards and guidelines
5. Leverage data as an asset enabling the organisation to meet its objectives more efficiently and effectively
6. Act as one point of contact in relation to data management for the organisation

It is noted that the Data Protection Officer requirement as set out under legislation should be independent of the role described above.

The Irish Government Statistical Service (IGSS – operated by the CSO) and the Irish Government Economic and Evaluation Service (IGEES – operated by DPER) will continue to provide seconded analytics and economics staff to Departmental data divisions.

Actions

- Define and publish a self-assessment data maturity framework for PSBs to execute
- Define and publish a data strategy template for PSBs to use when developing their own data strategy
- PSBs, where appropriate, will appoint an officer with overall responsibility for data, and the development of their own data strategy in line with this document

5.12 Geospatial

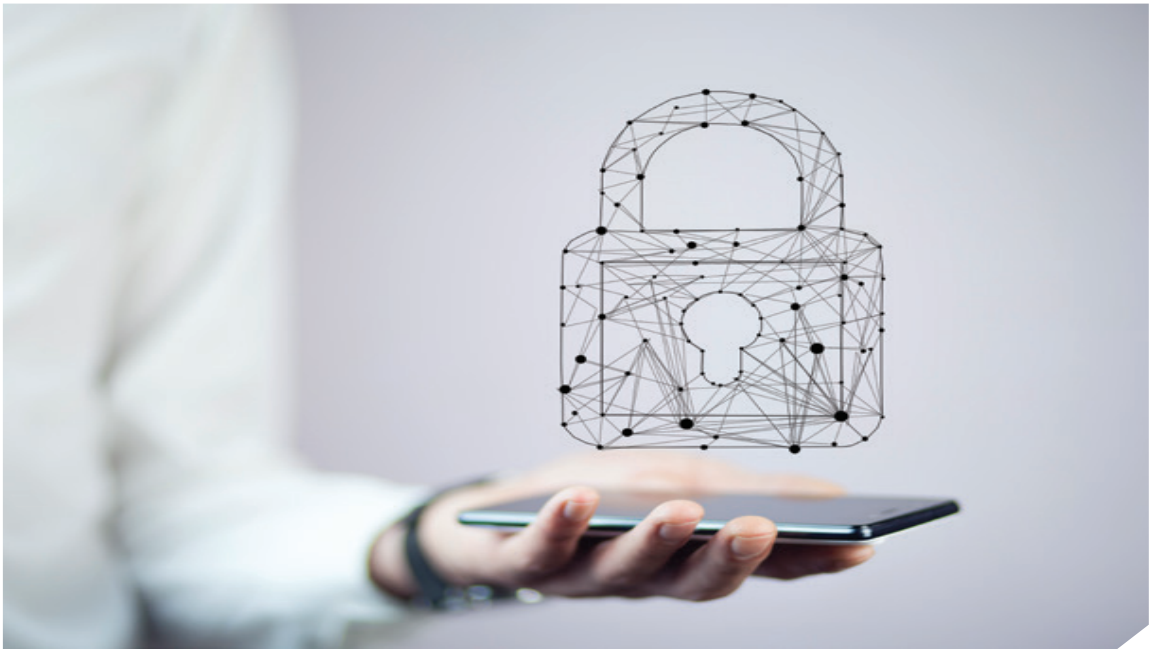
Geospatial data is a key enabler for evidence-based decision making and according to the United Nations Committee of Experts on Global Geospatial Information Management (UN-GGIM, 2015) it is no longer just used for mapping and visualisation, but also for integrating with other data sources, data analytics and modelling.

Geospatial relates to the geographic location and characteristics of natural or constructed features and boundaries on, above or below the earth's surface and can be delivered as digital mapping, imagery and reference systems. When and where things happen is important in many aspects of public policy including the planning, targeting and delivery of services by PSBs. Government, through its many activities, is investing in the collection of geospatial data. The role of authoritative geospatial data provides the means to organise and deliver the answer to both national and global challenges, including sustainable development and environmental management.

The ability to reuse and link geospatial data is a key challenge to enable more insightful analysis of the data collected by Government. The Ordnance Survey Ireland (OSi) maintains a common set of unique geographic identifiers (UGIs) for location data and provides the ability to assemble different datasets in support of evidence-based policies and decisions.

The INSPIRE directive aims to create a EU spatial data infrastructure for the purpose of evaluating environmental policies and activities. This strategy seeks to progress our geospatial infrastructure, and align with the INSPIRE directive to facilitate the sharing of environmental spatial information among PSBs, facilitate public access to spatial information across Europe and assist in policy-making across boundaries.

PSBs, via the publication of geospatial standards, best practice methodologies, and further development of the State's geospatial data hub (GeoHive), will continue to build on the value that such data can bring to their operational and strategic objectives.



Actions

- Encourage PSBs to catalogue and share geospatial datasets, where appropriate to do so using a common reference (i.e. a UGI)
- Further develop the State's geospatial data hub (GeoHive) providing discovery, evaluation and access to Government geospatial data
- Ensure the appropriate governance structure and best practice methodologies are in place through the Data Governance Board to optimise the state's geospatial data and related resources

5.13 Records Management

Records management relates to a broad set of corporate responsibilities dealing with the permanent preservation of data (or records), it enables PSBs to carry out their functions effectively in addition to supporting the smooth operational requirements of National Archives, Freedom of Information and Data Protection legislation.

The Freedom of Information and National Archives Acts vest authority with regard to records management in the Department of Public Expenditure and Reform. The National Archives has an oversight and guiding role and is mandated to preserve the records of Government Departments, the courts and other State agencies which are listed in the Schedule to the National Archives Act, 1986

In 2017, Government approved a Public Service Records Management plan, implemented by the National Archives, with support from the Office of the Government CIO, which aims to deliver the policies, guidelines, structures and systems to achieve the following objectives:

Immediate:

- To give direction to PSBs with regard to records management, supporting the meeting of legislative obligations such as National Archives, FOI and GDPR.
- To reduce spend on offsite storage for records not meriting long term preservation.
- To produce a framework by which PSBs can implement electronic systems for the efficient and effective management of digital records.

Longer-term:

- To develop capacity and capability within the Public Service with regard to records management and increasingly electronic records management.
- To develop capability and capacity in the National Archives to accession and preserve digital records.

Actions

- Implement Governments Public Service Records Management plan

6 Action Summary

The table below includes a summary of the actions associated with each of the strategic themes in

Protection & Legislation	
Action 1	Complete the Data Sharing and Governance Bill and bring it into law
Action 2	Create a framework to support PSBs in sharing data in line with the Data Sharing and Governance Bill
Action 3	Each PSB that processes personal data will ensure their data processing practices are demonstrably in line with data protection legislation

Governance & Standards	
Action 1	Establish a Data Governance Board to oversee and monitor data management practice within the Public Service with appropriate supports
Action 2	Define and publish a set of standards and guidelines, in line with GDPR Article 40, addressing areas of data management

Privacy & Security	
Action 1	Publish privacy-by-design and security guidelines for which PSBs must have regard, and apply in the context of public tenders
Action 2	PSBs to implement appropriate security and privacy measures to comply with Data Protection obligations
Action 3	PSBs should ensure that personal data is protected online at point of access and collection via the use of MyGovID
Action 4	Implement a secure cross-agency Digital Postbox solution

Digital Collection	
Action 1	PSBs to adopt digital data collection as the default method of collection where appropriate, while exploring opportunities for a shared service approach
Action 2	Develop a secure platform for online surveys that has general applicability to multiple surveys and is capable of scaling to accommodate very large surveys, including the Census
Action 3	Establish a UI/UX procurement framework to assist PSBs in accessing UI/UX skills and consider establishing a Government UI/UX style guide for online content. This will help build a more consistent look and feel to Government online, including data collection and input forms
Action 4	Develop a platform for online self-service forms that meets the needs of PSBs seeking to collect non-complex data as part of an administrative process

Interoperability Platform	
Action 1	Incrementally develop an Interoperability Platform and supporting guidelines and processes to support interoperability

Analytics	
Action 1	Develop an analytics platform supporting secure virtual data rooms with a standard analytics and visualisation toolset, and governance process to facilitate cross-agency data analysis
Action 2	PSBs to adopt analytics and visualisation tools to ensure policy development can engage with available data in a meaningful and intuitive manner

Discovery	
Action 1	Develop a Government data catalogue, for internal and public use, cataloguing key data holdings within PSBs, supporting reuse and transparency
Action 2	Develop a Government API portal, as part of the Interoperability Platform supporting the discovery of data and services that are available for reuse via a machine to machine mechanism

Trusted Identifiers	
Action 1	Promote rollout and adoption across the Public Service of the PSC, MyGovId and Eircode
Action 2	Progress the UBI initiative to assess the introduction of a unique identifier for business

Base Registries	
Action 1	Develop base registries and the processes required to govern their operation

Transparency	
Action 1	Develop a secure Personal Data Portal for citizens, underpinned with appropriate legislation
Action 2	PSBs to publish data sharing agreements on a Government portal, complementing the Government data catalogue
Action 3	PSBs to catalogue and release open datasets in line with the Open Data Strategy 2017

Capability	
Action 1	Define and publish a self-assessment data maturity framework for PSBs to execute
Action 2	Define and publish a data strategy template for PSBs to use when developing their own data strategy
Action 3	PSBs, where appropriate, will appoint an officer with overall responsibility for data, and the development of their own data strategy in line with this document

GeoSpatial	
Action 1	Encourage PSBs to catalogue and share geospatial datasets, where appropriate to do so using a common reference (i.e. a UGI)
Action 2	Further develop the State's geospatial data hub (GeoHive) providing discovery, evaluation and access to Government geospatial data
Action 3	Ensure the appropriate governance structure and best practice methodologies are in place through the Data Governance Board to optimise the state's geospatial data and related resources

Records Management	
Action 1	Implement Governments Public Service Records Management plan

Appendix A: Data Lifecycle

Good data management is fundamental to supporting a well-functioning data ecosystem. In order to provide good data management we need to ensure it is applied throughout all stages of the data lifecycle, and by PSBs in a uniform manner.

Multiple versions of a data life cycle exist with variations in practices across different business domains. The lifecycle outlined below was developed to assist the consideration of this strategy in terms of the scope of coverage of the term data management within Government.

Plan: Plan the creation of data, what data, is it personal or potentially personal data, why is it needed, for what purpose, the associated the legal basis to obtain such data, and has it already been collected by the Public Service.

Collect: The factors involved in gathering data such as where do we get it – has it already been collected by the Public Service, and how we do get/validate the data – digital collection or data sharing.

Storage: Where and how is the data is stored is particularly important with a view to utilising

base registries, eliminating data silos, and reusing data across PSB boundaries.

Access: Who is accessing the data, is it secure and protected, and how is access managed in line with data minimisation principles. Logging and auditing are key concerns.

Process: How is data processed - from a legal, technical and operational perspective. Is it transparent?

Publication: Consideration should be given to what data can and should be made public, and how this data should be presented. Open data, data visualisation tools should be considered.

Archive or Destroy: Data must be considered in terms of an end of life or end of usefulness. Decisions and processes to archive, or destroy the data in a secure manner should be made in accordance with relevant regulations (records management and GDPR in particular).

There are exceptions to these lifecycle stages, and Data Quality, Data Protection and Data Security must be considered across all stages. The above diagram illustrates that data management and its associated governance / compliance considerations have multiple phases that must be managed appropriately across Government.

Appendix B: Glossary

A glossary of terms used throughout this document has been provided to assist the understanding of this document.

API	Application Programming Interface
CSO	Central Statistics Office
DEASP	Department of Employment Affairs and Social Protection
DPER	Department of Public Expenditure and Reform
DTTAS	Department of Transport Tourism and Sport
FOI	Freedom of Information
GDPR	General Data Protection Regulation
GP	General Practitioner
UGI	Unique Geographic Identifier
HSE	Health Service Executive
IAM	Identity Access Management
ICT	Information and communication technology
IGEES	Irish Government Economic and Evaluation Service
IGSS	Irish Government Statistical Services
IHI	Individual Health Identifier
OECD	The Organisation for Economic Co-operation and Development
PPSN	Personal Public Service Number
UBI	Unique Business Identifier
UN	United Nations