Consultation on Data Sharing & Governance Bill Proposals

Joint Submission from Digital Rights Ireland and Castlebridge Associates

Submission prepared by Daragh O Brien, TJ McIntyre, and Dr Katherine O'Keefe on behalf of Castlebridge Associates and Digital Rights Ireland

www.castlebridge.ie | www.digitalrights.ie

Contents

Figures

About Castlebridge Associates

Castlebridge Associates (http://castlebridge.ie) is a leading training and consulting firm specializing in Data Governance, Data Protection, Information Quality management, and Information Strategy

Castlebridge Associates has provided Data Governance and Data Protection training and consulting services to public sector organisations including the Revenue Commissioners, the CDETB, and SUSI. We have also advised on Data Governance strategy for a leading, high profile, EU institution, as well as for a range of private sector organisations in a number of industry sectors.

In addition to our training and consulting work we organize specialist conferences on Information Quality, Data Governance, and Data Protection under the "Information Governance and Quality Ireland" brand. See www.igq.ie for details of our latest upcoming event.

About Daragh O Brien

Daragh O Brien, is an internationally regarded expert on Data Governance, Information Quality, and Data Protection practice. He is a Fellow of the Irish Computer Society, a member of the International Association of Privacy Professionals, a former Director of the International Association for Information and Data Quality (IAIDQ), and is currently Global Privacy Advisor to the Data Management Association (DAMA).

Daragh holds a degree in Business and Legal Studies from UCD, and is a Certified Information Quality Practitioner, Six Sigma Green Belt, and Certified Data Protection Professional. He lectures on Data Governance and Data Protection practice on the Law Society of Ireland's Professional Certificate in Data Protection Practice.

About Dr. Katherine O'Keefe

Dr. Katherine O'Keefe is an Analyst Consultant with Castlebridge Associates, specializing in Data Governance and Data Protection implementation and training.

Katherine has worked on Data Governance programme design for a leading telecoms company and has worked with a number of clients on Data Protection compliance reviews and gap remediation.

About Digital Rights Ireland

Digital Rights Ireland is dedicated to defending Civil, Human and Legal rights in a digital age. We are a small, focused organization. We are a member of European Digital Rights (EDRI) and also work with other civil rights groups such as the Irish Council for Civil Liberties and international colleagues in groups such as Privacy International.

Our volunteers work in three key areas:

Working with Government and Legislators

We work to help legislators to understand the issues involved in online rights. For example, we recently appeared before an Oireachtas committee in relation to the issue of cyber-bullying.

Legal Challenges

We are bringing a constitutional challenge against the Irish government in relation to their policy of retaining internet and telephone records on the entire population. This case has a major European dimension and we have already achieved a landmark victory before the European Court of Justice. The Irish Human Rights Commission appears as an amicus.

Digital Rights Ireland itself sought leave to intervene as an amicus in relation to attempts by international record labels to block IP addresses of certain file sharing websites.

Public Activism

We explain these issues in public and help assemble public campaigns in relation to them. We regularly contribute to radio programs and print and online publications in relation to these topics. In 2012 we helped organise the Stop SOPA Ireland campaign and achieved international publicity and condemnation of government proposals for internet blocking.

Executive Summary

We welcome the opportunity to comment at this early stage on the proposal for a Data Sharing and Governance Bill.

We are broadly welcoming of the initiative to improve Data Governance and Sharing in the Public Sector. This represents a key opportunity for meaningful change in the Public and Civil services that has potential to improve customer interactions, drive expenditure reductions, and improve efficiency. These are laudable objectives that have the potential to build on isolated case study examples of good practice cited in the Proposal document, such as the sharing of data between Revenue Commissioners and SUSI to streamline the payments process for student grant assessments.

However, such a vision can only be achieved with a strong and consistent emphasis on Data Governance to avoid repeating the failures of other public service data integration and data sharing initiatives. This Data Governance focus must also address currently identified weaknesses in Data Protection compliance capability across the public sector, which will only be compounded should widespread data sharing become the norm.

In that context we are of the view that:

1. The proposal needs to address the causes of previous failures of public sector initiatives otherwise there will be further failures. These failures were not because of technical or legislative failures but because strong and coherent data governance was missing (For example, see Comptroller and Auditor General Special Report into eGovernment and REACH). This is in line with wider industry research that identifies absence of data governance as a root cause of data integration project failure rates.
2. Data Sharing already takes place between Public Sector bodies and between Public Sector and Private Sector bodies with clear legislative bases. It is unclear what additional sharing capability would be provided by an umbrella legislation, other than the promotion of reuse, which in turn requires effective Data Governance for standards, formats, and usage of data.
3. Data sharing is no panacea. It brings problems of its own in terms of data quality and effectiveness. Data that is fit for one purpose may not be fit for another, and the public service may find itself sinking under a deluge of data it does not understand. There is a far greater possibility of an unthinkable data protection breach.
4. We propose an alternative definition of "Data Sharing". This definition better reflects the reality that different levels of sharing that are required in different circumstances and takes into account the different purposes for which sharing might occur.
5. Data Governance is not defined at all in their proposal. Many of the issues with data sharing in the public sector have their heart in failures of Data Governance and a failure to apply customer-centric and data-driven thinking in the right governance framework, which necessitates a clear vision of what Governance is. We have defined it. We believe the bill should focus on formalising and providing a mandate for transparent and effective Data Governance across the public sector, which will enable safer sharing and support reform.

6. The proposals go beyond the scope of what is required for compliance with the EU Reuse of Public Sector Information Directive. Other aspects, such as the limitation on data sharing to public sector bodies within the State, do not meet the requirements of the Directive.
7. The definition of Data Sharing contained in the proposal document is insufficient and we provide an alternative definition.
8. The role of the Data Protection Commissioner as an independent arbiter must be maintained. It is not appropriate that they have direct input into Data Governance in the Public Sector as this goes against the necessary segregation of Duties. A Data Governance Office for the Public Service could provide the appropriate "honest broker" for common principles, standardised practices, and common governance across the Public Sector, with particular reference to improving standards in Data Protection practices and the development of a common "Business Data Glossary". This mirrors the practices in large private sector organisations when dealing with the Data Protection Commissioner. As an entity that is independent of Government under EU Treaty provisions, it is essential the engagement of the State with the DPC be on the same terms as other large Data Controllers and Data Processors in the Private Sector.

We are of the opinion that, should our concerns and suggestions be taken on board in the drafting of this legislation, there is a significant opportunity for Ireland to establish a "best of breed" model for effective and balanced sharing of public sector data, while at the same time driving efficiencies and economies in the sector through improved Data Governance; clarity of roles, responsibilities, and accountabilities; improved potential for reuse of data; standardization of common work practices, procedures, and training for Data Protection; and collaborative resolution of information quality errors and prevention of 'scrap and rework'.

The sharing of public sector data will always raise issues of trust, transparency, quality, and compliance. Recent high profile cases such as the disclosure of GRO data of living individuals via an Ancestry research website, unauthorized access to personal data held by Government departments such as the Department of Social Protection, and concerns raised in the media about the Data Protection compliance of data handling by Irish Water, all serve to undermine that trust in how State bodies handle personal data.

With the former Data Protection Commissioner openly decrying the failure of Public Sector leadership to engage appropriately with their obligations under Data Protection law, and warning of the need for "continued vigilance about the encroachment of the State into the private lives of individuals" (Hawkes) it is essential that any reform of Data Governance and sharing addresses these concerns in a forthright and transparent manner.

This Bill provides a unique opportunity to establish a data sharing framework that is underpinned by transparent Data Governance principles that will be deserving of and supporting of public trust. In this way, an appropriately structured Bill, which focuses on the obligations of Governance rather than the minutiae of execution, can provide a stable foundation on which to build a reformed culture and practice of trusted, trustworthy, safe, and compliant Data Sharing in the Public Sector.

Introduction

Effective sharing of information between organisations has the potential to streamline the delivery of public services. However, experience in both the public and private sectors has shown that increased access to and sharing of information does not always translate into an increase in efficiency and effectiveness. Furthermore, industry research has shown consistently that data integration and sharing initiatives that do not address data governance have a significant risk of failure. This has been borne out by C&AG reviews of data sharing and data integration initiatives over recent years in the Irish Public Service.

The very clear and trenchant comments of the former Data Protection Commissioner about the culture of Data Protection compliance in the Public Service, is symptomatic of systemic failures in Data Governance in the Public Service and the absence under current legislation and structures of clear decision rights, responsibilities, and accountability for data processing activities, especially in the context of Data Protection. We must also acknowledge the creation and use of legislative basis for data sharing in a number of high profile government initiatives such as the establishment of Irish Water. Based on the experience of Castlebridge Associates advising on Data Governance and Data Protection aspects a number of Public Sector initiatives we must also recognize the often low levels of maturity of understanding Data Governance principles and specifics of Data Protection law and practice.

On that basis it is clear that the emphasis within any Data Governance and Sharing Bill should be placed not on the legislative basis for sharing of data, but rather on implementing clear and standardized structures to ensure the effective and efficient governance of data, which will in turn provide a foundation for trusted and transparent sharing of data to support efficiency and transformation in the public service.

In this document we have set out a series of detailed responses to the questions posed in the consultation process. In preparing our responses we note that the questions in the consultation document were not numbered sequentially, with question numbers being repeated in the document. This may pose difficulties in comparing responses between submissions, hence we have not relied on the number of the questions but have used section headings containing the text of each individual question.

We have also included a detailed analysis of the definitions of Data Sharing contained in the document and put forward what we believe is a more detailed and descriptive definition that reflects the different categories of sharing that might arise in practice. We have also provided a working definition of Data Governance, which we note was not actually defined in the consultation document. We have also outlined a possible framework for a Data Governance Office for the public sector, to support the development and definition of common standards, business data glossary, independent oversight of Data Sharing arrangements, and standardization of training and work practices for Data Protection

Officers across the public sector. This DGO function would support a segregation of duties between the execution of public sector data sharing and the Data Protection Commissioner, further ensuring independence of the Office of the Data Protection Commissioner as required under EU law.

We also request clarification on the degree of overlap between the requirements of the Reuse of Public Service Information Directive and the requirements of Open Data in government and the implicit vision of granular data sharing between public sector bodies for operational purposes. We submit that these are two distinct purposes and should not be conflated for the purposes of sharing data. Provision of aggregated and statistical data for PSI and Open Data purposes requires a different level of and approach to Data Governance and Sharing then the sharing of data for transactional purposes.

It is clear that data is and will be shared between public sector bodies and between public sector entities and private sector firms. This sharing can be addressed on a case-by-case basis with specific legislation. In our submission we point out that it may not be possible for a "one-size-fits-all" over-arching Data Sharing provision given the requirements under EU law for processing to be proportionate. We set out potential solutions to this, but highlight the essential emphasis on effective governance of data to promote reuse of standardized data sharing services for common purposes.

As sharing occurs, and will continue, we are of the opinion that any new legislative provisions should focus on ensuring a strong foundation is established for a robust Data Governance capability within the Public Sector. It is this capability, combined with a coherent strategy for data sharing, which will support efficiency and effectiveness in the Public Sector as well as providing a comprehensive platform for Public Sector reform through data.

Absent a focus on developing a consistent and appropriate data governance framework within this Bill it is inevitable that increased sharing of data will lead to increased likelihood of costly project failures due to data governance and data quality issues, as well as placing the personal and sensitive personal data of citizens at increased risk of unauthorized processing, theft, or misuse. While no system of governance will ever be perfect, any form of statutory-based Data Governance with a sufficiently clear mandate and authority will clarify roles, responsibilities, and accountabilities for data in the Public Sector.

Important lessons about the importance of effective Data Governance as part of Privacy by Design can be learned from the implementation of Data Sharing in Irish Water, which has significant legislative basis for data sharing provided for in the Water Services Act 2013. Due to a failure to engage clearly and transparently with Data Governance and Data Protection issues, concerns about the Data Protection compliance of Irish Water's processing, and significant confusion as to their entitlement to request PPS Numbers and the purposes for which those details would be used, resulting in extensive (and avoidable) media comment and scrutiny from the Data Protection Commissioner's Office.

This Bill represents a singular opportunity to define a statutory framework for common Data Governance standards to underpin improved Data Protection compliance in the Public Service, implement appropriate data sharing based on agreed principles, drive reform of Public Services through a focus on data, and demonstrate transparency and trustworthiness of public service data processing to the relevant data subjects – the citizens.

We would hope the Minister considers our comments and submissions and seizes the opportunity to drive a radical data driven reform of the Public Service through improved Data Governance to support trusted and trustworthy sharing of data.

Data Sharing and Open Data: A disconnect in the proposals?

As part of our review of these Policy Proposals, we have sought to validate the stated rationale and reason for the Data Sharing framework and associated legislation against the specific policy proposals contained in the document. This analysis has informed some of the rationale behind our responses to the formal questions raised in the consultation document.

The scope of the directive and proposed legislation

We are concerned that the scope of the proposed legislation goes beyond the scope of the EU directive it proposes to address and beyond both its stated objectives and legal justification.

Query: Does the proposed policy go beyond the requirement of the PSI Directive?

Page 17 of the Data-Sharing and Governance Policy Proposal positions the suggested bill as "containing the necessary provisions required to transpose the Public Service Information Directive (DIRECTIVE 2013/37/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information) into Irish Law. However, Directive 2013/37/EU addresses "Documents produced by public sector bodies of the Member States" which "constitute a vast, diverse and valuable pool of resources that can benefit the knowledge economy" and encourages open data policies to establish "a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States." (Article 1) These objectives are addressed in actions 21-25 of the eGovernment strategy "Supporting Public Service Reform 2012-2015" (April, 2012 http://per.gov.ie/wp-content/uploads/eGovernment-2012-2015.pdf).

Query: Is what is proposed under this Policy proposal a framework for data integration as opposed to Open Data?

PER's paper proposing a data sharing and governance initiative across public bodies defines the subject of the proposed bill as ". . . data-sharing consists of two public service bodies sharing structured data about an entity (such as a person, business, property or event)", suggesting that "the implementation of an “ask-once, use many” vision will help to significantly reduce the administrative burden on citizens and businesses,. . ." (Data Sharing and Governance Bill Policy Proposals, 2).

The proposal is not an open data initiative that addresses the directive in scope or content. Rather, the "ask-once, use many vision" and the "overall database of identity information" (12) for the purpose of: "a) the matching of identity data provided by multiple public bodies so as to provide the public service with a system-wide view of identity data and b) to provide a general identity verification service" (11) suggest a large scale data pooling project which is appears far beyond the scope of legislation required by 2013/37/EU.

Given the well publicised issues of inappropriate access and unauthorised disclosure of personal data in a number of Public Sector organisations, and the very explicit criticism by the Data Protection

Commissioner of the Data Protection culture within the Public Service, the creation of a larger, more integrated, data repository of citizen data gives pause for concern. Notwithstanding our concerns that the proposed registration goes beyond the requirements of the Directive, any legislation that enables greater access to a richer data set describing identifiable must balance the risk to privacy with clear and decisive sanctions for misuse or abuse of this data, and robust controls to build-in risk mitigation and require Privacy by Design/Privacy by Default principles to be respected at a senior level across the Public Service and Government.

Conflict with Proportionality Principles and the Objectives of the Directive

Paragraph 25 of Directive 2013/37/EU states: "In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives. This Directive should achieve minimum harmonisation, thereby avoiding further disparities between the Member States in dealing with the re-use of public sector documents".

We would query how the proposal fits with this emphasis on proportionality and avoiding further disparities. It would seem, rather, that in going far beyond the scope of the EU directive, PER's proposal may in fact violate the purposes of the Directive. It is also to be noted that 2013/37/EU specifically identifies "to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products" as objectives of the directive (paragraph 25). As such is the case, both the specific exclusion of "sharing of data with a public body in another EU member state" in the proposal's definition of data sharing and the focus of the proposal on large-scale aggregation and matching of personal data are incompatible with the European directive.

We would also query the compatibility of the proposal with the fundamental human right of data privacy as recognized in the EU Charter of Human Rights, the Data Protection Directive (Directive 95/46/EC), and in the Irish Data Protection Acts of 1988 and 2003.

Query: Is there a 'disconnect' between the stated policy objectives and the proposed policy framework to be transposed into legislation?

We are concerned by an apparent disconnect between the stated purpose of the proposed Data Sharing and Governance bill, and the actuality set forth in the proposal. The stated purpose of the proposed bill as set forward has been expressed thus by Minister Brendan Howlin:

> *The purpose of the proposed Bill is:*
>
> *1. To improve the experience of citizens accessing services by requiring public bodies to use data that is already available electronically in the public service when delivering services by removing the option of relying on certain paper documents to verify provided information, but instead requiring that it look up the data or seek it from the relevant public body. Removal of the option to request a particular paper document by a particular public body will only take place where the purpose(s) for which the document was being requested can be met by other channels, and where there will no adverse effect on the efficiency or control measures of the particular public body.*
>
> *2. To provide a legal framework to support access to data held by other public bodies. It is expected that when the new Data Protection Regulation comes into force that all data-sharing and linking in the public service will require an explicit legal basis, and a legal framework usable by smaller public bodies will be required to facilitate the establishment of such a legal basis in a reasonable timeframe.*
>
> *3. Set down data-sharing and data-linking principles for all public bodies, including requirements around structure, project governance and security. These would provide a statutory basis for best practice, building on existing DPC guidelines and PER Circular 17/2012, and including a requirement to conduct a Privacy Impact Assessment prior to undertaking any new data-sharing projects.*
>
> (http://www.per.gov.ie/government-agrees-measures-to-improve-data-sharing-in-the-public-service/)

The proposal goes beyond these stated objectives in a number of ways. We believe that our recommendation to place a focus on establishing a clear Data Governance framework and oversight entity will better meet the stated policy objectives than the focus on sharing of data that appears to be the current focus of the proposed Bill.

Query: Where in the proposal is there a clear statement of Information Processing Principles

We note a distinct absence of clear data-sharing and data linking principles in the proposal, particularly in the case of structure and project governance. Although the proposal starts with a suggested definition for "data sharing", the resulting proposed definition refers back to the term it purports to define. A definition of "Governance" is not attempted. Thus, neither "data sharing" nor "governance" are clearly defined, with a resulting lack of clarity in the proposal. Without clarity in understanding the

Governance structures, rights, and accountabilities to be set in place, it is difficult to gauge how this proposed bill will set in place frameworks that bypass the existing legal protections without contravening the fundamental human rights that the current legal framework is designed to protect. In the case of data sharing between public bodies without the consent of the data subject a specific legal basis is required. Currently, primary legislation sets forth the specific need for an explicit legal basis to share or re-use data for a purpose not specified on collection. This provides the legal framework that protects the data subject's fundamental right to privacy that Minister Howlin notes when he states: "in Ireland we benefit from strong constitutional protections relating to individual privacy, which are reinforced in terms of data sharing by the extensive safeguards embodied in EU data protection law." (http://www.per.gov.ie/creating-confidence-in-data-sharing/).

While the "Data-Sharing and Governance" bill proposal states that the proposed framework for data sharing will remain subject to the requirements of Data Protection law, it is unclear how the proposed bill would accommodate the fundamental need for the legal specifications of a particular data sharing requirement without the primary legislation under which successful examples of data sharing provided in support of the bill were successfully engineered.

We would query the specifics as to what in the proposed bill will ensure data sharing is conducted in compliance with fundamental human rights.

The Interoperability Objective

At the heart of any discussion of data sharing is the question of interoperability. How this question is framed depends in many respects on what is understood by the term "data sharing" and how this aligns with the requirements of the interoperability framework that is developed within any Data Governance structure or legislative oversight.

It is particularly important that the definition of what constitutes "data sharing" and "Data Governance" under the scope of the proposed legislation is sufficiently clearly constructed so as to be unambiguous. It is the experience of Castlebridge Associates that among the key causes for failures in Data Governance initiatives is a failure to properly define what is meant by Data Governance, to clearly articulate a Vision for Data Governance, and to define unambiguously fundamental core principles that should under pin the processing of data of any kind, in particular personal data.

The policy proposal, as it stands, fails in our view to clearly articulate:

1. What data sharing is, and equally what it is not. This creates a potentially significant risk of 'scope creep' or 'function creep' in the operation of Public Services.
2. What Data Governance is understood to mean in the Public Service, and what the format and structure of that Governance would be.

Given the very public and trenchant criticisms by the Data Protection Commissioner of the general attitudes and approaches to Data Protection within the Public Sector in recent months (but going back many years) and the apparent difficulties faced by Public Service management in preventing, detecting, and taking action on foot of breaches of information security and Data Protection, it is our strong opinion any "interoperability framework" for data sharing must be built on very clear Fundamental Information Processing Principles, with a very clear common definition, vision, and application of Data Governance.

In addition, we would be concerned that the policy proposal as currently framed conflates Data Sharing and Data Governance. This, in effect, conflates the action of doing data sharing and data processing with the establishment of appropriate Governance structures to oversee that sharing and processing. This failure to draw a distinction between the two issues has its root in the definitions which underpin this proposal and results in a failure to clearly delineate an appropriate segregation of duties and responsibilities within the policy framework.

We strongly believe that, in the absence of a clear differentiation between the function of sharing and processing data and the function of implementing and operating effective oversight and controls, there is a strong risk that the current deficiencies and weaknesses in control of, oversight of, and protection of data (whether sensitive, personal, financial, or operational) within the Public Sector will persist.

We would recommend that a clear distinction be drawn in proposals between Data Governance and Data Processing, including Data Sharing. This is in line with established best practice for Data Governance initiatives.

Defining Data Sharing

As highlighted elsewhere in this submission, we disagree with the definition of Data Sharing that has been put forward in the current draft legislative proposal.

The definition currently put forward **does not actually define data sharing**. It describes certain specific actions and actors which may be in scope within a *process* for sharing of data. It presumes that there is a common understanding of data sharing as a discipline and practice.

We are concerned that this lack of definitive definition would give rise to unanticipated and undesirable scope creep or function creep in data processing and data sharing on one hand, and avoidable confusion and objections to valid and legitimate initiatives on the other. Indeed, from our review of the current Policy Proposal it is unclear at times whether the 'sharing' being proposed is a case by case exchange of data for specific operational purposes (e.g. the exchange of data between SUSI and the Revenue Commissioners pursuant to the Student Finance Act 2011) or the creation of a 'Single View of [Entity]' shared data repository.

Furthermore, the definition as set out in the current proposal does not adequately distinguish between the act of data sharing and the act of and practice of *governing* the sharing of that data. These are two distinct concepts and should be defined and addressed separately (we define Data Governance below).

We believe that it is fundamentally important that the definition of data sharing be clear, non-recursive, and unambiguous so as to ensure that all current and potential future purposes and mechanisms for sharing of data are addressed appropriately. We also submit that a failure to distinguish between the act of sharing data and the operation of governance over that sharing would allow the current climate wherein effective governance of data is often placed second to the execution of a data related process to persist, representing a significantly wasted opportunity for reform in the Public Sector.

An Alternative Definition of "Data Sharing"

We would propose the following definition:

> *Data Sharing is the execution and operation of defined processes for the exchange of information between one or more entities for the purpose of supporting the delivery of statutory public sector services, or the execution of obligations under EU law.*
>
> *Data sharing processes may operate on*
>
> *a) a case by case basis for the validation and verification of data;*

b) *on a defined batch processing basis for the validation, verification, and updating of specific populations of data;*
c) *or as once-off consolidation and integration of disparate data sets to form a new, shared, master data repository. This may also be called Data Pooling or Data Consolidation.*

Defining Data Governance

Data Governance is defined by the Data Governance Institute as:

> *"A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods" (The Data Governance Institute)*[1]

Data Governance is not defined as a concept in the Data Governance and Sharing Bill proposal. Given that some Public Service organisations, including regulatory organisations, have defined their own definitions of Data Governance and Information Governance, for example HIQA's Guidance on Information Governance (Health Information & Quality Authority), there is a distinct risk of cross Departmental variances in definition of and application of Data Governance principles and practices absent a clear *centralized* standard definition of the term. This objective may be served through an appropriate legislative intervention, coupled with a clear framework for ensuring the definition and its associated principles are consistently and effectively communicated and applied throughout the Public Service.

With regard to whether Data Governance issues are a question of implementation, we refer you back to our core working definition of Data Governance from the Data Governance Institute.

Data Governance Definition Element	**Comment**
A System of Decision Rights…	The establishment of a system of decision rights for the processing of data is an organizational and cultural issue. While a legislative basis for the system may provide a common framework, it will fall to organization leadership from the top down to drive the cultural change necessary to execute effective Data Governance. The current Data Protection Acts provide an example of an existing system for a framework of decision rights, but we have still seen an apparently systemic inability on the part of the Public Sector to translate this into practical management.

[1] Other definitions can be found in *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program* by John Ladley, Morgan Kaufmann, 2012

Data Governance Definition Element	Comment
…And accountabilities for information-related processes …	The concept of accountability is essential in any Data Governance framework. This goes beyond accountability for breaches of information security and the related provisions of the Data Protection Acts by front-line staff, but should encompass accountability throughout the management hierarchy for decisions relating to the scoping, design, implementation, and operation of data processing activities throughout the life cycle of information (Plan, Obtain, Store/Share, Maintain, Apply, Dispose). Legislation can create penalties and sanctions but cannot ensure their application and enforcement. If laws could, in and of themselves, change behavior we would be instantly crime free.
…executed according to agreed-upon models…	Legislation can establish, to an extent, the general principles and structures for establishing agreed-upon models for executing information-related processes. However, ultimately it is, in Castlebridge Associate's experience on engagements in Public and Private sector, a matter for organizational implementation and prioritization to ensure that models are actually agreed and, more importantly, followed. This is not just an implementation challenge. It represents a significant cultural and leadership challenge in any organization. Furthermore, we would point out that there is a legacy of disagreement on models for Data Protection compliance in the Public Sector that go beyond the high profile cases of unauthorized access and include the decision by the Department of Health in 2012 to ignore an enforcement notice from the Data Protection Commissioner in regard to heel prick test data retained without a specific purpose or consent.
…Which describe who can take what actions with what information, and when, under what circumstances, using what methods	This is the operationalization of Data Governance and represents the point at which Governance and execution of information related processes intersect. Legislation may set out broad specification of actions that are to be taken with information under what circumstances.

Data Governance Definition Element	Comment
	The operational compliance with legislation requires effective governance oversight, controls, and accountabilities to be in place. Given the Data Protection Commissioner's trenchant admonishing of the Public Service for failing to ensure that the right actions are taken with the right data using the right methods under *current* legislation, we would question the effectiveness of the Data Governance function in the Public Service as it currently stands.

Under this breakdown, Governance is the system that determines *who* defines the processes and methods of data sharing, *what* data may be shared, *how often*, to *whom*, and under *what* legislatively supported circumstances. It is to be reiterated that Governance must involve not only decision rights but also accountabilities, in order to ensure the systems and processes under governance operate effectively.

Therefore with regard to the question (numbered 13 but actually the 17th question in the Proposal document), "*Do you agree that 'The problem [of data governance] is therefore primarily one of better implementation, rather than an absence of legislation.'?*", our answer must be in the negative as neither implementation nor legislation alone address the challenges and opportunities inherent in effective Data Governance.

A key challenge of Data Governance is organization culture and 'tone from the top', which in turn impacts on implementation. Absent a consistent and coherent definition of Data Governance and an associated consistent and coherent definition of Data Governance principles across the Public Service (which may benefit from a legislative basis), any legislative or 'bottom up' implementation approach will almost certainly fail to achieve the desired operational and strategic outcomes in a sustainable manner.

It is a fundamental principle in Quality Management that 80% of the defects and errors in a system (Deming) are the fault of management in and of that system. While the media and Regulatory investigations may focus attention on the acts and actions of individuals at the front-line of service delivery, any improvement of the system requires management to accept accountability for the outcomes within the system. This is a critical element in effective Data Governance.

The Importance of Segregation of Duties in Data Governance

Data Governance is not and should not be a function performed by those involved in the day to day management of information. Data Governance is tasked with ensuring that data is managed, not managing data. Data Governance functions need to be able to focus on ensuring that the right standards and practices are being applied consistently in the act and action of managing information.

A key concept in Data Governance is the "Data Governance V" which highlights the segregation of duties that *must* be respected in the design and execution of systems of decision rights, responsibilities, and accountabilities for data and information. This is a fundamental concept that aligns with established practices in the management of other asset classes in an organization such as people, equipment, and financial assets.

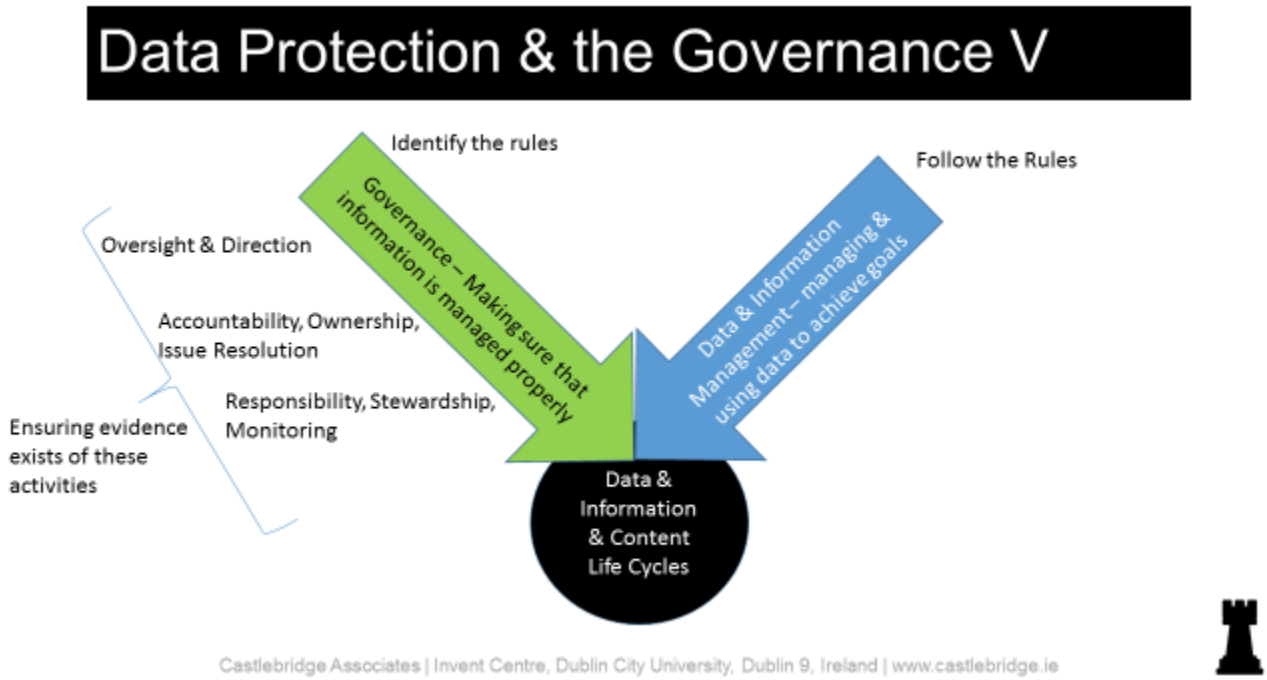

Figure 1 The Data Governance V - based on work by John Ladley

The left side of the Governance V provides input to data and content life cycles as to what the rules and policies are, and activity to ensure that data management is happening as it is supposed to. The Data Governance function is separated from the day to day management of data such that it can serve as an 'honest broker' and ensure that appropriate information stewardship and oversight activities are actually happening.

The rights side of the V is the "hands-on" implementation of and execution of data management processes. The overlap between the two is in the execution of processes (Content life cycles) where the

right rules need to be followed in the right way, acting on the right data, for the right reasons, at the right time.

In Figure 2 below we illustrate the various layers of segregation of duties that should exist in the context of Data Protection compliance, however in the context of Master Data Management and establishing any form of Service Oriented Architecture for data services across a large organization, there are a number of additional governance factors that will need to be considered. For the purposes of the illustration we have not shown the Private Sector segregation of duties as a 'V' but the best practice is that a segregation of duties exists there too.

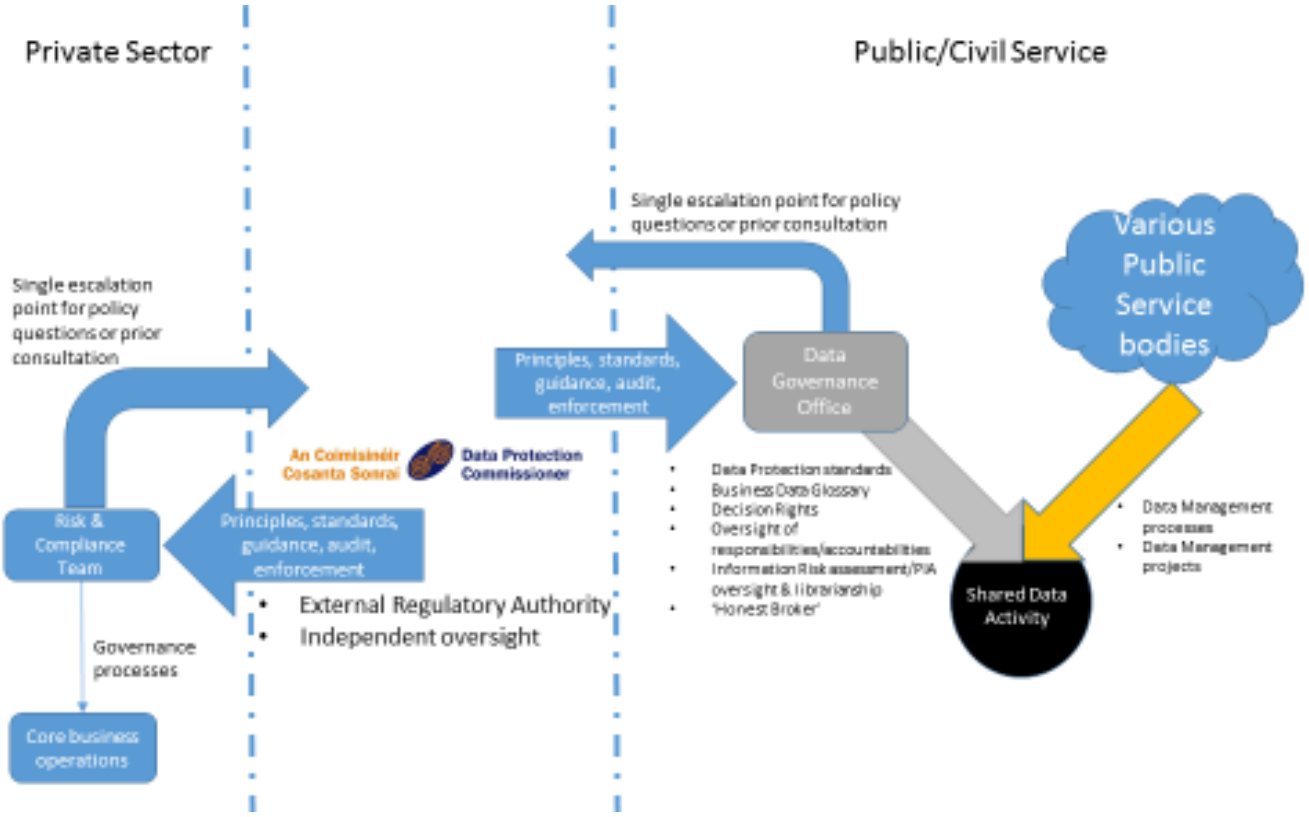

Figure 2: A Segregation of Duties model example

Learning from prior experience

In the scoping and framing of this Data Sharing and Governance Bill we would hope the Government would learn the lessons of past failures in data sharing and data integration initiatives in the Public sector. Examples include PPARS, REACH, and, more recently, PeoplePoint.

The REACH initiative is a relevant case study as it proposed the creation of a Public Service Portal for citizens to interact with public services via a single "broker". This initiative failed to achieve the hoped for potential. In their report on its failure (Office of the Comptroller & Auditor General), the C&AG

identified weaknesses in governance as being a key root cause for the sub-optimal delivery of REACH, which was delivered three years behind schedule and at a cost over 2.5 times the original estimates.

While many of the specific comments made by the C&AG relate to the financial management of projects, we are of the opinion that the same general principles that the C&AG has applied to the financial asset class of eGovernment initiatives should be applied to the Information Assets as well. The C&AG has stated that:

> *"eGovernment projects that cross organisational boundaries present opportunities for more efficient and effective delivery of government services. However, by channelling funding through traditional departmental 'silos', existing budgetary arrangements may have militated against effective cross-cutting eGovernment developments. Consequently, cross-cutting projects should have unitary management."*

In the same way, government projects that share data across organizational boundaries present opportunities for more efficient and effective delivery of government services. However, by channeling the Governance of shared data through traditional departmental 'silos', variances in local data standards, business rules, access controls, and understanding of data may militate against effective cross-cutting eGovernment or effective data sharing developments. Consequently, cross-cutting initiatives should have a unitary management of the Data Governance function.

In our view it is this centralized Data Governance function, with responsibility for data standards, for defining and ensuring the implementation of transparent decision making rules, roles, and responsibilities for data in the Public Sector. With a mandate to define and develop common standards and work practices for Data Protection, data definition, and data-driven technology development such a function would provide the basis for sustainable, proportionate, and trustworthy sharing of data within the Public Sector.

Looking further afield, it is worth noting the value that is placed on effective Data Governance for shared data in public sector organisations in other jurisdictions. The International Finance Corporation in the World Bank has been a pioneer of Data Governance for improved information quality. Various information quality and data governance professional association conferences world-wide feature case studies on Data Governance in public sector organisations. Examples and, where available to us, copies of presentations can be provided to the Department on request.

Detailed Responses to Specific Questions Raised in Consultation

Due to the mismatch in number of questions in the proposal document itself, we have opted to provide detailed responses to each question, with the question being restated as a sub-heading in this document.

Do you agree with this definition of data-sharing?

As we will discuss in detail below (see page 16), we do not agree with the definition of Data Sharing that has been included in this proposal. In our view:

1. It fails basic rules of definition as it defines the thing (data sharing) with reference to itself (sharing of data).
2. It conflates the distinct concepts of Data Governance and Data Sharing, and also does not differentiate between categories of sharing which may raise different requirements re: complexity of appropriate Governance.
3. By excluding one-off transfers of data it would appear to exclude on-off transfers used to populate new data repositories for new purposes or for the purposes of creating new consolidated data sets.

We outline our reasons for disagreement with this definition in detail on page 16.

If you do not agree, how do you believe the definition could be improved?

As the definition provided is circular, recursively defining a term ("data sharing" with reference to itself ("sharing of data", it does not define the concept of "data sharing" in a useful or meaningful way. The first step to improving the definition of "data sharing" would be to clearly identify the concept to be defined and describe it in plain language that does not use the words being defined.

We provide a detailed analysis of how the definition might be improved, and a suggested alternative definition, on page 16.

What do you believe are the priority areas for data-sharing to contribute to improved public services?

If this question seeks to identify priority subject-matter areas which would, could, or should be in scope for data sharing arrangements within the Public Sector to contribute to improved Public Services, then we submit that this question is not relevant to a consultation on a legislative proposal and is more properly a question for the definition of Information Strategy within the Public Service, and the operational execution of data sharing/data integration processes as part of Public Service delivery.

If, however, this question relates to issues which must be addressed in order to ensure that sharing of data might contribute to improvements in Public Services, we would submit that the following areas are a matter of immediate concern:

1. Steps must be taken to address deficiencies in the *culture* of Data Governance in the Public Service, particularly with reference to Data Protection. It must be clearly addressed as a matter of

fundamental rights, with appropriate leadership and resourcing within each Department and other public sector body.
2. Global data standards, metadata definition, data quality standards, and agreed models for decision making around data are required to ensure the correct sharing of the correct data consistently. Assumptions about the nature of data must be validated against a definitive Business Data Glossary.
3. Staff must be trained correctly in data handling, in particular Data Protection processes. It is a best practice in the private sector for staff in organisations to complete annual or bi-annual Data Protection Compliance training, we believe it should form a formal part of PMDS reviews in the Public Service.

In short, we do not believe that it is data sharing *per se* that can improve public services. Rather we believe that effective Data Governance, supported by a robust culture and 'tone from the top' around the importance of data and the importance of its effective governance are essential to improved public services whether data is being shared/integrated or not. In this way data can be shared in a trusted and trustworthy manner, avoiding unnecessary 'scrap and rework' costs, and minimizing risk.

The core Data Protection principles, if adopted as core principles for data governance rather than seen as barriers to data processing can have a significant impact on effectiveness of public service delivery.

An example data quality stories shared with us by a delegate at a recent training course:

- On being made redundant in 2009, they went to sign on. DSP records indicated they were married to their spouse, but there was no corresponding record showing that their spouse was married to them. This delayed the processing of Job Seekers Benefit and required data to be manually corrected at the local office. Query: If this data was being shared with other Public Sector organisations, what impacts might have arisen?
    - Data was inaccurate (breach of Data Protection principles)
    - Data was incomplete (breach of Data Protection principles)
    - Data was not adequate for purpose (breach of Data Protection principles)
    - A simple control report would have identified instances of this kind of inconsistency and supported a cleanup of defective data. However the underlying process error would need to be identified to prevent future occurrences.

Do you agree that more effective data-sharing can help drive public service reform?

It is not possible to answer this question in the affirmative, notwithstanding our strong belief that improvements in Data Governance and related improvements in Information Quality across the public service will help support reform. We do not believe that sharing of data, absent a sea-change in Data Governance practices and culture, including but not limited to an improved focus on Data Protection principles and compliance across the public service, will lead to effective reform given the significant failure rates on data sharing and data integration initiatives, across all industries, that do not address Data Governance and Information Quality issues.

The question of whether data sharing will help drive public sector reform is complex. A facile response might assume that "more effective data sharing" means better quality information, and that information

quality will drive reform. It is easy to agree that improved data quality and improved data standards are desirable and will result in more accurate and efficient execution of processes and provision of services.

However, underlying this general agreement are the fundamental questions of how to improve data quality, and how data quality and data sharing are related. We would strongly advise that in advance of beginning a new data related initiative, it is critical to determine what is a cause or driver and what an 'outcome' is in this context.

We submit that, as it is currently phrased, the question poses a 'chicken and egg' dilemma. If the objective of the legislation is to allow more effective data sharing, one must immediately ask "To what purpose?" This question needs to be answered to ensure that any sharing of data meets the requirements of the Data Protection Directive, and the forthcoming Data Protection Regulation.

We submit that sharing of data, whether effective or not is not an outcome and cannot be a goal.

Sharing of more effective data may have a benefit on public service reform. The benefits will likely come not from increasing the amount of data being shared or the scope of data being co-mingled in public service processes. Rather any impact on public service reform will arise from changes in the way in which the public service, from a senior level down, views and prioritizes the effective governance of information. This constitutes a cultural shift that must be managed, and a change initiative that can be underpinned by legislation but must be executed by people.

The change in culture will be required to ensure appropriate changes in Data Governance and the management of Information Quality.

Improving Information Quality

One definition of Information Quality (or Data Quality) states that, Information Quality is:

> *"The degree to which information and data can be a trusted source for any and/or all required uses.*
>
> - *Real - accurate reflection of real world*
> - *Recent - up-to-date information*
> - *Relevant - information our customers and the business needs and cares about"*
>
> (McGilvray, Danette. Ten Steps to Quality Data: An Overview)

It is worth noting that these attributes of quality data, "real", "recent", and "relevant", are embedded in the eight fundamental rules of Data Protection which state that personal data must be accurate and up-to-date (Data Protection rule 5), and personal data must be adequate, relevant, and not excessive (Rule 6). Thus, an outcome of quality data is also an outcome in which the fundamental rules of data protection are respected.

How do we know that information is relevant? Relevance as an attribute of quality data means that "quality" is experienced at the point of consumption. "Relevance" can have both technical aspects affecting interoperability and integration of data (completeness, accuracy, timeliness, currency [up to date-ness] as well as "soft" aspects such as whether the output of the processing met customer expectations. Privacy, and a respect for fundamental rights would be just one of the "soft" aspects, and many of the more technical aspects feature in the Data Protection principles. In the proposed case of several public sector bodies sharing information, governance structures and decision rights will have to be implemented to determine what constitutes relevant and accurate data.

Is information considered relevant or accurate in one department exactly the same as information considered relevant or accurate by another department? If each entity sharing their data is sure their data was captured correctly and is relevant for the purpose it was obtained, how are possible conflicts in data sets resolved? What differences in standards for obtaining data could cause conflicts? Are the data models of different entities compatible? What format is it in? Does the metadata match up? Who has the right to change or update the data, and under what circumstances? What are the knock-on effects of a change?

Which raises another question: What are the causes or drivers for Data Quality? The pooling of data sets which may include large volumes of information that is of poor quality is unlikely to support Public Sector Reform. It will inevitably cause rework and the creation of 'local trusted copies' of data, which could have the undesirable effect of bogging down effective reform. Improvement in the quality of data is not, of itself, a driver but is a desired outcome that will support reform. Quality data is not achieved through sharing of data, at least not without appropriate Data Governance and structures and processes to address errors, reconcile variances, and manage expectations of 'fitness for purpose'.

The unexamined idea that data sharing will result in improved data quality skips over the question of what causes data quality problems. This is a "tip of the iceberg" situation. The sharing or pooling of data discussed in this proposal's questions is a visible end result; underneath that and not observed or examined in this relation of "data sharing" to "public sector reform" is the massive amount of underlying governance structures which create an environment in which quality information is an outcome. The design and implementation of systems in which accurate data is obtained, maintained, shared, ensuring that it is accurate, relevant, and up-to-date, is addressed by Data Governance. In order to ensure that data sharing is implemented successfully, proper governance of data must first be in place.

As leaders in Information Quality have commented in observing businesses: "*An ineffective common practice is to immediately start extracting and assessing data without confirming what you need. The result is multiple extracts and assessments before the relevant data is obtained*" (McGilvray, 10 steps to Quality Data

and Trusted Information: An Overview) – note how this aligns with the Data Protection principles of adequacy of data, relevance of data, and non-excessiveness of data.

Data Migration and Data Integration projects have a notoriously high failure rate. Research by Philip Howard in Bloor Research has identified risks of cancellation or overruns, in terms of time and/or cost, of data integration projects of almost 40[2]%.

Key root causes of failure in Data Integration projects, according to the Bloor research, are:

1. 18 % of respondents cited failure to adequately and accurately scope the data migration as a cause of failure. **Management of scope requires clarity on Data Governance roles/responsibilities/accountabilities**, and also requires clear guidance on the relevant and applicable business rules and legal rules relating to the data in question.
2. 13% cited data quality issues as a factor. Data Quality issues can be divided into issues arising from flawed assumptions about the quality of data in source data sets and into issues arising from failure to define and agree common metadata standards, reference standards, and data governance controls and practices to ensure quality data.
3. Unrealistic project expectations and a failure of Business/IT alignment are the next most cited causes of failure. These again have a significant Data Cultural and Data Governance dimension to them.

If we want improved data quality in order to help improve results, we must implement appropriate data governance. Information quality and privacy are both outcomes of proper information governance. Appropriate use of data for clearly defined purposes, with appropriate data governance and information quality controls can help improve efficiencies.

However, sharing of data without a fundamental reform of culture and governance and an evolution of work practices to support proper governance must be in place to create the possibility of effective data sharing. In the absence of common data standards, common data terminology, common metadata definitions, and other fundamental Enterprise Information Management components, it is more likely that sharing of data could contribute to inefficiencies arising from avoidable 'scrap and rework'.

Does it support Reform?

Public service reform will be supported by the proposal if, and only if, appropriate governance structures are designed and implemented in order to ensure data quality and protection. Effective sharing of information and improved information quality are both desired outcomes that may be driven by reforming the systems, processes and culture of the public sector in order to ensure proper governance of information, not the other way around.

Both Castlebridge Associates and Digital Rights Ireland would be of the view that respect for fundamental data privacy rights and compliance with Data Protection laws are, in and of themselves, a

[2] While high, this is significantly lower than the findings in earlier research by Bloor which put the failure rate at over 80%.

quality output of processing of data. Breaches of rights and breaches of privacy occur not because data is being processed, but rather as a result of the failure of management systems and Governance over the design and operation of that processing. If a 'Privacy by Default' ethos is adopted and Privacy by Design enforced as a fundamental principle in Public Sector information processing, *whether shared data or not*, we would suggest that many of the root cause issues identified for issues of information quality and information inefficiency could be addressed in that context.

It is to be hoped that the introduction of formalized structures and systems for the governance of, and accountability for, data would be greater adherence to already existing legislation and standards for data protection and data sharing.

What are the main areas where you believe that this can be achieved?

Please note that this question presumes a positive answer to the previous question and also presumes that sharing drives effectiveness.

We believe that the optimum areas for reform in the first instance will relate to:

- Culture and 'tone at the top' regarding the governance of data in accordance with commonly agreed principles, including the core principles of the Data Protection Acts and the Charter on Fundamental Rights.
- Implementation of data governance frameworks and initiatives to establish a common 'Business Glossary' and appropriate decision rules, rights, responsibilities, and accountabilities.
- Linking of Data Protection and Data Governance responsibilities to management accountabilities and cascading that to line of operations staff.
- Implementation of standardized scorecards for the measurement of information quality across key sectors *prior* to the sharing of data taking place.

Do you share the assessment that a new legislative framework for data-sharing is required? Please give reasons for your answer.

Although a legislative framework for the publication of certain aggregated data under the PSI Directive is required, the existing provisions of the Data Protection Acts operate to provide a strong control framework that necessitates clearly reasoned and governed decisions around legislative bases for sharing on a case by case basis.

We would query how this proposal in its current form would facilitate effective data sharing without violating the principles of proportionality, purpose specification, and other basic data protection principles including the ability to opt out of new purposes as defined in the European Interoperability Framework.

We would agree, however, that an improved legislative basis for the governance of data within the Public Sector may have benefits in terms of establishing a legislative basis for cross-functional data

governance, centralized management of data standards and data definition, and improved sanctions for breaches of policies and procedures for the protection of personal data.

We would submit, however, that a more effective culture of data protection and 'tone from the top' within the Public Service would help support reform while also allowing Ireland to establish itself as a country that "walks the talk" in terms of Data Protection compliance and practices. A legislative platform for effective cross-functional Data Governance that establishes clear lines of escalation and authority in the event of disputes or differences on the operation of how data is defined and governed and the application of appropriate controls, up to and including the creation of a formal "Data Governance Office" within the Public Sector to co-ordinate *all* data governance principles and practices could support such a culture change. However, this must be in addition to and in support of the general principles set out in the Data Protection Acts and not seen as a replacement for or a 'work around' for compliance with the Acts and the Directive and respect for fundamental rights under Article 8 of the EU Charter on Fundamental Rights.

In terms of the interoperability framework set out above, what do you see as the main obstacles to data-sharing, and how should they be addressed?

Leaving aside possible conflicts with the European Charter of Fundamental Human Rights, obstacles are likely to include:

- Lack of clearly agreed upon standards,
- Absence of common data definitions,
- unknown data quality levels in source systems,
- lack of 'data centricity' in thinking,
- failure of internal governance,
- lack of appropriately skilled resources (data governance, data protection, technology)
- absence of 'tone at the top' regarding issues such as Data Protection,
- lack of appropriately enforced controls on inappropriate access,
- lack of clarity on the purposes for which data is and will be shared/pooled, including the specific legal basis for sharing, with particular reference to the scope and extent of sharing.
- Inappropriate technologies applied to data sharing
- Absence of a cross-functional Governance framework for information

It is important to note that the industry average failure rate for Data Integration projects in 2007 was 84% (source: Bloor), this has reduced to just under 40% in 2011 research but the root cause for this failure rate invariably arises from a failure to address data standards, data definition and data governance.

We have mapped our initial assessment of obstacles to the high-level categories set out in the interoperability framework set out in the proposal document in Figure 3 below. We have also included a detailed review of some of the issues which will affect interoperability from page 15 in this document.

Interoperability Level	Description of Issue
Legal	• EU Directive 95/46/EC and the draft General Data Protection Regulation are both clear that processing must be for a specified and lawful purpose and must be adequate and not excessive. This will likely require case by case assessments as to whether the category of processing proposed goes beyond any original basis for the processing of personal data. • While common data request service types (assuming the technical implementation of a Service Oriented Architecture) requiring access to data can be defined, novel uses or variations on the scope of processing will require review and may require new legal basis. • The CJEU has made it clear that processing must not be disproportionate and has reaffirmed the importance of fundamental rights such as the right to rectification and erasure. These will pose challenges for Data Sharing absent a comprehensive and robust Data Governance framework.
Organisational	• The internal culture of data governance and data protection in the public sector has been directly criticized by the former Data Protection Commissioner. ***This is a key barrier to sharing of data as, unless public trust is restored, there will be resistance to increased sharing of data from the public.*** • There is no formalized cross-organisational Data Governance body to act as the "honest broker" to address issues of data standards, data definition, oversight of scope. This Data Governance Office *must* be outside the day-to-day management of data sharing (see our note on Segregation of Duties below) • There is a limited skillset in the Public Service in effective Data Governance and Data Protection oversight. Due to the policy of generalization of skills, experienced staff with experience of issues are often rotated out of Data Protection roles, resulting in a loss of knowledge and experience. • There is a lack of clear accountability for data protection failures in the public service in general.
Semantic	• There is no common Business Data Glossary for the public sector. It is inevitable that synonyms and homonyms exist for critical data items. • There appear to be no standardized metrics for data quality across the public service, based on a single agreed definition.
Technical	• Technical skill issues may arise • Inappropriate technologies are often used for sharing of and publication of data. • Inconsistent technology platforms for ETL/Data Interchange

Figure 3: Specific obstacles within the interoperability Framework.

How should these be addressed?

We would submit that the Data Sharing and Governance Bill is a unique opportunity for the creation of a cross-organisational Data Governance function that would, amongst other things:

1. Establish common standards for data, including the management of the Business Data Glossary for the public service
2. Establish standards and practices for Data Protection Officers across the public service, including:
    a. Standardised competency framework
    b. Common training and methodologies
    c. Co-ordination of a "Community of Practice" model for knowledge transfer and skills development among Data Protection Officers and other roles responsible and accountable for Data Governance functions in the public service, in the form of an Interdepartmental working group network.

We suggest that the scope of this office be broader than simply co-ordination of Data Protection and extend to ensuring the co-ordination of Data Governance standards and practices across the public service. This would recognize the fact of different levels of Data Governance maturity across the public service and provide a framework for establishing and implementing best practices, particularly if the operation of this office was to have a statutory basis as the 'honest broker' and point of reconciliation of variation and dispute on standards and practices for data management in the public service.

This model is similar to the structures that were implemented as part of the CPU to support the consistent implementation of FOI across the public service. It is also consistent with internationally established best practices for Data Governance and is similar to frameworks used by organisations such as the World Bank's International Finance Corporation and some of their peer organisations.

Establishing a centralized function for Data Governance would send a clear message regarding 'tone from the top' and would allow Data Governance decisions to be separated from the day to day actions of data management in individual departments. This is in line with the segregation of duties principles in Data Governance we discuss later in this document.

Do you have suggestions for how best to embed these data protection principles in the Data-Sharing and Governance Bill?

We would query why this would be integrated into a new bill.

The Data Protection Acts already constitute robust standalone legislative provision with a strong EU Treaty and Charter of fundamental rights basis. The problem rests in the failure on the part of public service organisations to respect the existing legislation and work to comply with it as a core part of culture. Creating another piece of legislation to codify principles that are wilfully and systemically ignored currently will not improve the situation.

We are of the view that respect for Data Protection principles needs to be embedded not in another piece of legislation but in the core operating culture and leadership of the public service and cascaded through Data Governance practices and controls.

Bluntly: there is already legislation that embeds Data Protection principles that is regularly ignored or sidelined in public service operations. Creating a second reference set of principles that are ultimately ignored will not address the issues of public trust and State compliance with EU Data Protection rules.

We would submit that:

1. Increasing general sanctions and penalties under the Data Protection Acts would present a strong message about their importance
2. Adopt a general sanctions for the unauthorized access of, disclosure of, or processing of personal data by any member of the public service, similar to the provisions s851A of the Taxes Consolidation Acts, but with *significantly* increased penalties for breaches.
3. From ministerial level down it must be made unambiguously clear that the Data Protection Acts embody a critical component of how to execute data-related change in the public service while maintaining public trust in those services.

The establishment of an appropriate system of governance of data in the context of any proposal or legislation for data sharing may go some way to supporting the embedding of the principles in the culture of the public service, particularly as the legislative focus at EU level is moving to Privacy by Design/Privacy by default and the CJEU is now increasingly clear on the importance of data privacy as a fundamental right of EU citizens. The judgment of the Court in Schrems v Data Protection Commissioner presents an extremely good synopsis of the nature and state of Data Privacy in Ireland post the Lisbon Treaty and should be referenced in this regard.

Do you have any ideas or proposals to ensure that consideration of these proposals benefit from wide public consideration, analysis and debate?

We would suggest that to ensure buy-in to the proposed changes, transparent and well-publicised debate engaging the public is advisable, including conducting wider surveying, focus groups, and awareness campaigns.

Key lessons should be learned from the response of the general public to non-transparent applications of data sharing in recent Public Sector and Private sector projects and discussion should begin sooner rather than later. A 'mushroom management' approach is likely to engender groundless fears over data sharing, but equally will result in well-grounded concerns being overlooked.

Engaging with civil society organisations such as Digital Rights Ireland would be one potential avenue.

In addition, engagement with professional bodies specializing in information quality, data governance, and data privacy may bring forward relevant experts and platforms for discussion. For example, Castlebridge Associates is hosting an event in collaboration with the International Association

Information & Data Quality and the Data Management Association in Dublin in November 2014, featuring international experts on Data Governance and Data Protection, which is considering a number of issues potentially relevant to this legislation. Similar events are planned in 2015.

How far can the Bill go in providing the necessary powers to share data while at the same time ensuring clarity around what exactly is permitted?

Given the recent rulings by the CJEU on the importance of proportionality and purpose limitation in the processing of personal data, and the requirement under Directive 95/46/EC that processing be for a "*specified* and lawful purpose" we believe that the actual scope of this bill to directly mandate the sharing of data and provide necessary powers for sharing of data is potentially limited to the formal establishment of a framework for ensuring that data sharing takes place in a well governed manner.

The legislation may support the sharing of data and provide clarity as to what exactly is permitted by establishing a formal basis for a cross-public service Data Governance function to drive common standards and data culture and provide an independent escalation point for decision or points of dispute.

We note that many of the provisions for which data sharing is proposed to be permitted under the Bill replicate existing grounds for the processing of data under the existing Data Protection Acts (statutory functions of a Minister, substantial Public Interest, investigation and detection of criminal activity). We welcome the enumeration of a number of examples of 'legitimate interests' which might be served by the sharing of data (collection of debts owing to the State, audit of effectiveness of a public body, identification and rectification of erroneous data). However, we would submit that the extent of the remit of the Bill would be limited to defining these purposes in general, perhaps in the form of a consolidation of existing data sharing purposes, while requiring any specific instance of sharing to undergo appropriate risk assessment and to be conducted under appropriate governance.

We also are of the view that the Bill could deliver benefits to public sector projects by mandating privacy impact assessments and privacy by design approaches throughout the life cycle of information, which would necessitate consideration of information issues and risks during the drafting of new legislation or the definition of new purposes and objectives for the processing of information. This is in line with the established Asset Life Cycle model for Information.

Life Cycle Stage	Potential Legislative Impact
Plan	• Bill could require an Information Risk Impact Assessment (Privacy Impact Assessment plus consideration of other potential information related issues and risks) on any new legislation or proposed change in process or work practice in the Public/Civil service. • Bill could mandate that the legislative process require a statement of information categories likely to be required/processed

Life Cycle Stage	Potential Legislative Impact
	• Bill could codify formal principles for data sharing and data governance to be considered and addressed during legislative drafting.
Obtain	• Bill could mandate a level of engagement with a formalized Data Governance body to ensure data is obtained from the correct source • Bill could empower Data Governance body to establish standards for data formats, applicable technologies, and approve vendors for data sourced from third party sources.
Store/Share	• Bill could mandate role for Data Governance body in setting standards for data storage including security • Bill could mandate role for a Data Governance body to act as arbiter in decisions about granting access to data for sharing purposes • Bill could mandate role for Data Governance body to manage and maintain centralized Business Data Glossary for Public/Civil service so that correct data shared in the correct way. • Bill could mandate a role for Data Governance body to maintain a register of what data is shared between what bodies, in what format, and for what purpose – data sharing not registered in this way would need to be considered unlawful as it would not necessarily be auditable and it would be impossible to accurately impact assess changes to systems feeding shared data processes without such a register.
Maintain	• Bill could mandate a role for Data governance body to act as arbiter in disputes about reconciliation of competing records of fact between two areas • Bill could mandate Information Stewardship as a concept wherein holders of "system of origin" data would be required to consider other potential consumers of that data when changing data or systems • Bill could mandate a role for Data Governance body to maintain Business Data Glossary for public service.
Apply	• Bill could mandate role for Data Governance body to ensure that sharing activites are undertaken in compliance with relevant legislation • Bill could mandate a *de minimis* policy regarding data sharing that would require the minimum data necessary to achieve purpose is shared and the appropriate level of sharing to achieve goal is applied
Dispose	• Bill could mandate a role for the Data Governance body to centrally define standardized Data Retention/Destruction policies for public

Life Cycle Stage	Potential Legislative Impact
	sector bodies based on existing collective best practices and legislative requirements • Bill could mandate a role for the Data Governance body to review on a regular basis the operation of and justification for any data sharing. • Bill could mandate role for the Data Governance body to provide updated guidance on specific Data Retention and Destruction standards as part of Privacy Impact Assessments or Regulatory Impact Assessments.

Figure 4: Information Asset Life Cycle and Legislative Impact

"Should both personal and sensitive personal data (within the means of the Data Protection Acts) be covered by these provisions? If so, what extra protections are required around sensitive personal data?

This could be counterproductive to exclude or differentiate either category of data as it is already dealt with in the Data Protection Acts.

Unless the intention is to include additional rights, duties, or obligations this would create redundant legislation and could in fact be confusing once the EU Data Protection Regulation comes into effect which would supersede any national legislation in this regard.

We would suggest however that this legislation would be an opportune time to introduce a standardized set of sanctions across the public service for breaches of the Data Protection Acts by public and civil servants. This could be introduced as part of a core Data Governance strategy which the Bill would underpin.

We would also propose that the additional protections for sensitive personal data could be addressed through an appropriated and transparent Privacy Impact Assessment process that should commence at the planning stage of any initiative, ideally from the point of policy definition. This would ideally see information risk and data privacy impacts being subject for consideration from Regulatory Impact Assessment stage onwards, with a key focus being on identifying the appropriate level of sharing necessary to achieve the purpose proposed. This would be in line with obligations under Article 8 of the Charter of Fundamental Rights to ensure any processing is proportionate.

Should the Oireachtas have a role in overseeing or approving some types of data sharing arrangements? If so, how extensive should this role be?

We assume that what is proposed here is a Data Governance role for the Oireachtas. It is normal practice in commercial Data Governance for there to be some level of reporting to the Executive on progress and some avenue of escalation to the Executive for resolution of otherwise irreconcilable differences re: definitions, standards, and appropriate business rules.

However, we would be of the view that this would be more appropriately served by having a clear and properly constituted Data Governance Office function with responsibility for cross-governmental

Data Governance within a formalised Data Governance structure. The nature of the decisions that would be taken in the context of data sharing are far reaching with significant impacts on citizens and fundamental rights and it would not be appropriate to have them subject to short-term political expediency.

We would submit that the mechanism by which the Oireachtas can have a role in approving or overseeing some types of data sharing would best be met by having a transparent Data Governance framework within which a clear decision point existed to invoke the existing powers of the Oireachtas to pass legislation permitting specific instances of data sharing arrangements and, in so doing, specifying additional controls or oversight functions.

We would also submit that for other forms of Data sharing, the appropriate mechanism would be to have the Data Governance Officer function accountable to an appropriate Dail Committee, as is currently the case for civil and public service functions. Consideration may need to be given to the mechanisms for accountability where data is shared with external bodies for the purposes of executing functions on behalf of the State to ensure that the Data Governance Office and any Oireachtas oversight can execute effective governance over entities processing shared data on behalf of the State.

What other specific data-sharing arrangements should be considered?

As per the alternative definition of data sharing which we set out on page 20 of this document, we are of the view that there are three generic forms of "data sharing" that might take place in any organization:

1. A 'case by case' basis for the validation and verification of data;
2. a defined batch processing basis for the validation, verification, and updating of specific populations of data;
3. or as once-off consolidation and integration of disparate data sets to form a new, shared, master data repository. This may also be called Data Pooling or Data Consolidation.

When considered in light of these three archetypes, there are few data sharing arrangements that are not covered. However, we would be concerned that data sharing between Public Sector and Private Sector organisations (for example the provision of Revenue data to Irish Water under section 26 of the Water Services Act 2013) currently is not subject to any oversight and we would ask that the Data Governance and Sharing Bill ensure that appropriate governance controls are defined and put in place to ensure a *de minimis* sharing of data between Public/Civil Service organisations and Private Sector businesses, with a particular focus on preventing or mitigating the risk of misuse or abuse of public service data by private sector firms, ideally by ensuring they do not have excessive data for the specific type of processing that is required for their purpose.

Notwithstanding the existing Single Customer View which is maintained by DPER on behalf of the DSP, we are strongly of the opinion that the focus of legislative reform in this area should be on

ensuring the correct Data Governance environment and framework is put in place to allow local successes to scale securely in an operating environment that enables balanced and appropriate data sharing and data interoperability rather than focusing on any single mechanism or arrangement for sharing of data. Such considerations should be design decisions in the implementation of sharing, not policy and principle decisions about the activity of data sharing.

Establishing a clear Data Governance function to drive Business Data Glossary, data standards, and ensure that decision making models for the selection of an appropriate format for data sharing and volume of shared data, in line with agreed principles (including Data Protection compliance requirements) would be a more sustainable reform objective of the legislation.

The selection and definition of a specific data sharing arrangement should be managed by the entity proposing the purpose for which the data would be shared. How the arrangement is defined, designed, and executed should be governed by the principles established by common Data Governance function.

Master Data Management is complex in itself. Establishing standard categories of Master Entity, common metadata standards, data format rules, data definitions, and defined protocols for case by case data querying for specific purposes would enable a Data Exchange layer to be implemented that could provide specific data in response to specific queries while mitigating risk of over-reaching access. It would also have the advantage of driving accountability for local data quality and data governance within each department but based on shared standards.

With regard to Data Protection compliance, we would recommend that the Irish Government implement a standard similar to BS10012:2009, the British Standard for Personal Information Management Systems, as a reference benchmark for governance of Data Sharing schemes and data processing in general.

Should a general provision be added to enable widespread access to information on Births, Marriages and Civil Partnerships?

What is meant by "widespread access" needs to be defined here. We are unclear as to why this is a specifically distinct category of data in this regard. GRO data could be made accessible via an API in a Service oriented architecture environment. For services where details of birth or notice of death are required one would assume this data is already being accessed, particularly after the issues with the Electoral Register in 2006. If it is not, and if a standard API-type mechanism for accessing data from the GRO does not exist, it would lend strength to our recommendation for a single Data Governance body to co-ordinate the definition of appropriate sharing practices.

A key element of the response is an identification of what level of sharing is required. We refer to our proposed alternative definition of Data Sharing on page 20.

- If verification is required of a person's registered marital status, fact of birth registration, fact of death, or other data point, this is a case-by-case validation check that does not require detailed data transfer
- If additional data is required to update data about that person (e.g. to update a date of birth registration, date of marriage, or date of death) that is a category of data sharing defined in our definition
- If GRO data to be consolidated with a new master data register that is a third category of data sharing a defined in our alternative definition and would require more scrutiny and different governance.

We would also point out the potential for errors or for unauthorized disclosure of sensitive personal data in instances where the name that a person uses in day to day life does not match their registered birth name, such as in the case of a transsexual individual or a child of a divorced or bereaved couple who has taken the surname of a step-parent. Removing the human interface from scenarios such as this could result in certain segments of the population encountering additional issues engaging with State services.

"Some jurisdictions are examining the concept of an "honest broker" or "trusted third party" – this would have the power to accept any data and process it on behalf of public bodies, while preventing the public body from accessing the raw data. Is this a concept that could usefully be included in the Bill?

The only example of a public sector entity for data sharing on the basis described in the question is the Honest Broker Service established in the Department of Health, Social Services, and Public Safety in the Northern Ireland Executive. There are examples of this form of intermediary entity existing in academic and commercial clinical research however, and it does provide a buffer between requesting entities and the original source systems of record which can help minimize data exposed or shared.

We note that, in almost all examples we looked at as part of framing our response to this question, that the data being discussed was anonymized, pseudonymised, or aggregated data. Specifically, the website of the DHSSPS HSC Honest Broker Service (HSC HBS) states that:

> *"The HBS will enable the provision of anonymised, aggregated and in some cases pseudonymised health and social care data to the DHSSPS, HSC organisations and for anonymised data for ethically approved health and social care related research"*

This sharing of anonymized and aggregated data is conducted by the HSC HBS under the oversight of an Information Governance Board that is responsible for ensuring good governance of data and ensuring that data is provided in compliance with Data Protection regulations and standards.

Whether an "honest broker" could be usefully introduced under this Bill depends on the definition of "honest broker" in the context of Data Sharing and Data Governance. If the definition is a structure similar to the HSC HBS – an entity that aggregates data and provides aggregated/anonymized data sets

to requesting bodies, then we would respond yes, and we would welcome the introduction of a 'one stop shop' for aggregated data as it would reduce the need for multiple points of data sharing for similar purposes. We would also submit that this honest broker function would necessitate the establishment of the Data Governance Office that we have referenced in response to earlier questions to:

1. Ensure common business glossary across potential data sources such that the correct data was combined in the correct manner in aggregated data.
2. Ensure that anonymization/pseudonomyisation practices and protocols were appropriate and complied with
3. Ensure that appropriate controls and protocols are in place to prevent unauthorized access across multiple systems in a way that would breach Data Protection principles
4. Process requests for new forms or formats of aggregated data and ensure they are subject to appropriate privacy impact assessment and other controls.

Subject to appropriate controls it may also be the case that an 'Honest Broker' model could be used to facilitate specific reusable data sharing components, along the lines of a Service Oriented Architecture (SOA) approach. Specific commonly occurring purposes for sharing of data could be defined and a standardized interface implemented and provided by the Honest Broker, subject to appropriate Data Governance and related controls.

The Data Governance function would ideally perform an "honest broker" function in respect of data definitions, standards, and disputes re: interoperability between source data repositories. This is in line with the general role of Data Governance organisations in a variety of private and public sector organisations such as Walgreens in the US or the International Finance Corporation in the World Bank and which Castlebridge Associates has recommended in a leading EU institution.

We note that the United Kingdom's Government Digital Service division has developed a strong capability in developing data access and data sharing services across the UK Government sector and has produced a significant amount of data about the cost inherent in and cost reductions possible in Government services in the UK. They are a centralized solution design organization operating across multiple UK Government departments to deliver standardized data access mechanisms.

Tellingly however, their strategic plan for 2014 to 2015 stresses the importance of having the "necessary governance in place" to enable them to deliver hoped for benefits from digital services investment in the UK public sector (Government Digital Service).

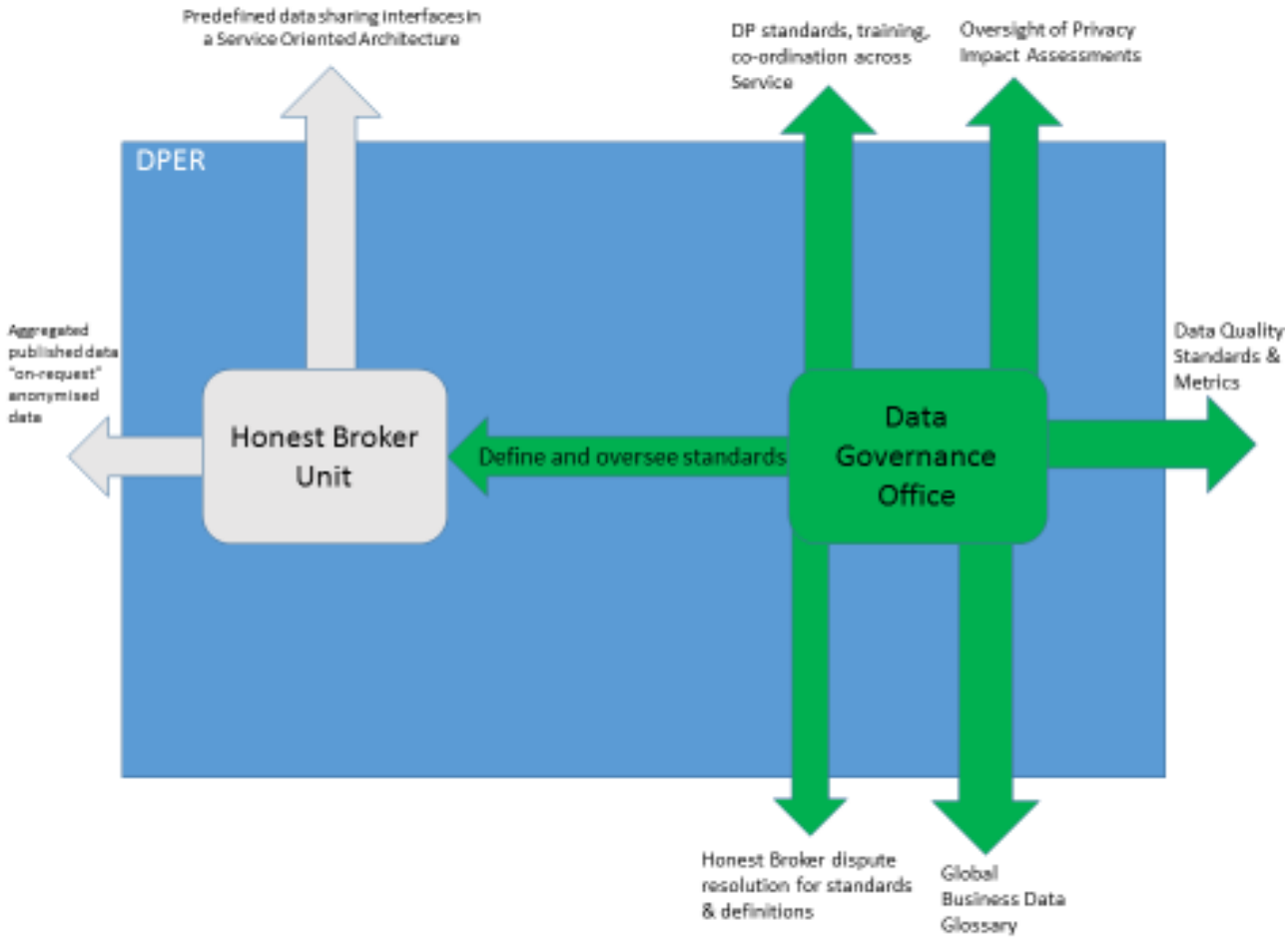

Figure 5 A potential Honest Broker Governance model

A key root cause for the failure of data sharing and data integration projects of this kind is a failure to address Data Governance, Data Quality, and 'human factors' elements. Examples of such failures in the public sector would include PPARS, REACH, and the apparently on-going data quality challenges faced by PeoplePoint.

The creation of any large "single source" repository of data could raise questions of proportionality of processing and data minimization under Directive 95/46/EC and Article 8 of the Charter of Fundamental Rights, as well as creating increased risks of loss or damage arising from information security breaches. It is imperative therefore that the benefit case for sharing in this way be clearly defined and articulated and appropriate governance put in place *prior* to the development of new capabilities. Key lessons can be learned from the failure of care.data in the UK and the negative publicity associated with it.

In many circumstances compartmentalization of data, with 'sharing through validation' checking serves a valuable function, allowing processes to be automated with minimal sharing of data and

minimized risk of data breach. This *de minimis* approach could be applied to the development of standard validation purpose protocols which could be reused on approval by a central Data Governance function.

"Should specific provisions relating to the sharing of "anonymised" data be included?

Sharing of anonymised data reduces risk of breaches of data privacy rights. However, anonymisation is neither absolute nor a panacea, particularly in this age of "Big Data".

To quote from a recent Castlebridge Associates Whitepaper (O Brien):

> *"Recent research has highlighted the risks to personal privacy arising from the ability to analyse large volumes of even anonymized data. For example:*
>
> - *80% of Netflix users can be re-identified from an anonymous data set based solely on when and how they rated movies they had rented* (Narayan and Shmatikov)
> - *Researchers analysing anonymous Facebook "Likes"* (Kosinskia, Stillwell and Graepel) *were able to:*
>   - *Identify sexual orientation in men with a .88 probability*
>   - *Distinguish between African Americans and Caucasian Americans with 0.95 probability*
>   - *Distinguish between Republican voters and Democrat voters with a 0.85 probability"*

These weaknesses with anonymized data are not new. The Castlebridge Associates whitepaper continues:

> *"As far back as 1990, researchers demonstrated how it was possible to re-identify 87% of the US population based only on the five digit Zip code, gender, and date of birth* (Sweeney). *In that context legislative restrictions or mandates to anonymize data are toothless where organisations lack controls to prevent re-identification of that data. Those controls constitute a definable set of decision rights, responsibilities, and accountabilities which must be defined in organisations to ensure that the wrong things are not done with the right data."*

In that context it would be appropriate for the Bill to provide a firm legislative basis for Data Governance controls preventing the re-identification of anonymised data sets and requiring data sharing arrangements to ensure that appropriate controls and governance is in place with all parties to a data sharing arrangement to mitigate the risk of re-identification.

In order to support the accountability requirement of Data Governance, the Bill should include clear and robust penalties for unauthorized re-identification of anonymised data by, for example, combining multiple anonymised data sets to create an identifiable entity. Furthermore, operational governance of data sharing should require that any key data capable of re-identifying data (e.g. look up tables for pseudonymised data, encryption keys for anonymized data, or similar) should be kept separate from

the actual data itself. This is a basic organizational and technological step that can be taken to protect data.

In this context it is worth bearing in mind the Article 29 Working Group Opinion on the definition of Personal Data and the definition of Personal data in the draft General Data Protection Regulation as "personal data" is no longer simply names and addresses but spans a range of data that would enable an individual to be singled out.

Do you agree that "The problem [of data governance] is therefore primarily one of better implementation, rather than an absence of legislation."?

No. Data Governance is a cultural and procedural issue that may be defined as, "A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods". Neither this question nor the overall proposal address Data Governance as defined here in a meaningful way.

In particular we would question the ultimate value of a 'point solution' for data governance in this Bill focused simply on data sharing. Case by case data governance requirements are already dealt with within existing legislation and the implementation of data sharing agreements. The sharing of data between SUSI and Revenue is a key example, with very specific terms introduced in data processor agreements on the SUSI side regarding the scope and nature of the processing[3].

We believe that, to be effective and to support effective reform of the Public Service, this Bill must introduce a general framework for Data Governance that supports standardization of methods and procedures, develops a *lingua franca* for the meaning and purpose of common data elements in the Public Service, and ensures that there is a robust framework of decision rights and responsibilities supported by actionable accountability.

Regarding the provisions that are considered likely for inclusion in the Bill:

Provision	Comment
Transparency	The publishing of data sharing arrangements and informing individuals of the legal basis for the processing of their data is to be welcomed, indeed it is a requirement under the "Fair Obtaining/Fair Processing" obligations under Directive 95/46/EC

[3] Castlebridge Associates provides Data Protection and Data Governance advisory services to both the CDETB and SUSI and was directly involved in the Data Protection aspects of SUSI from very early. We directly negotiated and defined the Data Governance framework between SUSI and Revenue.

Provision	Comment
	We would be of the view however that clear standards would need to be implemented regarding the format and structure of publication as part of Data Governance. We would also be of the view that this would be best met through the creation of a central Data Governance Office, and that it would be more 'customer-friendly' if, rather than having to seek information on a myriad of public sector websites, that a single central searchable public register was established. This could be a publicly accessible extract of the Business Data Glossary maintained by a Data Governance Office.
Record-Keeping	The requirement to formally document data sharing arrangements, specific governance arrangements, and other information is welcomed. However it will not support efficiency or reform if each public sector body can define and prescribe their own format for the recording and presentation of this information. We would submit that effective reform of public sector data management practices would be best supported by the establishment of a Data Governance Office to define standards, promote best practices, and maintain a centralized searchable register. This would have the additional benefit of supporting reuse of defined common data sharing mechanisms and ensuring common oversight and accountability.
Mandatory PIA	We welcome the inclusion of mandatory Privacy Impact Assessments in this Bill. However, it is a recommended best practice that a centralized repository of Privacy Impact Assessments be established to promote cross-organisation learning and reuse of concepts. This is a recommended best practice from the Canadian Office of the Privacy Commissioner and, in light of the provisions in Article 33 of the current draft Data Protection Regulation permitting sets of similar processing to be covered by the same PIA, it would drive efficiency by having a single reference library. Decisions to bundle similar processing to be covered by a pre-existing PIA would, however, need to be subject to transparent and effective governance and may require a Risk Assessment as per Article 32 GDPR This would be a key role for a Data Governance organization in promoting agreed upon models for decision rights, responsibilities, and accountabilities. It would also improve efficiency by eliminating the need for public sector bodies to 'reinvent the wheel' for each iteration of data sharing.

Provision	Comment
	The creation of a Data Governance Office would facilitate the regular post-implementation review of data sharing to ensure compliance with PIA undertakings, as is required under Recital 74(a) of the European Parliament agreed text for the Draft Data Protection Regulation, and Article 33a of the proposed Regulation (European Parliament).
Prior notice of adverse action	We welcome this provision, which relates more to the operational processes which would act on shared data than on the process and activities of sharing data or the actions of governing the sharing of data. On our reading, this would appear to introduce a manual action for notification in the event of adverse action which would satisfy the requirements of Section 6B of the Data Protection Acts 1988 and 2003, while giving the Data Subject an opportunity to exercise their rights under Section 6A to object to the processing that is likely to cause damage or distress.
Lead Agency	While recognizing the New Zealand model, we are of the view that this method could be implemented through the inclusion of record keeping provisions in any legislation requiring or enabling a specific instance of data sharing. We are also of the view that the practicalities of negotiating a lead agency in each case could lead to delays in implementing data sharing and could lead to inconsistencies in lead assignment between agencies sharing different data for different reasons. We would propose that better model would be that the retention of records be the responsibility of a Data Governance Office who can define standards and ensure oversight. This would be similar to the role of a "Data Contract Librarian" in traditional IBM MQ-Series Data Contract environments and would support reuse, transparency of publication, consistency, and efficiency. Data Sharing agreements would be between a "Requesting Party" and a "Providing Party". The Requesting party would equate to a "lead agency".

The New Zealand Model

In formulating our response to this question we conducted research on the operation of the New Zealand Approved Information Sharing Arrangements model, as set out in Part 9A of the New Zealand Privacy Act, as amended by the Privacy Amendment Act 2013 (New Zealand Parliament). This legislation bears a striking similarity to the Data Sharing provisions currently under review.

We note that the New Zealand legislation requires the publication of a central register of Data Sharing arrangements under Schedule 2A of the Acts. This schedule is under the oversight of the New Zealand Privacy Commissioner. An analogous schedule of uses of data exists under Section 262 of the Social Welfare Consolidation Act 2005 where all users of PPS Numbers must be listed under Schedule 5 of that legislation. The Department of Social Protection's Client Identity Service has published a register of users for the PPS number. However, in the absence of a formal statutory basis, this register is incomplete and out of date. Given that this is the public source of information about who is entitled to use PPS Numbers, and indeed the *only* source of information other than trawling through legislation, we would submit that the management and maintenance of this Register is a critical piece of effective Data Governance for public sector data which is effectively ignored in practice.

The New Zealand legislation requires that any party processing shared data provide prior notice of adverse action. This echoes the provision in the proposed Bill. We note that the New Zealand legislation allows for a 10 working day window for an individual to dispute the correctness of personal information used to make a decision. This aligns with the rights of the individual under Section 6A of the Irish Data Protection Acts 1988 and 2003.

The New Zealand model does not codify the allocation of responsibility or accountability in the event of a breach of a data sharing agreement. A breach is viewed as being legally equivalent to a breach Data Protection principles in the Privacy Act and is dealt with accordingly. Given the former Data Protection Commissioner's parting comments on Irish public sector attitudes to and enforcement of Data Protection internally, this does not instill confidence that a Lead agency model as operated in New Zealand would work in the Irish Public Service.

It is interesting to note that the New Zealand model distinguishes between Information Sharing and Information Matching (http://www.privacy.org.nz/information-sharing/information-matching-reports-and-reviews/) This is in line with our concerns regarding the current definition of data sharing in the proposed Bill which conflate a number of different types of information exchange under a single "data sharing" heading.. A separate register is kept of data matching that is taking place and under what legislative provisions. We believe this would be a worthwhile addition to the overall governance of and transparency of existing data interchange in the Irish Public Service, as currently there is no readily accessible central register of any information interchange and its statutory basis in the Irish Public Sector. The New Zealand model in this instance goes beyond simply listing the legislative section and processes that apply the information, but includes a large amount of business and technical metadata detailing the purpose for the matching process, the data used, and operational statistics.

We also note that the New Zealand model currently has only two Approved Information Sharing arrangements in place, with only one of them having had any reporting obligation in the most recent financial year. There has been insufficient volume of Information Sharing arrangements and

insufficient duration of operation for the full range of potential issues with this approach to have emerged. It must therefore be concluded that there is therefore insufficient evidence available at this time to confirm the effectiveness or otherwise of the New Zealand model for information sharing in the Public Sector.

We would expect the specifics of implementation of the New Zealand model to evolve as the number of and complexity of information sharing arrangements increases and specific challenges arise to the effectiveness of the lead agency model. We suggest that, rather than copying verbatim the New Zealand model, the Data Governance and Sharing Bill incorporate proven Data Governance practices from other private and Public Sector organisations as well as taking relevant inspiration from the New Zealand model.

We also note that the oversight of Information Sharing in New Zealand rests with the Privacy Commissioner. While we recognize this may be appropriate in the New Zealand context, we would be of the view that this would be inappropriate in an Irish context for a number of reasons including:

1. Requirement to maintain effective segregation of duties
2. Narrow focus on *just* Data Privacy issues rather than wider issues of data interoperability, standards etc.

We address this aspect in more detail in our response to the next question.

Legislation vs Implementation

As to the question of legislation vs. implementation, this is potentially a false dichotomy. Legislation already exists, however culture, values, and clearly defined and applied decision rights and accountabilities to drive application of and adherence to legislation are absent. Addressing that will result in better implementation.

We will further expand upon the definition and function of data governance in the "Defining Data Governance" section of this document.

"Should the Data Protection Commissioner have a role in monitoring and reporting on compliance with these governance provisions?

The Data Protection Acts 1988 and 2003 already give the Data Protection Commissioner a role in the monitoring of compliance with the requirements of Data Protection legislation

If the question here is whether the ODPC should have a direct role in oversight of the governance of data management in public sector organisations, we would point out that the DPC does not have that role in relation to private sector organisations. It is important that the role of the DPC as an entity independent of government and of the public service is maintained.

We would propose that the role of monitoring and reporting on the operation of data governance provisions should rest with a Data Governance Office within the Public Service, which in turn would be subject to Oireachtas oversight and would be a participating stakeholder in audits and reviews by the Data Protection Commissioner.

The proposed EU Data Protection Regulation contains a requirement for data controllers and processors toshow that they have a documented data governance framework in place and to be able to produce evidence of its effective operation to a Data Protection Authority. If this Bill contained a similar 'demonstrate and evidence' requirement for Public sector data governance it would create an appropriate role for the DPC and would align with impending changes in Data Protection law and practice across the EU.

However, we are of the view that it would constitute a breach of the principle of segregation of duties and potentially compromise the operational independence of the Data Protection Commissioner if they were to be directly engaged in the day to day monitoring and reporting of data governance operations in the public sector, particularly as they do not have that role in the private sector.

The operational focus of the ODPC should be directed on ensuring the full, fair, and consistent operation of and regulation of Data Protection law within the State. We believe a new, separate, oversight function spanning the Public Service and ensuring standardization of policies, practices, data definition, and governance structures would better support the objectives of data governance, enable effective oversight of data sharing, and provide a platform for data-driven reform of the Public Service.

In what circumstances should a Department be able to "opt out" of the transparency requirement for a particular data-sharing arrangement?

Given the fact that fair obtaining and fair processing obligations under Directive 95/46/EC and the draft General Data Protection Regulation require transparency, we would submit that the circumstances under which any organization can 'opt out' of the transparency requirement should be extremely limited. The impact on transparency should be proportionate to the risk being mitigated by the opt-out.

Issues such as national security, or operational security of Defence Forces personnel or members of An Garda Siochana would obviously be relevant here. However, we would propose that a request for opt-out would need to be subject to a rigorous examination by a Data Governance Board and formally approved to avoid it being abused and the transparency principle being worked around in practice. In the context of the types of scenario where transparency might need to be over-ruled, we would be satisfied that provisions in the Freedom of Information Act would allow for documented decisions to be taken that would be part of the record for Data Governance purposes but would not be disclosed such as to jeopardise security.

As the scope of proposed data sharing in the Bill is confined to public service organisations within the State, we would be of the view that issues such as 'commercial confidentiality' would not be relevant and should not form grounds for opting out of transparency requirements.

Is it practicable for these arrangements to apply to all existing data-sharing arrangements, not just new ones?

Yes, not only is it practicable but it is desirable and would be a key building block of effective governance. Given the stated intention in the legislation to publish certain details of data sharing arrangements in keeping with the transparency requirement, and the intention to require effective record keeping and mandatory privacy impact assessments we would suggest that this is a prime example of why a centralized Data Governance function is required.

We would propose a transition structure be implemented where by existing sharing arrangements are:

1. Registered with the Data Governance Office, with basic information re type of data being processed, requesting entity, providing entity, and summary of purpose and statutory basis
2. Subjected to a privacy impact audit to identify proportionality, quality and adequacy of documentation and governance controls, and clarity of legal basis.
3. Assigned a remediation plan to address gaps identified which may pose an information privacy or information quality risk, or to promote reuse

Existing Data sharing arrangements could then be clustered and analysed to identify commonly occurring patterns and purposes for data sharing which could then be instantiated as standardized repeatable services with a general statutory basis, subject of course to the obligations of *de minimis* rules and proportionality requirements.

Replication and duplication of sharing could be identified in this way and rationalization of processes and data sharing protocols would be supported. It would also provide a basis for the development of common standards for data definition and data governance across the public service. It is possible that other areas of waste (information scrap and rework, data sharing that is redundant and no longer acted on etc.) could be identified through this process.

The method of implementation of the centralization of information would need to be addressed in the scoping and definition of a program and the definition of the authority and mandate of a Data Governance Office, some of which might be addressed in legislation (authority and mandate) and other elements of which will be operational in nature.

Particular attention will need to be paid to scenarios where data is being shared or has been shared with private sector organisations to ensure that the data is being processed and/or retained in accordance with the required purposes, in compliance with Data Protection requirements, and subject to appropriate governance and oversight.

Is the base register concept a useful one?

The base register concept is, in essence, a Master Data Management definition of a System of Record. The identification of a System of Record is a good practice in an MDM context and is, in general, useful. However, MDM systems of record are impacted from an information quality perspective by the fact that they may not contain all necessary data for downstream applications and, furthermore, their internal data quality critieria are often defined from the perspective of the business area (Department) that has created that System of Record. This can occur in intra-organisation data sharing as well as inter-organisation data sharing.

One key issue will be the "fitness for purpose" of core entities if data changes from a "client" department, which are necessary for the functioning of that department are not applied by the "owning" entity. This will necessitate a different technical and operational implementation of data sharing. A key lesson from private sector "Single View of Customer" type initiatives is that there are often multiple views of a particular entity, depending on their relationship to an organization and the purposes for which data is being processed. As this is often a fluid issue, it would be inappropriate for Base Registers to be specifically defined in the legislation, particularly as the organization structure of Government Departments can be changed on the whim of a government without necessarily assessing the impact on data flows and data controls.

We would be of the view that a transparent process where by a Data Governance Office could be empowered to decide on MDM Systems of Record and would have an oversight role in the development and execution of processes that access data from or update data into these Systems such that any 'satellite' data marts of data that are linked to the MDM system of record are properly governed and controlled. The determination of MDM systems of record/base registers could be published by the Data Governance Office and, should it be so required, be subject to a relevant Ministerial approval (e.g. the Minister in whose Department the DGO sits could approve new Systems of Record).

This would remove the need to define now future candidates of MDM systems of record and allow for 'governed flexibility' while maintaining a framework for 'honest broker' resolution of differences in data standards, data definition, business rules for deriving or calculating data, or controls over processes to access or use data between different organisations via the Data Governance Office.

There are ample references available regarding the operational implementation of Data Governance frameworks for MDM and Castlebridge Associates would be happy to discuss specific details on request.

What other base registers could usefully be defined?

As we have responded previously, we believe it is inappropriate for the Bill to formally enumerate base registers or to attempt to establish and exhaustive list in legislation. It would be appropriate for a Bill to

provide definitive oversight and governance protocols for the formal establishment and retirement of such base registers.

The definition of an MDM (Master Data Management) 'System of Record'/Base Register brings with it requirements to ensure effective governance of that information asset. We believe it is more appropriate that a Data Governance Office be empowered, by way of a transparent and published process, and potentially subject to Ministerial or Oireachtas approval, to define MDM Systems of Record as part of the definition of and operation of decision rights and accountabilities within a Data Governance framework.

We strongly feel that this function should be centralized to facilitate stronger oversight, consistent governance, and easily accessed transparent record-keeping, and to facilitate accountability to both the Data Protection Commissioner as Regulator and the Oireachtas.

Queries arising from items not covered by questions asked in the proposal:

Requirements for unambiguous identification

We would ask why it is considered that this requirement is not met currently through section 262(9) Social Welfare Consolidation Act 2005? The requirement to unambiguously identify people is not a function of a service or a by-product of data sharing, but is rather a requirement of a process, which in turn is a specifiable purpose for processing and therefore something that can be dealt with through the current mechanisms for data sharing on a defined statutory basis.

We note that the REACH initiative in the then Department of Social and Family Affairs attempted to provide a platform for unambiguous identification across the Public Service and failed. The C&AG cited failure to address Governance issues as a key root cause for this failure.

Open Data and Reuse of Public Service Information

We believe that what is proposed in this document goes beyond the scope of the PSI Directive in a number of areas and goes beyond what is required for Open Government Partnership processes. As the proposal specifically excludes sharing of data with other EU government bodies, which is a requirement under the PSI Directive, we would query whether the proposed bill is compatible with the Directive.

Much of what is proposed may constitute a re-use of public service information in the context of intra-organisation data sharing and a "capture once-use often" vision, but that is a distinctly different objective from the requirements of the Public Service Information Directive. For both requirements to co-exist we submit that a focus on the end-to-end life cycle of information and its governance is essential to ensure high quality and trusted information for what we would term 'operational processes' within the Irish Public and Civil Service, as well as ensuring accurate and trustworthy aggregation of data for external reporting under obligations such as the PSI Directive or the Aarhaus Convention.

Bibliography

Data Governance - in Practice & Over Time. Perf. Head of Information Quality, IFC Elizabeth Davis. Presentation to Canadian Information & Records Management Association, Toronto. 2008. http://www.irmac.ca/0809/Data%20Governance%20-%20In%20Practice%20and%20over%20Time.ppt.

Deming, W. Edwards. *Out of the Crisis*. MIT Press, 1986.

European Parliament. "European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such dat." 12 March 2014. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212.

Government Digital Service. "GDS Business Plan April 2014 to March 2015." 07 2014. *Government Digital Service.* https://www.gov.uk/government/publications/gds-business-plan-april-2014-to-march-2015/gds-business-plan-april-2014-to-march-2015. 14 09 2014.

Hawkes, Billy. "Data Protection – the State, Technology and other Challenges." IIEA, 21 07 2014. http://www.iiea.com/events/keynote-address-billy-hawkes.

Health Information & Quality Authority. "Guidance on Information Governance." HIQA, 2012.

—. "Guidance on Information Governance." HIQA, n.d.

Howard, Philip. "Data Migration." 2007. http://bloorresearch.com/research/white-paper/data-migration/.

Kosinskia, M., D Stillwell and T Graepel. "Private traits and attributes are predictable from human behaviour." *Proceedings of the National Academy of Sciences of the United States of America*. 2013. http://pnas.org/content/early/2013/03/06/1218772110.full.pdf+html.

McGilvray, Danette. "10 Steps to Quality Data and Trusted Information: An Overview." n.d.

Narayan, A and V Shmatikov. *Robust De-anonymization of Large Sparse Datasets*. 2008. http://www.cs.utexas.edu/~smhat/shmat_oak08netflix.pdf.

New Zealand Parliament. "Privacy Act 1993." n.d. http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

O Brien, Daragh. "Everything is Outcomes: Reframing Information Quality, Data Protection, and Data Governance for a Big Data World." 2014. http://castlebridge.ie/products/whitepapers/2014/04/everything-outcomes-data-protection-and-big-data.

Office of the Comptroller & Auditor General. "eGovernment - Comptroller & Auditor General Special Report." 2007. http://www.audgen.gov.ie/documents/vfmreports/58_eGovernment.pdf.

Sweeney, L. "Simple Demographics often identify people uniquely." *Data Privacy Working Paper 3*. Carnegie Mellon University, 2000. http://dataprivacylab.org/projects/identifiability/paper1.pdf.

The Data Governance Institute. *The Data Governance Institute*. n.d. http://datagovernance.com. 27 08 2014.