safe

security action for everyone

Data Protection Impact Assessment– template for report

Information Assurance and Risk

March 2018

Scottish Government
Riaghaltas na h-Alba
gov.scot

Data Protection Impact Assessment (DPIA) – template for report

This template was developed by the SG Data Protection and Information Assets team.

This template was last updated in March 2018.

Before conducting the Data Protection Impact Assessment, please refer to the guidance that accompanies this template.

1. Introduction

The purpose of this document is to report on and assess against any potential privacy impacts as a result of the commencement of the Digital Government (Scottish Bodies) Regulations 2018.

2. Document metadata

2.1 Name of Project: The Digital Government (Scottish Bodies) Regulations 2018

2.2 Author of report: Data Sharing Unit; Data, Statistics and Outcomes Division, Digital Directorate

2.3 Date of report: 28th March 2018

2.4 Name of Information Asset Owner (IAO) of relevant business unit: Roger Halliday, Chief Statistician and Chief Data Officer, Data, Statistics and Outcomes Division, The Scottish Government

2.5 Date for review of DPIA

Review date	Details of update	Completion date	Approval Date
May 2019	This PIA will be published and updated at critical milestones. It will be revisited as additional bodies or objectives are added to the powers under section 35 of the Digital Economy Act 2017 involving the approval of regulations by the Scottish Parliament.	May 2018	

3. Description of the project

3.1 Description of the work:

The aim of these Regulations is to enable Scottish public bodies, or persons providing services to Scottish public bodies to be able to disclose personal data under the new Public Service Delivery powers, set out in section 35 of the Digital Economy Act 2017 (the "Act"). The addition of Scottish public bodies into Schedule 4 of the Act will create a new legal gateway to enable the sharing of information to/from reserved bodies.

Only those public bodies or persons providing services to public bodies listed at Schedule 4 of the Act are able to make use of the Public Service Delivery power. The power is permissive, which means that persons who are potentially able to share information under it can choose whether or not to do so where that is permitted in particular under data protection legislation, but are not under a duty to do so. Schedule 4 of the Act does not yet list devolved Scottish bodies and it is for the Scottish Parliament to approve Regulations adding Scottish public authorities with only devolved functions or mixed devolved and reserved functions or those providing services to them. This is the purpose of the current regulations.

Section 35(1) provides that public bodies wishing to share personal data with each other for the purposes of Public Service Delivery may only do so for the purposes of an objective which is a specified objective in relation to each of those bodies. These objectives need to be specified in regulations.

Sections 35(9) – (12) of the Act identify three conditions which specified objectives must fulfil and which pertain to any information sharing under a specified objective;

The first condition is that the objective has as its purpose—
(a) the improvement or targeting of a public service provided to individuals or households, or
(b) the facilitation of the provision of a benefit (whether or not financial) to individuals or households.

The second condition is that the objective has as its purpose the improvement of the well-being of individuals or households. The reference in subsection to the well-being of individuals or households includes—
(a) their physical and mental health and emotional well-being,
(b) the contribution made by them to society, and
(c) their social and economic well-being.

The third condition is that the objective has as its purpose the supporting of—
(a) the delivery of a specified person's functions, or
(b) the administration, monitoring or enforcement of a specified person's functions.

These conditions mean that the power must demonstrate how it leads to the improvement in the delivery of a specific public service for individuals or households, or provision of a benefit to individuals or households – and that these are aimed at supporting the wellbeing of individuals or households. The third condition was added in response to feedback from parliament, suggesting that

Ministers should be required to specify closely delineated objectives which supported the delivery of a specified public authority's functions.

The planned Digital Government (Disclosure of Information) Regulations 2018 specify four objectives for which personal information can be disclosed to improve Public Service Delivery. These are;

i. Multiple Disadvantage
ii. Television Retuning
iii. Fuel Poverty
iv. Water Poverty (not relevant to Scotland)

Each of the bodies listed in the Digital Government (Scottish Bodies) Regulations 2018 will be identified with one or more of these objectives. The scope of any proposal to share personal data is limited to the specified objective identified with the specified body. Any further sharing would require further objectives to be specified by further affirmative Regulations.

The powers can only be used in well-defined policy delivery instances where improved information flow between bodies would allow for improved public service delivery to those people or households defined within the relevant objective and where there is not already a legal gateway for this to happen. This case will need to be fully set out up front and should make clear why the service cannot be delivered using other less sensitive or non-personal information.

The requirements of data protection, in particular the General Data Protection Regulation which comes into effect from 25th May 2018 will continue to apply to the use of the data and the new Data Protection Act 2018 will supersede the previous 1998 Act, once the new Act is commenced.

Third parties providing services to specified pubic bodies and sharing personal information using the public service delivery powers will need to be appropriately contracted, including through compliant data processing agreements, that specify the conditions for any processing and the obligations and instructions under which they are processing personal information and processes and reporting in the event of a breach.

3.2 Personal data to be processed.

Variable	Data Source
To be detailed in individual data sharing agreements and proposals to make use of the powers	Scottish Government
To be detailed in individual data sharing agreements and proposals to make use of the powers	A Scottish local authority – a council constituted under section 2 of the Local Government etc. (Scotland) Act 1994
Employment status of individual young person living in Scotland (aged 16-24 inclusive) to be checked by HMRC and sent back to Skills Development Scotland, along with individual's personal	Skills Development Scotland

identifying information in order that SDS can make contact, or remove from list of those eligible. • Employer Name • Employment Start Date • Employment End Date • Employment Pay Frequency • Hours Worked in Period • Taxable Pay in Period • Self-Assessment indicator (y/n) • Employer PAYE Reference	

3.3 Describe how this data will be processed:

PROCESSING

A number of safeguards are in place around the powers to ensure the processing of personal data preserves privacy, is done proportionately and securely, with due regard to legal and ethical frameworks.

Security

Each instance of processing will need to;

- demonstrate that appropriate operational and technological processes and procedures are in place to keep the Personal Data safe from unauthorised use or access, alteration, transmission, publication, loss, destruction, theft or disclosure.

- comply with the requirements of the UK HMG Security Policy Framework and UK HMG Information Security policies, guidelines and standards, including those produced by the UK Government's National Technical Authority for Information Assurance.

- implement appropriate technical and organisational measures in accordance with Article 32 of the General Data Protection Regulation to protect Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure - such measures being appropriate to the harm which might result from any unauthorised or unlawful processing accidental loss, destruction, or damage to the personal data and having regard to the nature of the personal data which is to be protected.

Section 35(6) of the Act provides that Scottish Ministers, in making regulations to add Scottish bodies to Schedule 4 must have regard to the systems and procedures for the secure handling of information by that body. This safeguard requires Ministers to scrutinise the security and procedural arrangements supporting the secure handling of data.

- adhere to the UK Government Information Sharing Code of Practice

Information sharing under these powers must adhere to the ICO data sharing code and other existing guidelines on data security, and the requirements of data protection legislation. Any complaints, objections or requests under the right of access to personal information must be addressed swiftly and effectively. Periodic checks will be conducted to ensure data security best practice is adhered to and publish details online of what checks are to be carried out and when. These are often spelt out in individual data sharing agreements. Anyone with concerns about a person's systems and procedures for handling data may raise those concerns with the responsible Minister.

Codes of Practice and Data Protection Legislation

A draft Information Sharing statutory Code of Practice covering Public Service Delivery will accompany the draft Regulations as these are laid in Westminster. The Code of Practice, which is subject to approval by the UK Parliament under the Act will set out the processes and safeguards to be adopted in sharing information using the Public Service Delivery powers. The purpose of the Code is to provide a set of principles and guidance for the use and disclosure of information under the powers. Section 43(3) of the Act provides that a person to whom the Code applies must have regard to the information Sharing Code of Practice – in disclosing information under any of sections 35 to 39, and in using information disclosed under any of those sections.

Scottish Ministers will expect public authorities and other participants in an information sharing arrangement to agree to adhere to the Code before any information is shared. Failure to have regard to the Code may result in public authorities losing the ability to disclose, receive and use information under the powers. In addition, there are criminal sanctions for disclosing personal information in ways that are not permitted by the Act (see sections 41 and 42 of the Act in particular).

The Code refers to other requirements when sharing personal data such as relevant data protection legislation and makes reference to the Information Commissioner's Privacy Impact Assessment Code of Practice and accompanying guidance. At the time a specified public body wishes to share data, it will need to conduct a Privacy Impact Assessment/Data Protection Impact Assessment and identify the legal bases for sharing personal data under relevant Articles 6 and 9 of the General Data Protection Regulation and list these as part of a data sharing agreement. Any personal data, or special category personal data processed using these powers must do so in line with relevant data protection legislation.

Section 43(2) provides that the Information Sharing Code of Practice must be consistent with the code of practice issued under section 52B of the Data Protection Act 1998, as altered or replaced from time to time.

Fairness and Transparency

Parties using the information sharing powers from section 35 will be required to ensure that practices are fair and transparent and only share information once satisfied of this. This is necessary in order to comply with lawfulness, fairness and transparency principle under data protection legislation. The Information Sharing Code of Practice sets out a number of specific obligations for reporting information sharing activities under the powers, building on and in addition to, requirements under data protection legislation.

Details of information sharing agreements concerning non-devolved bodies for disclosures under the PSD powers must be submitted to the Public Service Delivery Secretariat in the Department of

Digital, Culture, Media and Sport who will maintain a searchable electronic register available to the general public. Under data protection legislation, data controllers are required to keep records of their data processing activities.

Compliance with the Code

Any serious security breaches or serious breaches of the data protection legislation need to be reported immediately to the Public Service Delivery Review Board. This is set out in the Information Sharing Code of Practice. Any breaches should be reported in accordance with the requirements of the data protection legislation (including to the ICO if required). Any breaches of the Code or of the terms of a specific information sharing agreement should also be reported immediately to the Review Board.

Monitoring the use of the powers

The Review Board for UK-level and England-only information sharing will meet quarterly to review proposals for new objectives and will provide strategic oversight of the powers in Section 35. The Board will consist of senior officials from relevant information governance or social policy areas and will be attended by representatives from the ICO and invited members from appropriate public representative bodies.

3.4 Explain the legal basis for the sharing with internal or external partners:

The current Regulations will provide a legal gateway for sharing personal data under the Public Service Delivery power from Chapter 1 of Part 5 of the Digital Economy Act 2017 in certain circumstances where compatible with data protection legislation. Other specific legal gateways will be used instead where suitable, and the relevant legal bases will be identified separately for each proposed data share, as these are developed. Legal bases will refer to relevant data protection legislation.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish public	
The Skills Development Scotland Co Ltd	Wish to be added to Schedule 4 through the current set of Regulations so that they may make use of the powers to receive personal data from HMRC where appropriate to allow them to check the employment status of individual young persons and so re-engage at the point they fall out of work.
COSLA	Wish local authorities to be added to Schedule 4 through the current set of Regulations so that they may make use of the powers where appropriate.

	The power means that a person providing services to a Scottish local authority can share data with specified bodies listed on Schedule 4 – including to other persons providing services to a public authority where that public authority is listed on Schedule 4. Data processing agreements and other contractual documents will need to specify the terms of the processing and security, technology and safeguards around handling personal data.
Scottish Government (including executive agencies where legally the Scottish Ministers, Disclosure Scotland, Education Scotland, Transport Scotland, Scottish Public Pensions Agency, Scottish Prison Service, Student Awards Agency)	Wish to be added to Schedule 4 through the current set of Regulations so that they may make use of the powers.

4.2 Method used to consult with these groups when making the DPIA.

A public consultation was held from 12th December 2017 to 5th February 2018. The responses and Scottish Government response will be made available on the Scottish Government website at the time the Regulations are laid in Scottish Parliament.

The Scottish Government engaged with a broad reach of Scottish public bodies in relation to the objectives being laid in Regulations in Westminster, gauging interest in use of the powers for the purposes of public service delivery. Scottish Government officials worked with the Cabinet Office on the multiple disadvantage objective so that it would work within a Scottish public service delivery context.

Scottish Government officials have engaged with SDS officials to explore whether existing legal gateways could be used to obtain the required data from Her Majesty's Revenue and Customs. HMRC officials have also visited Scotland and met with SG and SDS officials to discuss options for data sharing. As part of these conversations, the technical security protocols of SDS have been scrutinised.

4.3 Method used to communicate the outcomes of the DPIA .

This DPIA will be be submitted with the Policy Note and other Impact Assessments as the Regulations are laid in the Scottish Parliament.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

The Scottish Regulations propose to add three Scottish bodies to Schedule 4 of the Act; Scottish Ministers; each of the Scottish local authorities, and Skills Development Scotland.

In addition the Regulations propose adding persons providing services in connection with a specified objective (within the meaning of section 35) to a specified person who—
(a) falls within this Part of this Schedule; and
(b) is a public authority.

Any third parties providing services to Scottish bodies specified in Schedule 4 will need to fulfil the same security and technical requirements.

This approach is proportionate and enables only these specified bodies to use the powers in the Act and only for sharing for the objective/s to which they are paired in the Regulations under section 35(7). Any requirement to use the Public Service Delivery powers in the Act by other Scottish bodies will require separate Regulations that list those bodies at Schedule 4 and will require separate objectives to be specified (in connection with these specified bodies) and also laid in Regulations. The approach has not been to add the wider class of Scottish Public authorities without regard for uses of the data.

5.2 Anonymity and pseudonymity

To preserve individuals' privacy, personal data will only be processed and shared where required to deliver the services focused on the specified objectives set down in the UK Regulations.

Appropriate techniques will be used to pseudonymise and de-identify personal data and access to personal data will be restricted to core individuals involved in processing. This will need to be fully explained as part of any information sharing agreement, setting out how personal data will be stored securely and access to it restricted to a named list of appropriately qualified personnel.

All data flows will need to be documented in information sharing agreements that make clear where and why identifiable data is required and the safeguards in place around this.

Public authorities making their data available must make sure that they share the minimum amount of personal information required to properly fulfil the purpose for which it is being processed. This "data minimisation" principle should guide the way organisations design and structure their information sharing processes. The Information Sharing Code of Practice sets out a series of Principles to be followed, in addition to data protection principles set out in legislation.

5.3 Technology

Data format and sharing protocol follow relevant standards set out in the Open standards for government data[1] and technology and the API standards[2].

[1] https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology

Organisations involved in an information sharing arrangement should also agree procedures and processes for correcting inaccurate data, deleting data where there is a right to erasure, contacting the data subject were appropriate, how to treat subject access requests, how data subjects can exercise their rights to restrict and object to processing.

The Information Sharing Code of Practice sets out three specific requirements for Security;

1. Public authorities and receiving parties should consider the standards and protocols that apply to their organisation when providing or receiving information before agreeing appropriate standards and protocols; all parties should be satisfied that they provide a level of security that is both appropriate and meets or exceeds their own standards and protocols.

2. Each party involved in the data share must make sure effective measures are in place to manage potential or actual incidents relating to the potential loss of information; and

3. public authorities and data processors, together with any third parties must be fully engaged in the resolution of a potential or actual data incident.

As part of any formal data sharing agreement, security plans will need to be evidenced and documented to include; secure storage arrangements, protective marking; assurance around process for restricted access by individuals; notification protocol in the event of a breach; procedures to investigate cause of any breach.

5.4 Identification methods

Specific to individual data shares

5.5 Sensitive/Special Category personal data

Specific to individual data shares

5.6 Changes to data handling procedures

The specified bodies listed at Schedule 4 will need to fully specify data handling procedures and methods for transferring data where this has not occurred previously. These decisions will need to take account of the nature and content of any data being shared.

5.7 Statutory exemptions/protection

[2] https://www.gov.uk/service-manual/technology/application-programming-interfaces-apis

Requirement to comply with other legislation;

- Data protection legislation in particular the General Data Protection Regulation and related legislation, with references to be updated by amendment under the Data Protection Bill in due course
- Parts 1-7 or Ch 1 of Part 9 of the Investigatory Powers Act 2016
- obligations in European law which are binding in UK law
- and the Human Rights Act 1998

Data sharing powers are not in general suitable for the sharing of information which is sensitive on national security grounds and subject to express restriction or disclosure. Any data share must adhere to the Security Policy Framework and observe handling controls in relation to protective markings.

5.8 Justification

Section 35 of the Act is intended to remedy the lack of clear legal gateways for sharing information across public services, and in particular disclosures from reserved departments. To help ensure that any sharing under these powers is justified and proportionate the powers are constructed to only allow public authorities to disclose information for purposes consistent with tightly constrained objectives.

Scottish bodies wishing to disclose or receive personal data using these powers will need to register details of the Information Sharing Agreement with the Department for Digital, Culture, Media and Sport for inclusion on a public register. The register will allow government, the Information Commissioner and the public to understand what information sharing is taking place under the provisions to assess their effectiveness and value. Where an organisation providing services to a public body uses the powers in this Act to share data, their role will need to be appropriately documented in the Register and for publication.

5.9 Other risks
5.10

Bodies that are defined as public authorities do not always directly deliver public services; the ability to use external partners and sub-contractors is essential to improving the effectiveness and efficiency of those services. In these situations, public authorities are likely to need to access data from external delivery partners and sub-contractors or to provide them with information so that they can fulfil their duties. These organisations will be required to handle information to the same standards as public authorities, including compliance with the Code of Practice and relevant data protection law and contractual agreements where necessary.

6. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Risks to individuals of disclosure of personal identifying information		Examine proposals of specific data share and document through data sharing agreements, Data Protection Impact Assessments, Data Processing Agreements that detail security and protocol to promote secure handling of data. Following the Information Sharing Code of Practice and ICO data sharing Code of Practice. Only the minimum necessary personal information consistent with the purpose of the data share should be processed, ensure access to personal data is restricted to named individuals with appropriate training in safe handling of personal data. Clarify why data cannot be pseudonymised to minimise sharing of personal identifiers where not required, following data minimisation principles	Reduce and manage
Corporate Risks		Reputational risk in the event of a breach. Ensure appropriate IG protocols in place to report breach in line with data protection legislation – that these protocols are understood throughout the relevant organisation using the power to share personal information. Ensure processes in place to regularly review Information Assets, keeping these accurate and updated – to avoid duplication of data or incorrect/out of date personal information being processed. Request that retention and archive periods are identified in data sharing agreements and justified.	Reduce and manage

		Training staff in identifying and responding to Subject Access Requests and other requests from data subjects. Ensure robust breach detection and investigation and internal reporting procedures – and that these are understood by staff. Maintain records of any data breaches.	
Compliance Risks associated with breach of Data Protection law and other legal codes.		Risks associated with non-compliance will be managed through publication of the Code of Practice. A review board will be established for all non-devolved and England-only data sharing to ensure a consistent approach to sharing using the powers. The review board will also be responsible for strategic oversight of the public service delivery power including the searchable electronic register of data sharing. The board will advise Ministers on information sharing under the power, consider complaints and act as a point of contact with the ICO. The board will also consider and coordinate any revisions to the code of practice as necessary. A draft Code of Practice for Public Service Delivery will accompany the draft Regulations as these are laid in Westminster. The Code of Practice will set out the processes and safeguards to be adopted in sharing data using the Public Service Delivery powers. Data sharing agreement requires sign off before start of project/any data being transferred. All parties aware of roles and	Reduce and manage

		responsibilities for ensuring compliance with DPA and SG standards.	

7. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of the proposed Digital Government (Scottish Bodies) Regulations 2018 has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	**Date each version authorised**
Roger Halliday, Chief Statistician and Data Officer, Scottish Government	May 2018