Data Protection Impact Assessment for Legislation

This template is for policy teams developing a legislative proposal (that is, in primary or secondary legislation) or statutory guidance, where that proposal may have an impact on the protection of personal data within the meaning of the General Data Protection Regulation (GDPR).

The very first question you should answer is **does the proposal involve processing of personal data in some way?**

For the purposes of the GDPR, the key term is "**processing"**, which is very broad in scope and includes (but is not limited) to collecting, storing, recording, altering, using, consulting, transmitting or erasing data- in short, just about any possible use. "**Personal**" is also very broad in scope and means any information relating to a living person, where that person can be directly or indirectly identified.

For example if the proposal is to establish a new public body, there may be new data sharing provisions needed to ensure that body can carry out certain functions or to deliver certain services. The proposal may involve new technologies for the collection or storage of data or a change in how existing processes operate with respect to processing of data. Some provisions will involve similar sorts of processing as currently take place but there may be a significant change to the context or purpose.

Where a potential impact is identified, a full assessment of the proposed provisions and the impact on data subjects must be undertaken.

You may find in working through the preliminary questions in this template that a full DPIA is not necessary under the GDPR; however if so, it is recommended that you document your reasoning as why that is the case and to that end it may still be helpful to work through the form.

The template operates works in conjunction with the Article 36(4) ICO consultation form, in the event the draft legislation requires consultation with the Information Commissioner's Office (ICO).

Separately, the proposal may also have implications which will need to be considered in respect of ECHR, in particular Article 8 rights to privacy.
Please note that questions below seek to articulate how the proposals will meet the requirements of Article 32 of GDPR, Article 35 GDPR and other relevant elements of both GDPR and Data Protection Act 2018, as well as providing an appropriate assessment of the impact on individuals.

Article 35(1)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out and assessment of the impact of the

envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

Article 35(7)

The assessment shall contain at least:

a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation [GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned.

Article 32 (Security of processing)

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Introductory information

Summary of proposal:	Review of Island Communities Impact Assessments Decisions (Scotland) Regulations under Section 9 of the Islands (Scotland) Act 2018
Your department:	Directorate for Agriculture and Rural Economy (D:ARE) | Rural Economy and Communities Division
Contact email:	Paul.Maxton@gov.scot
Data protection support email Data protection officer	dpa@gov.scot dataprotectionofficer@gov.scot **Stuart Gardner, Data Protection Officer| iTECS | Scottish Government** Stuart.Gardner@gov.scot
Is your proposal primary legislation, secondary legislation or other form of statutory measure?	Secondary legislation
What stage is the legislative process at? Please indicate any relevant timescales and deadlines.	The draft Regulations are in the final stages of the internal checking process. The laying date was 29 October 2020, but with Ministerial approval is now 3 November 2020.
Have you consulted with the ICO using the Article 36(4) form (please provide a link to it)?	**Yes** https://erdm.scotland.gov.uk:8443/documents/A30000314/details
If the ICO has provided feedback, please include this.	**Yes** https://erdm.scotland.gov.uk:8443/documents/A30000552/details
Do you need to hold a public consultation and if so has this taken place	We issued a paper on 26 June 2020, seeking views on a proposed overview of the review scheme under Section 9 of the Act to allow consultation with relevant authorities listed in the Islands (Scotland) Act 2018.

	We also consulted island communities on Island Community Impact Assessments as part of our consultation to develop the National Islands Plan.
Were there any comments/feedback from the public consultation about privacy, information or data protection?	There was minimal feedback around privacy or data protection. One respondent considered, in regard to third party representations, that the authority would be handling information from parties other than the applicant and suggested that there may be potential for data protection implications arising.

Version	Details of update	Version complete by	Completion Date
1	1st draft	Paul Maxton	14 /9/2020
1.1	Comments from DPIA Team	Heather Maclean	18/09/2020
1.2	Comments from Unit Head	Erica Clarkson	22/09/2020
1.3	Updated following comments from Heather Maclean and Erica Clarkson	Paul Maxton	28/9/2020
1.4	Updated following comments from Heather Maclean and Erica Clarkson regarding including narrative re process in risk section	Paul Maxton	1/10/2020
1.5	Approved DPO	Stuart Gardner	2/10/2020

	Question	Comments
Article 35(7)(a) – "purposes of the processing, including, where applicable, the legitimate interest pursued by the controller"		
1	What issue/public need is the proposal seeking to address? What policy objective is the legislation trying to meet?	The proposal provides a mechanism for the review of decisions by public authorities related to island communities impact assessments. The policy objective is the empowerment of island communities.
Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects" and Article 35(7)(b) "…necessity and proportionality of the processing operations"		
2	Does your proposal relate to the processing of personal data? If so, please provide a brief explanation of the intended processing and what kind of personal data it might involve. Who might be affected by the proposed processing? Is the processing considered necessary to meet a policy aim? Is there a less invasive way to meet the objective (for example, anonymising data, processing less data).	Yes. The applicant would require to state their name and contact details in an application form. A copy of the readcted application would be published on the public authority's website asking if interested parties wish to make representations. Interested parties who wish to make written representations will also require to provide their name & contact details and this personal data (along with the representations) will be shared with the applicant (Regulation 8). The lawful basis, the purpose for processing and the and reason for sharing names etc will be highlighted in a relevant Privacy Notice (PN) on the Scottish Government (SG) website along with the application and the representation form. It would be envisioned however that each Public Authority would be responsible for publishing their own PN as SG with have no sight of the data submitted to them. (ii) if the relevant authority serves notice requiring additional information from any party, the name and contact details of those parties will be disclosed to all other parties on whom notice is served in order that the additional information can be sent directly to them. Comments and representations of third parties will also be

		published on the website of the relevant authority (Regulation 13). The personal data involved would be the name and contact details of the applicant, third parties who make representations and third parties who are served notice requesting additional information from the public authority. The data would be published on the relevant authority's website in the interests of transparency. The personal details/name and address would be anonymised throughout the process. The personal data would not be sensitive or special category data or relate to criminal convictions or offences.
	Please also specify if this personal data will be sensitive or special category data or relate to criminal convictions or offences (Note: 'special categories' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data about a person's sex life or sexual orientation and sensitive personal data means criminal information or history)	The processing of the personal data is considered necessary to assist the policy aim of inclusiveness and empowerment of island communities.
Part of your consideration in relation to Article 35(7)(a) and (b) should be in respect of ECHR. "		
3	Will your proposal engage any rights under ECHR, in particular Article 8 ECHR? How will the proposal ensure a balance with Article 8 rights? If the proposal interferes with Article 8 rights, what is your justification for doing so – why is it necessary? **Article 8 ECHR:** **Right to respect for private and family life**	The proposal will engage with ECHR Article 8. However, the anonymizing of the name and contact details of parties would ensure a non-invasive approach without compromising Article 8.

	1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. You may also wish to consider Article 6 right to a fair trial (and rights of the accused) Article 10 right to freedom of expression Article 14 rights prohibiting discrimination Or any other convention or treaty rights?	It is considered that the process will be fair and transparent by allowing an applicant to respond to any third party representations. It is considered that the review process contributes to freedom of expression by allowing island communities to challenge public authority decisions. No

Article 35(7)(b) "…necessity and proportionality of the processing operations" *Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"* *Article 35(7)(d) "measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned"* *Note Article 32 GDPR for s.4 also*		
4	Will the proposal require regulation of : □ technology relating to processing □ behaviour of individuals using technology □ technology suppliers □ technology infrastructure □ information security (Non-exhaustive examples might include whether your proposal requires online surveillance, regulation of online behaviour, the creation of centralised databases accessible by multiple organisations, the supply or creation of particular technology solutions or platforms, or any of the areas covered in questions 4a or 4b.)	*Please provide details* No
4a	Please explain if the proposal will have an impact on the use of technology and what that impact will be. Please consider/address any issues involving: ○ Identification of individuals online (directly or indirectly, including the combining of information that allows for identification of individuals, such as email addresses or postcodes); ○ Surveillance (necessary or unintended); ○ Tracking of individuals online, including tracking behaviour online; ○ Profiling; ○ Collection of 'online' or	The proposal will have a minimum impact on technology. Essentially, relevant authorities will be required to publish ICIAs on their websites. The process will also require relevant authorities to publish applications and representations from third parties on their websites. Since the personal details of the applicant etc will be anonymised, there is a low risk of individuals being identified.

	other technology-based evidence ○ Artificial intelligence (AI); ○ Democratic impacts e.g. public services that can only be accessed online, voting, digital services that might exclude individuals or groups of individuals (Non-exhaustive examples might include online hate speech, use of systems, platforms for delivering public services, stalking or other regulated behaviour that might engage collection of evidence from online use, registers of people's information, or other technology proposals that impact on online safety, online behaviour, or engagement with public services or democratic processes.)	
4b	Will the proposal require establishing or change to operation of an established public register (e.g. Accountancy in Bankruptcy, Land Register etc.) or other online service/s?	No.
Article 35(7)(b) "…necessity and proportionality of the processing operations" *Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"* **Note exemptions from GDPR principles where applicable*		
5	Please provide details of whether the proposal will involve the collection or storage of data to be used as evidence or use of investigatory powers (e.g.in relation to fraud, identify theft, misuse of public funds, any possible criminal activity, witness information, , victim information or other monitoring of online behaviour)	Not applicable.
Article 35(7)(b) "…necessity and proportionality of the processing operations" *Article 35(7)(c) "assessment of the risks to the rights and freedoms of data subjects"* *Article 35(7)(d) "measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with [GDPR] taking into account the rights and legitimate interests of data subjects and other persons concerned"*		

6	Would the proposal have an impact on a specific group of persons e.g. children, vulnerable individuals, disabled persons, persons with health issues, persons with financial difficulties, elderly people? (Please specify) In what way?	No.
7	Will the Bill necessitate the sharing of personal data to meet the policy objectives? For example ○ From one public sector organisation to another public sector organisation; ○ From a public sector organisation to a private sector organisation, charity, etc.; ○ Between public sector organisations; ○ Between individuals (e.g. practitioners/ service users/sole traders etc.); ○ Upon request from a nominated (or specified) organisation?	Paragraph 4 narrates the processes where personal data will require to be anonymised. As such, there will be no sharing of person data. It is envisaged that one public sector body could be an applicant (eg. a local authority that requests a review from another public body (eg. Skills Development Scotland or the Scottish Ministers).
	If so, does the Bill make appropriate provision to establish a legal gateway to allow for sharing personal data Please briefly explain what the gateway will be and how this then helps meet one of the legal basis under Article 6 of the GDPR. (Please provide details of data sharing, e.g. if there is a newly established organisation, if it is new sharing with an already established third party organisation, if it is with a specified individual or class of individuals, or any other information about the sharing provision/s. State what is the purpose of the sharing and why it is considered to be necessary to achieve the policy aims.)	Not applicable.

8	Is there anything potentially controversial or of significant public interest in the policy proposal as it relates to processing of data? For example, is the public likely to views the measures as intrusive or onerous?	No.
	Are there any potential unintended consequences with regards to the provisions e.g. would the provisions result in unintended surveillance or profiling.	No.
	Have you considered whether the intended processing will have appropriate safeguards in place? If so briefly explain the nature of those safeguards and how any safeguards ensure the balance of any competing interests in relation to the processing.	The process will involve a relevant authority receiving information containing person data directly from the applicant or respondent. This will be received electronically or be comprised entirely of, hard copy documents. • Data will be stored securely either electronically or as hard copy documents. All published ICIAs will be stored on existing secure Scottish government website under Island Communities Impact Assessment. All applications and representations from third parties will also be stored on existing Scottish government website. Any hard copies of applications and representations from third parties will be Kept in secure offices by staff handling such applications. All staff must attend information handling Training regularly.
		• A privacy notice will be attached to the application form and will form part of the guidance for applying which will give details about the subject's rights, what will happen to their personal

		data, why the relevant authority are able to process their personal data, and for what purpose it is being processed. • Before sharing any application, the relevant authority will require to satisfy itself that there is a lawful basis for sharing the information and ensure that a third party agrees to handle the data in conformity with the applicant's rights.
9	Are there consequential changes to in other legislation that need to be considered as a result of the t proposal or the need to make further subordinate legislation to achieve the aim? (This might include, for example, regulation or order making powers; or provisions repealing older legislation; or reference to existing powers (e.g. police or court powers etc.).	No.
10	Will this proposal necessitate an associated code of conduct? If so, what will be the status of the code of conduct (statutory, voluntary etc.)?	No.

Summary – Data Protection Impact Assessment

11	Do you need to specify a Data Controller/s?	**No.**
12	Have you considered whether the intended processing will have appropriate safeguards in place, for example in relation to data security, limitation of storage time, anonymisation? If so briefly explain the nature of those safeguards Please indicate how any safeguards ensure the balance of any competing interests in relation to the processing.	• The Privacy Notice associated with the application process will provide more details on the retention of data. • The Privacy notice will also give details of anonymising personal information when publishing the application and the sharing of information with third parties and the public.
13	Will the processing n of personal data as a result of the proposal have an impact on decisions made about individuals, groups or categories of persons? If so, please explain the potential or actual impact. This may include, for example, a denial of an individual's rights or use of social profiling to inform policy making.	No.
14	If the proposal involves processing, do you or stakeholders have any relevant comments about mitigating any risks identified in the DPIA including any costs or options, such as alternative measures.	There were no comments regarding risk made in the consultation. Any risks identified have been reduced to a low level by ensuring appropriate mitigation is put in place.

Risk	Solution or mitigation	Result
1. Personal data is mistakenly shared with other organisations/members of the public.	Ensure all staff are given regular data protection training, understand the contents of data sharing agreements and the lawful basis for sharing information.	Reduce risk
2. Non redaction of applications	Ensure all staff understand the importance of redacting an application through regular data protection training.	Reduce risk
3. Insufficient redaction of applications where applicant comes from a small island community	Ensure all staff understand that where an applicant comes from a small island community, the redaction of personal details may not be sufficient in itself and that further redaction of the content of the application may be necessary so as not to disclose the identity of an applicant. This would be covered by regular data protection training.	Reduce Risk
4. Process – inconsistencies in the handling of data	Guidelines on process handling will be made available to all staff on the ICIA Scottish government webpage to ensure that there is a consistent approach to the process. The guidelines will be regularly reviewed and monitored and will be incorporated within staff training and be augmented by awareness raising.	Reduce Risk

Authorisation

I confirm that the impact of Review of Island Communities Impact Assessments Decisions (Scotland) Regulations under Section 9 of the Islands (Scotland) Act 2018 **has been sufficiently assessed in compliance with the requirements of the GDPR**

Name and job title of a IAO or equivalent	**Date each version authorised**
Approved by Catriona MacLean Deputy Director Rural Economy and Communities Division 2 October 2020	**Final version approved on** **2 October 2020**

Explanatory note re risks

The data protection impact assessment for legislation is an iterative process. There are many ways that risks to privacy and/or data protection can arise in legislative proposals and also many options for addressing those risks through legislation. As with most responses to risks, these will vary in their implications and potential impacts (e.g. cost implications, creation of other risks, consequence scanning etc.).

Some of the risks you will need to consider as work develops on Bill proposals, ancillary documents, analysis of consultations, ICO feedback and other Bill development may include (but will not be limited to):

- There is insufficient justification for interference with Article 8 ECHR rights;
- Appropriate safeguards have not been included/incorporated into provisions;
- Appropriate safeguards have not been included/incorporated into provisions regarding impact to/on children;
- The legal basis for processing is not specified or not specific enough;
- The legal basis for processing is insufficiently expressed for the purposes of Article 9 GDPR or Schedule 1 Data Protection Act 2018 (processing of special category personal data);
- Data controllers are not specified (they are not required to be but, where appropriate, they should be specified);
- Legal gateways for data sharing are not included;
- Legal gateways for data sharing are not specific enough or are too specific (for example, a named organisation is specified which consequently changes it name/structure and there is no generalised provision to allow for continued data sharing, or the provisions are drawn so specifically that an area of data sharing is excluded even though, once implemented, that information is needed etc.);
- Provisions interfere with other ECHR rights (there will be an overlap between data protection (Article 8) and some of the other ECHR rights);
- Unintended consequences of the proposals lead to undesirable outcomes (including non-compliance) e.g. surveillance, impinging other rights, collection of more personal data than originally intended, invasive monitoring of citizens without appropriate safeguards, creation of ‘big data’ sets that allow for identification of individuals and discovery of unintended personal data;
- Data protection principles aren’t incorporated into the legislation itself and/or
- The implementation of the legislation (i.e once the Bill is enacted) is problematic because insufficient provision was included in the legislation (e.g. through express or implied powers, legal gateways, flexibility with regards to manner of implementation/powers to implement etc.);
- Controversial measures;
- Other legislation is not repealed or amended which contains provisions that make new proposed provisions unclear or uncertain;
- Statistics or other exemptions aren’t incorporated/become unclear through the new legislation;
- Failing to identify all of the personal data that will be created, that will need to be shared, the organisations it will need to be shared with, or failing to include

sufficiently wide provisions to allow for necessary use, sharing or access to the personal data (or other future proofing issues).