National Records of Scotland

Data Protection Impact Assessment (DPIA): Providing access to the 2011 Census secure microdata files at the eDRIS National Safe Haven at the Bioquarter in Edinburgh and Regional Safe Settings operated by the Administrative Data Research Centre (Scotland)

Please use this document in conjunction with the Data Protection Impact Assessment (DPIA) Policy and Guidance (Objective ID: A16760358)

Document Control

Title	**Data Protection Impact Assessment (DPIA): Providing access to the 2011 Census secure microdata files at the eDRIS National Safe Haven at the Bioquarter in Edinburgh and Regional Safe Settings operated by the Administrative Data Research Centre (Scotland)**
Prepared by	**Nancy Burns**
Approved by	NRS Privacy Group
Date of approval	06/02/2018
Review frequency	
Next review date	

Status Control

Version	Date	Status	Prepared by	Reason for Amendment
2.0	14/12/2017		Nancy Burns	Edited original DPIA for transfer of data to National Safe Havens, to cover access at the Regional Safe Settings. Amended to clarify information flows, and added information flows diagram.
2.1	06/02/2018		Nancy Burns	Edited to include additional IT security details provided by NSS and amendments from NRS privacy group.

Part 1: Data protection impact assessment screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions to align more closely to project you are assessing.

1. Will the project involve the collection of new information about individuals?

No.

2. Will the project compel individuals to provide information about themselves?

No.

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

No. This information is already available to researchers, but this proposal will provide more convenient access for researchers based in Scotland.

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

No.

5. Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

No.

6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

No.

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Yes, census data includes sensitive personal information. The census microdata has been de-identified.

8. Will the project require you to contact individuals in ways that they may find intrusive?

No.

NRS maintains a record of answers to the screening questions in order to document that the decision on whether to carry out a DPIA was properly considered. If after completing the screening questions you decided a DPIA is not necessary you must send a record your answers to the NRS Data Protection mailbox. The NRS Data Protection Officer will review answers, and where appropriate ask the NRS Privacy Group for their opinion.

Part 2: Data protection impact assessment report

Use this report template to record the DPIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a DPIA. The template follows the process that is used in the ICO code of practice. You can adapt the template to allow you to record additional information relevant to the DPIA you are conducting.

For further guidance please refer to the NRS DPIA Policy and Guidance (Objective ID: A16760358).

Step one: Describe the project and identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to NRS, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal or business case.

It is important to include information about the benefits to be gained from the project in order to help balance any risk identified in the DPIA. This can help inform decisions on the level of risk to privacy that is acceptable, when balanced against the benefits or other justification for the project. Is there a benefit to the public? If a statutory duty exists provide details of this. Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions) and identify the legal basis for processing.

This proposal aims to provide more convenient access arrangements for Scottish-based researchers seeking to analyse the secure microdata files from Scotland's Census 2011. Currently these data sets – 10% samples of de-identified person and household records from the 2011 Census - are only available to approved researchers who apply to the Virtual Microdata Laboratory (VML) at one of the sites managed by the Office for National Statistics. For Scottish-based researchers this can mean incurring travel and other expenses as well as being time-consuming. Providing a more convenient access path to Scottish-based researchers should reduce these cost and time burdens. It will also be conducive to more analysis of these data sets, resulting in improvements to the evidence base for policy and research interests.

This proposal is to store a copy of the 2011 Census secure microdata files for Scotland with the electronic Data Research and Innovation Service (eDRIS), to be stored on eDRIS servers at the Edinburgh Parallel Computing Centre (EPCC), for access by researchers at the eDRIS National Safe Haven at the Bioquarter in Edinburgh, or at one of the Regional Safe Settings operated by the Administrative Data Research

Centre Scotland (ADRC-S). Both the National Safe Haven at the Farr Institute and the Regional Safe Settings (currently in St Andrews, Aberdeen, Dundee and Glasgow) are operated by ADRC-S, supported by eDRIS, and subject to the same security protocols.

This DPIA covers the data protection risk implications of:

1) Transferring census data to eDRIS servers

Security implications of the one-off transfer of data from NRS to the eDRIS secure environment at EPCC

2) Storing census data on eDRIS servers

Security implications of the ongoing storage of census data in the eDRIS secure environment at EPCC

3) Providing access to census data to researchers via the ADRC-S safe haven and safe settings

Access to the Safe Haven and the Regional Safe Settings is controlled by trained local staff with appropriate security clearance. Additionally, use of the Safe Haven and the Regional Safe Settings is monitored remotely using CCTV viewed by ADRC-S staff at the National Safe Haven. The security arrangements for both the National Safe Haven and the Regional Safe Settings have been assessed by an independent IT security consultant.

The privacy impacts of CCTV monitoring users of the regional safe settings are covered under ADRC-S's Privacy Impact Assessment.

4) Risk specifically associated with the SARS census microdata sample.

While the data in the secure census microdata (10%) samples of person and household records are deidentified (and the samples were drawn in such a way as to exclude 'population uniques'), they include the highest level of detail and the largest sample size of all the census microdata products. Potentially sensitive variables such as ethnic group, religion and health are also included in the person data file. They are therefore afforded the highest level of access limitation. As this proposal represents providing access in alternative settings to the very secure environment of the VML managed by ONS, it is necessary to assess it in terms of privacy impact.

Further background information on the current access arrangements is available on the Scotland's Census website.

Step two: Describe the information flows

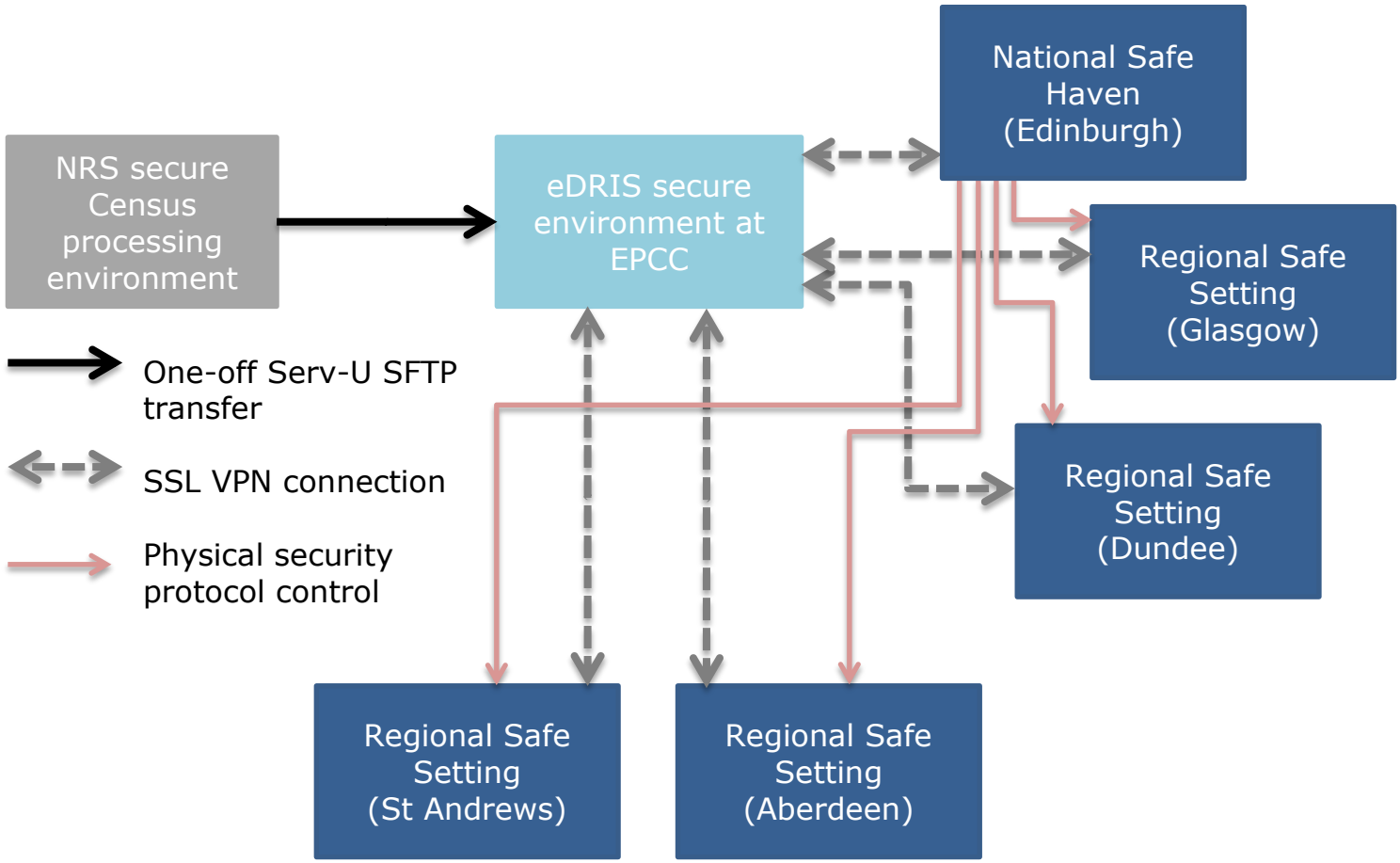
You should describe the collection, use and deletion of personal data here. You should also say how many individuals are likely to be affected by the project. Describe how the personal data will be processed. Provide information about the design and method. It is often helpful to include a diagram or flowchart that explains the information flows.

The data will be encrypted at source and transferred to the eDRIS secure environment at the EPCC using Serv-U SFTP. All members of staff involved in the data transfer and processing are appropriately trained and have signed confidentiality statements and the Census Confidentiality Undertaking. The technical infrastructure used to transfer and store the data was assessed by cybersecurity consultancy Evolve in February 2016.

There is no set time limit on how long the data can be stored in the eDRIS secure environment at the EPCC, but the associated Data Sharing Agreement (which includes a provision for NRS to require deletion of the data) will be reviewed annually. The EPCC secure environment is accredited by cyber security consultancy Evolve to hold official sensitive data.

Once stored on the eDRIS server, the data can be accessed from the National Safe Haven and from the ADRC-S Regional Safe Settings via a VPN with SSL encryption and two-factor authentication. The terminals in the National Safe Haven and Regional Safe Settings provide a thin client connection to the eDRIS server, which means the terminals cannot store local copies of data. All members of staff involved in securing access to the remote safe settings will be appropriately trained and have signed the Census Confidentiality Undertaking. Researchers accessing the data will also be appropriately trained and have signed both the Census Confidentiality Undertaking and the eDRIS User Agreement.

The secure census microdata files comprise de-identified record level data on around 524,000 individuals and 247,000 households. Further background information on the content of the secure microdata files is available on the Scotland's Census website.


National Safe Haven (Edinburgh)
NRS secure Census processing environment
eDRIS secure environment at EPCC
Regional Safe Setting (Glasgow)
One-off Serv-U SFTP transfer
SSL VPN connection
Physical security protocol control
Regional Safe Setting (Dundee)
Regional Safe Setting (St Andrews)
Regional Safe Setting (Aberdeen)

Step three: Consultation requirements

Describe the groups you will be consulting with and their interest in the project. Who should be consulted internally and externally? Explain the method you will use for consultation with any stakeholder groups and how you will communicate the outcomes of the PIA back to them. How will you carry out the consultation? Explain what you learned from the consultation process and how they shaped your approach to the management of privacy risks. Explain what practical steps you will take to ensure that you identify and address privacy risks. You should link this to the relevant stages of your project management process. You can use consultation at any stage of the DPIA process.

The appropriate legal gateway for NRS sharing census data is provided by section 5 of the Census Act 1920. Relevant conditions under the Data Protection Act 1998 and the General Data Protection Regulation for processing personal data and sensitive personal data fairly and lawfully for research purposes have been identified and met (see Step Five). The data will be used for purposes which are wholly compatible with the purposes for which the data was originally collected.

The NRS Privacy Group has approved an earlier iteration of this proposal. NRS technical security have been consulted on the updated proposal extending access to regional safe settings.

The Administrative Data Research Centre (ADRC) is not a data provider but requires submission of a formal application to their approvals panel before any project seeking access to census microdata can commence. This includes scrutiny of privacy risks as part of an assessment of research project proposals by an ADRC approvals panel.

Step four: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on a more formal risk register.

The questions under Part 3 can be used to help you identify the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) related compliance risks.

	Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation/ corporate risk**
1	Individuals are identified either deliberately or accidentally during analysis	Potential disclosure of sensitive personal data.	Breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. The researcher and/or institution may face sanctions as a result of a breach of eDRIS user agreement. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.
2	Data breach during transfer from NRS to EPCC.	Potential disclosure of	Breach of DPA/GDPR;	Reputational, operational and financial risk – trust in NRS and

		sensitive personal data.	breach of Census legislation; breach of compliance with government security policies; possible sanctions.	research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010.
3	Intruder access to safe haven or safe settings	Potential disclosure of sensitive personal data.	Breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.

				Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010.
4	Intruder access to EPCC server room (physical access)	Potential disclosure of sensitive personal data.	Breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010.
5	Intruder access to eDRIS server	Potential disclosure of sensitive personal data.	Breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies;	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's

			possible sanctions.	Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010.
6	Data breach during transfer and repair, if the disks storing the data develop a mechanical fault and have to be returned to the supplier	Potential disclosure of sensitive personal data.	Breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010.
7	Too much data is shared with researchers.	Increases the impact of any loss of data.	Excessive data sharing or use of irrelevant data is	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by

			against DPA/GDPR principles.	association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions – suspension for a fixed period or permanently from ADRC services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions from ADRC services and sanctions from listed funders.
8	No legal basis for sharing census data is established.	Processing must be legal under DPA/GDPR. Would be a breach of trust, but providing other privacy controls are in place not likely to create any	Would be a breach of DPA/GDPR or Census legislation and a breach of government security policies and professional standards.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO).

		detriment to individuals.		Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010. Researchers could face Safe Haven sanctions.
9	The conditions for lawful processing of personal data are not met.	Processing must be legal under DPA/GDPR. Would be a breach of trust, but providing other privacy controls are in place not likely to create any detriment to individuals.	Would be a breach of DPA/GDPR or Census legislation and a breach of government security policies and professional standards.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO).
10	Researchers are not adequately trained in handling personal information.	Increases the risk of a disclosure of personal data.	Increases the risk of a breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act

				1920 carries potential of fine and/or prison sentence.
11	Data is shared with organisations who will not act in a secure, ethical or professional manner	Increases the risk of a disclosure of personal data – possibly for financial gain	Increases the risk of a breach of DPA/GDPR; breach of Census legislation; breach of compliance with government security policies; possible sanctions.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions – suspension for a fixed period or permanently from ADRC services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions from ADRC services and sanctions from listed funders. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010

12	There is not enough public benefit associated with the project	Unlikely that this could be viewed to be fair processing if the public benefit doesn't justify the privacy risks	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/GDPR principles.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Researchers could face Safe Haven sanctions.
13	The project is not able to achieve its aims	Unlikely that this could be viewed to be fair processing if the public benefit doesn't justify the privacy risks	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/GDPR principles.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Researchers could face Safe Haven sanctions.
14	Data is shared with commercial organisations	Increases the risk of a disclosure of personal data – possibly for	Increases the risk of a breach of DPA/GDPR; breach of Census	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and

		financial gain	legislation; breach of compliance with government security policies; possible sanctions.	use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010 Researchers could face Safe Haven sanctions – suspension for a fixed period or permanently from ADRC services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions from ADRC services and sanctions from listed funders.
15	The security measures around the project are inadequate	Increases the risk of a disclosure of personal data	Increases the risk of a breach of DPA/GDPR; breach of Census legislation; breach of compliance with	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk

			government security policies; possible sanctions.	of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.
16	The data is used to contact individuals	Could cause distress or detriment to individuals. This would be beyond the purpose of this project and so would not be fair or ethical	This would be a breach of personal data and would breach DPA/GDPR and census privacy undertakings.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions – suspension for a fixed period or permanently from ADRC services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions from ADRC services and sanctions from listed funders.

17	The use of the data is incompatible with the original purpose it was collected	This couldn't be viewed to be fair processing if the purpose was incompatible	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/GDPR principles.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Researchers could face Safe Haven sanctions.
18	Individuals involved are not made aware of this use of their data	If individuals felt the processing was unfair or unwarranted it could cause them distress	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/GDPR principles.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO).
19	The project uses sensitive data or data referring to vulnerable groups	Data of this kind amplifies the privacy impacts of any breach or unfair processing	If the use of data of this kind is judged to be excessive this would be a breach of	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future.

			DPA/GDPR and other legislation. If the data required is sensitive or relates to vulnerable groups then this raises the compliance bar increasing the risk of a breach.	Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.
20	There is not adequate governance and control in place around the project	Increases the likelihood of something going wrong in the project resulting in a breach or unfair processing	Increases the risk of a compliance breach.	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.
21	There is no data sharing agreement in place for the data included in this project	Increases the likelihood of something going	Increases the risk of a compliance	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by

		wrong in the project resulting in a breach or unfair processing	breach.	association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Providing access to unauthorised people also carries the potential for a fine and/or a prison sentence under the Census (Scotland) Regulations 2010 Researchers could face Safe Haven sanctions.
22	Changes to physical infrastructure, supply chain or emerging cybersecurity issues compromise security arrangements	Increases the likelihood of a data breach	Increases the risk of a breach of DPA/GDPR	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison

				sentence.
23	Organisational changes within NRS, eDRIS/ADRC-S or EPCC affect communication channels	Impedes response to any security incidents or data breaches	Increases the risk of a breach of DPA/GDPR	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research process, reducing our ability to collect and use data in the future. Breach of DPA/GDPR creates potential risk of fine from the information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.

Step five: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

	Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
1	Individuals are identified either deliberately or accidentally resulting in a breach of privacy.	The secure census microdata files are 10% samples of persons and households. They are de-identified records, i.e. they do not include any personal identifiers such as name, date of birth or address. Only trained, accredited researchers are allowed access to the research data, and access is only allowed in the controlled environments of the National Safe Haven and Regional Safe Settings. Researchers will be required to follow a rigorous application and access process – further details on this process are provided at Annex D in the associated Data Sharing agreement.	Risk Minimised	Yes

		All outputs are subject to disclosure control by trained Safe Haven staff and oversight by the NRS statistical disclosure control expert before release to the researchers. Further details are provided at Annex C in the associated Data Sharing Agreement.		
2	Data breach during transfer from NRS to EPCC.	Encrypted data is transferred using Serv-U Secure File Transfer Protocols.	Risk Minimised	Yes
3	Intruder access to safe haven or safe settings resulting in privacy breach	Physical access to the safe haven and safe settings is carefully monitored by trained ADRC-S staff and using CCTV footage. Only approved researchers named on an approved project may access the safe haven or safe settings. Instance-specific two-factor authentication is required to access data on the eDRIS server from within the safe haven or safe settings Security at Safe Settings is subject to the same standards as the National Safe Haven. Security at the Safe Settings is overseen by National Safe Haven staff.	Risk Minimised	
4	Intruder access to EPCC server room (physical access) resulting in privacy breach	Physical security at the Safe Haven has been assessed both by CCP consultants (Evolve, Feb 2016) and by NRS security staff and accepted to meet requirements for storing Official Sensitive data. The data involved has been assessed at BIL3 level which is suitable for the security within the Safe Haven.	Risk Minimised	Yes

		Only University staff and approved contractors accompanied by University staff have access to the facility where the data are stored.		
5	Intruder access to eDRIS server (remote access) resulting in privacy breach	EPCC security assertions have been independently validated by an accredited cybersecurity consultancy (Evolve, February 2016). The secure analytic environment is patched regularly via monthly maintenance windows. Urgent security patches are applied as soon as they are discovered by the EPCC team or advised by vendors. The thin client devices in the eDRIS safe haven and Regional Safe Settings will receive all important security patches as soon as they are discovered by the NSS IT team or advised by vendors.	Risk Minimised	Yes
6	Data breach during transfer and repair, if the disks storing the data develop a mechanical fault and have to be returned to the supplier	Mechanically faulty disks will not be returned to the supplier, but instead will be destroyed following secure disposal and disk sanitisation procedures by NRS.	Risk Removed	Yes
7	Too much data is shared with researchers resulting in the processing being viewed as unfair or excessive.	The secure census microdata files, which are the same as the versions lodged in the Virtual Microdata Laboratory managed by ONS, include only those variables that have been identified as of use to potential researchers. Research proposals seeking to access this data for analysis will require agreement by the ADRC	Risk Minimised	Yes

		approvals panel, the NRS Privacy Group, and the Statistics Public Benefit and Privacy Panel who will make a judgement on whether they are appropriate and proportionate in terms of risk and benefits.		
8	No legal basis for sharing census data meaning the processing is not legal.	The legal basis has been established as being section 5 of the 1920 Census act, **"Preparation of statistics in respect of periods between one census and another.** It shall be the duty of the Statistics Board in relation to England and Wales and the Registrar General for Scotland in relation to Scotland from time to time to collect and publish any available statistical information with respect to the number and condition of the population in the interval between one census and another, and otherwise to further the supply and provide for the better co-ordination of such information, and the Board or Registrar General for Scotland may make arrangements with any Government Department or local authority for the purpose of acquiring any materials or information necessary for the purpose aforesaid."	Risk Removed	Yes
9	The conditions for lawful processing of personal data are not met.	In order to process personal data and sensitive personal data fairly and lawfully for research purposes a Schedule 2 condition and Schedule 3 condition of the Data Protection Act 1998 and the General Data Protection Regulation must be met.	Risk Removed	Yes

		For the processing by the Registrar General, Condition 5(b) of Schedule 2 and Condition 7(1)(b) of Schedule 3 of the Data Protection Act 1998 are met ('the processing is necessary for the exercise of any functions conferred on any person by or under any enactment'). Article 6(1)(c) ('processing is necessary for compliance with a legal obligation to which the controller is subject') and Article 9(2)(j) ('processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…') of the General Data Protection Regulation are also met. For the processing by ADRC-S, Condition 5(d) of Schedule 2 of the Data Protection Act 1998 is met ('the processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person'). Condition 10 of Schedule 3 of the Data Protection Act 1998 is met ('The personal data are processed in circumstances specified in an order made by the Secretary of State'). Paragraph 9 of the Data Protection (Processing of Sensitive Personal Data) Order 2000 is met ('the processing (a) is in the substantial public interest; (b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act); (c) does not support measures or decisions with respect to any		

		particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person'). Article 6(1)(e) ('processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller') and Article 9(2)(j) ('processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…') of the General Data Protection Regulation are also met.		
10	Researchers are not adequately trained in handling personal information, increasing the risk of a breach of privacy.	Researchers have been approved for the Safe Haven which requires them to have undergone 'safe researcher training' to allow them to handle personal data and understand what they can and can't do with it and sanctions for a breach of the conditions.	Risk Removed	Yes
11	Data is shared with organisations who will not act in a secure, ethical or professional manner increasing the risk of a breach of privacy.	Researchers proposing to access and analyse the secure census microdata files at the National Safe Haven or Safe Settings will have to go through a formal application process. Further details of this process are included at Annex D of the associated Data Sharing Agreement. Any sharing of data with parties other than the approved researchers would be a breach of eDRIS user agreement and would be prevented by the IT security measures in the National Safe	Risk Minimised	Yes

		Haven or safe setting.		
12	There is not enough public benefit associated with the project resulting in the project being viewed to be excessive or unfair processing	Census microdata has previously used in a variety of research areas relating to the public benefit – from key indicators of poverty to electoral registration in minority communities. The extending of access to the census microdata is likely to increase the use of Scottish data by providing far easier access to Scottish institutions. Each research project will be assessed by the ADRC panel to ensure there is adequate public benefit for the use of such data.	Risk Minimised	Yes
13	The project will not be able to achieve its aims resulting in the project being viewed to be excessive or unfair processing	Each research project will be assessed by the ADRC approvals panel to ensure it is likely to achieve its aims and thereby constitute fair processing. There is no indication that the initial aim of this project – to provide access to secure census microdata files to approved researchers in the National Safe Haven - is unachievable.	Risk Minimised	Yes
14	Data will be shared with commercial organisations increasing the risk of a breach of privacy	There are no private companies included in the project proposal. Any sharing of data with commercial organisations would be a breach of the terms of the sharing and use of the National Safe Haven and would be prevented by the IT security measures in the National Safe Haven.	Risk Minimised	Yes
15	The security measures around the project are inadequate resulting in a breach of privacy	The transfer mechanisms and National Safe Haven and safe settings have all be assessed against relevant technical security criteria and have been passed to hold data of this level of security	Risk Minimised	Yes
16	The data will be used to contact individuals	The secure microdata sample is made up of de-	Risk Minimised	Yes

	which would be a breach of privacy	identified records, so researchers will not be able to derive contact details or identifying details from the data. Any attempt to use the data to identify individuals would be a breach of the terms of the use of the data and the Safe Haven. Technical security would prevent any identifiable data being removed by researchers.		
17	The use of the data is incompatible with the original purpose it was collected resulting in the processing being viewed as unfair or excessive	Census data is collected for the purpose of producing statistics, therefore this use is compatible.	Risk Removed	Yes
18	Individuals involved are not aware of this use of their data increasing the chance that they would view the processing to be unfair	Data will be processed for purposes which are wholly compatible with the purposes for which the data was originally collected. It is not practical to re-contact everyone involved. The results of any research projects which involve access to the secure census microdata files in the National Safe Haven will be published. The Scotland's Census website will be updated to reflect this.	Risk Minimised	Yes
19	The project uses sensitive data or data referring to vulnerable groups increasing the impact of any breach of privacy	The project does include this type of data but extensive controls are in place to handle data of this type and not allow any breach to privacy to take place.	Risk Minimised	Yes
20	There is not adequate governance and control in place around the project	The project has been approved by data controller. Any proposed analysis of the data will be carried out under normal academic governance by legitimate researchers within the wider Administrative Data Research Centre (Scotland).	Risk Minimised	Yes

		Governance of the wider arrangements for making census data available through eDRIS is provided by a Governance and change management board which meets every 6 months.		
21	There is no data sharing agreement in place for the data included in this project	Data sharing agreement is in place.	Risk Removed	Yes
22	Changes to physical infrastructure, supply chain or emerging cybersecurity issues compromise security arrangements increasing the likelihood of a data breach	eDRIS will notify the Governance and Change Management board of any changes to physical infrastructure, supply chain or security issues affecting the security of the data as soon as possible. eDRIS will send quarterly security reports to NRS IAO (Kirsty MacLachlan) detailing	Risk Minimised	Yes
23	Organisational changes within NRS, eDRIS/ADRC-S or EPCC impede proper response to any security incidents or data breaches	All parties will notify the Governance and Change Management board of any changes to organisational structure which might affect the integrity of the data sharing agreement as soon as possible. The Data Sharing Agreement associated with this project allows NRS to request that the data holders (EPCC) securely destroy the data, in the event of a breach of the data sharing agreement.	Risk Minimised	Yes

Step six: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
The key underlying risks are: - that there is a breach to privacy through loss, leak or theft of data. - any analysis of the data is viewed as excessive or unfair and so fails to meet DPA/GDPR principles.	Key solutions are that the data is de-identified and any access would be in the highly controlled Safe Haven and Safe Settings environments by accredited researchers. Any proposed project to analyse the data would be subject to assessment by peers and independent experts for a judgement to be made on whether it would be either unfair or excessive.	The project has been approved in NRS by the Information Asset Owner (IAO) for Census data, Kirsty MacLachlan.

Step seven: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Respond to any concerns expressed by NRS Privacy Panel, NRS Security or SGLD	tbc	Sandy Taylor
Finalise sign off of DSA	tbc	Kirsty MacLachlan
Update Census website about access to data via Safe Haven	tbc	Sandy Taylor

Contact point for future privacy concerns
ADRC Scotland <adrc-s@ed.ac.uk>

Part 3: Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the DPA and the GDPR or other relevant legislation, for example the Human Rights Act.

DPA Principle 1 and GDPR Principle 1 (Article 5(1)(a))

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in DPA Schedule 2 and GDPR Article 6 is met, and

b) in the case of sensitive personal data, at least one of the conditions in DPA Schedule 3 and GDPR Article 9 is also met.

Have you identified the purpose of the project?

Yes. The proposal aims to improve research access to secure microdata files from Scotland's Census 2011. See step 1 for more information.

How will you tell individuals about the use of their personal data?

Information about our uses of census data has been published on the Scotland's Census website.

Do you need to amend your privacy notices?

No. Our privacy notices are up to date. The privacy section of the Scotland's Census website explains how we protect the confidentiality of census data and ensure transparency and confidence in all that we do.

Have you established which conditions for processing apply?

Yes. See step 5, section 7.

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Consent is not being relied on.

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

The census microdata files are de-identified and will not interfere with individuals' right to privacy under Article 8. The provisions of Article 8 allow public authorities to enquire into a person's private life where they have a legal authority to do so and where such an enquiry is necessary in a democratic society for one of the aims stated in the Article. Lawful authority for collection and processing of census is provided by the Census Act 1920 and that it is necessary for the economic well-being of the country and for the purposes of the protection of health and the rights and freedoms of others.

Have you identified the social need and aims of the project?

Yes. Analysis of census data supports evidence based policy making and research, and informs the allocation and targeting of resources.

Are your actions a proportionate response to the social need?

Yes. This proposal will improve access to census microdata files for research and analysis, within secure, controlled environments.

DPA Principle 2 and GDPR Principle 2 (Article 5(1)(b))

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Yes. The proposal improves access to census microdata for research purposes.

Have you identified potential new purposes as the scope of the project expands?

No.

DPA Principle 3 and GDPR Principle 3 (Article 5(1)(c))

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Extensive statistical methodologies and quality assurance processes are used to ensure that the census data is fit for purpose and best meet the needs of data users.

Which personal data could you not use, without compromising the needs of the project?

All of the data is required.

DPA Principle 4 and GDPR Principle 4 (Article 5(1)(d))– accurate, kept up to date, deletion

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

Not applicable.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

It is not necessary to keep census data up to date as the data collected by the census represents a snapshot in time.

DPA Principle 5 and GDPR Principle 5 (Article 5(1)(e))

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

There is no set time limit on how long the data can be stored in the National Safe Haven, but the associated Data Sharing Agreement (which includes a provision for NRS to require deletion of the data) will be reviewed annually.

Are you procuring software that will allow you to delete information in line with your retention periods?

Data can be confidentially deleted at the National Safe Haven.

DPA Principle 6 and GDPR Articles 12-22

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

The census data is exempt from data subject access rights under section 33 of the DPA.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

No marketing is involved.

DPA Principle 7 and GDPR Principle 6 (Article 5 (1)(f))

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

The technical infrastructure used to transfer and store the data has been assessed by a CCP consultant and provides adequate protection.

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

All members of staff involved in the data transfer and processing are appropriately trained and have signed confidentiality statements and the Census Confidentiality Undertaking.

DPA Principle 8 and GDPR Article 24

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the European Economic Area (EEA)?

No.

If you will be making transfers, how will you ensure that the data is adequately protected?

Not applicable.