National Records of Scotland

Data Protection Impact Assessment (DPIA): Providing access to Census data for data linkage projects at the eDRIS National Safe Haven

Document Control

Title	**Data Protection Impact Assessment (DPIA): Providing access to Census data for data linkage projects at the eDRIS National Safe Haven**
Prepared by	Liam Cavin
Approved by	Alan Ferrier
Date of approval	May 2024
Review frequency	Annual
Next review date	May 2025

Status Control

Version	Date	Reason for Amendment
1.0	06/02/2018	Created based on DPIA for providing access to Census Microdata via the national safe haven and regional safe settings
2.0	15/05/2018	Baselined version This is a live document and will be updated as circumstances change.
3.0	22/06/2023	Published DPIA was prior to UK GDPR. Review has updated DPIA to e.g. reflect changes to the UK Data Protection Legislation, organisational name updates, addition of remote working. Due to proposed changes in UK Data Protection legislation which are currently going though both Houses of Parliament the decision was made not to update the template of this DPIA until the next update.
4.0	03/05/2024	Updated to reflect new tools used in data processing.

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. Record-level Census data information is already available to approved researchers on application and subject to approvals. The initial DPIA of 2018 formalised an existing arrangement.

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? Does the project involve matching data or combining datasets from different sources?

NRS -No, NRS are not using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.

Individual data linkage projects - Yes – depending on the project. Census data may be matched to other data sources subject to the necessary approvals being obtained. Microdata are extracts of census data for whole households and individuals. Custom Microdata enables researchers to see combinations of census information that would not normally be possible from standard published census tables. The project approval process is described at 2.1, below.

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. Will you profile children or target online services at them?

No the project does not involve using new technology that might be perceived as being privacy intrusive.
NRS will not profile children or target online marketing services at children (see question 8, below).

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 special category personal information. Data will be provided without directly identifying information.

8. Will the project require you to contact individuals in ways that they may find intrusive? Is the project tracking individuals' location or behaviour?

No the project does not require NRS to contact individuals at all.

The Census asks questions relating to a respondent's locations e.g. it asks for the address of the respondent on the date of the Census and their address one year ago and their work address. The Census also asks certain questions relating to behaviour.

Analysing these questions it may be possible to track an individual's location or behaviour over time. However, such tracking would not have any consequences for the individual involved.

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 DPIA covers the arrangements for researchers to access Census data as part of data linkage projects via eDRIS through the National Safe Haven.

Each individual data linkage project obtains approval from the Statistics Public Benefit and Privacy panel (SPBPP), and where health data from Scottish NHS Health Boards is involved the NHS Scotland Public Benefit & Privacy Panel for Health and Social Care (HSC-PBPP). A separate Data Sharing Agreement is drawn up between NRS and the organisation conducting the research. This DPIA is intended to cover the general access arrangements for projects accessing Census data for linkage projects in this way. For more information, the DPIA covering Scotland Census 2022 can be found at Data protection impact assessment | Scotland's Census (scotlandscensus.gov.uk).

Bespoke Census extracts, linked to data from other sources, will be stored in the servers at the Edinburgh Parallel Computing Centre (EPCC), for access by named, approved researchers in the eDRIS National Safe Haven. Secure physical settings for access to the National Safe Haven are at the Edinburgh Bioquarter and the Regional Safe Settings (in St Andrews, Aberdeen, Dundee and Glasgow) are operated by SCADR, supported by eDRIS, and subject to the same security protocols. Since 2020, access to secure physical settings has not been

possible. Researchers can access data in the National Safe Haven remotely, an arrangement initially established to allow research to continue during the COVID-19 pandemic. We are currently reviewing these access arrangements with SPBPP and eDRIS.

This DPIA addresses 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
Linked data projects are delivered by 3 Digital Economy Act (DEA) accredited delivery organisations: National Records of Scotland (who act as trusted third party to create linkage keys), eDRIS (part of Public Health Scotland, and who act as data processors), and EPCC (commissioned by eDRIS to act as a sub-processor to run and maintain the National Safe Haven).

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

4) Remote Access (access to data by methods other than being in the physical location of a Safe Haven)
Due to the COVID-19 pandemic, remote access for authorised researchers and staff was granted as access in person to physical safe settings was not possible. This will be maintained until the Bioquarter is reopened for researchers. We are currently reviewing these access arrangements with SPBPP and eDRIS.

Further background information on the current access arrangements is available on the Scotland's Census website.
A Privacy Notice for Custom Microdata Census Projects is found here GROS - Census - General Report Template.dot (scotlandscensus.gov.uk).

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.

Scotland's census is the official count of every person and household in the country. The answers people give to census questions help build up a picture of the population. Government and other service providers rely on census data to make important decisions. Census data may also be accessed by approved researchers for projects with demonstrable public benefit.

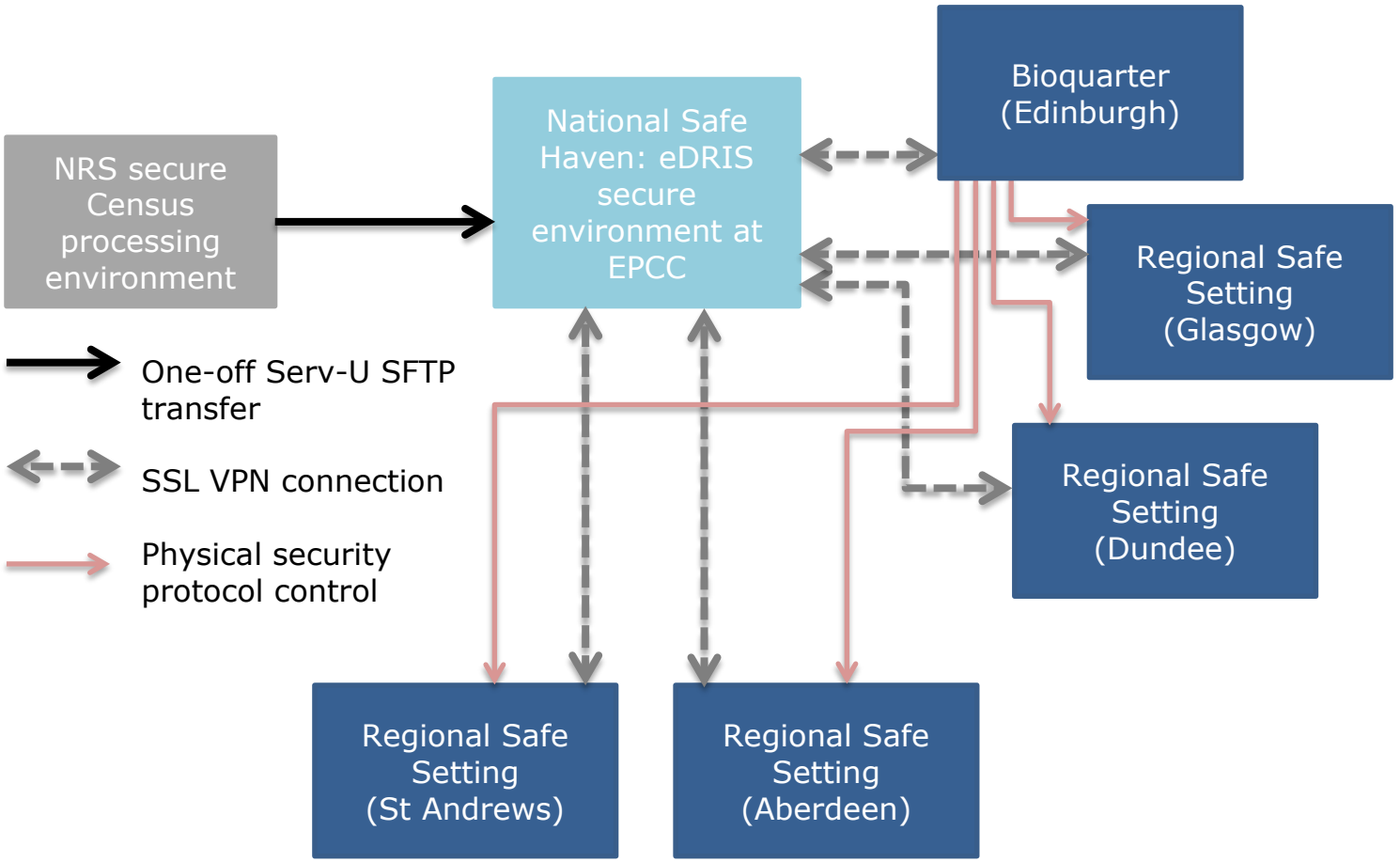
Microdata are small samples of census data for whole households and individuals. The information within each microdata set depends upon the project question being investigated by the researchers. Custom Microdata enables researchers to see combinations of information that would not normally be possible from standard published census tables. The people who receive access to Custom Microdata are generally researchers from academic institutions and the public sector within the UK who analyse the data to answer specific research questions.

The data will be encrypted by NRS at source and transferred to the eDRIS secure environment at the EPCC using a secure transfer method Serv-U SFTP. All persons involved in the data transfer, processing and analysis are appropriately trained and have signed the Census Confidentiality Undertaking form (this confirms they are aware of their legal obligations regarding use and disclosure of Census data and the penalties for unlawful disclosure of, unlawful use of and/or failure to keep the data safe. Such penalties include fines or imprisonment). This includes all NRS, eDRIS and EPCC staff as well as researchers.

Each project has a set end date for data access for analysis, and then a period of secure archival retention within the eDRIS secure environment at the EPCC to allow for publication and peer review quality assurance. The time periods for these are reviewed and agreed by the independent Statistics and Public Benefit Privacy Panel. On this end date no-one will be able to access the project data and all requests for access for the purposes of analysis via the National Safe Haven will be denied. At the end of the archive retention period, typically 5 years, the project data will be securely and confidentially destroyed.

Each project level Data Sharing Agreement (which includes a provision for NRS to require deletion of the project data) will be reviewed annually. The EPCC has been accredited for the provision of data under the DEA, with its security controls assessed against the ISO27001 security standard t. The accreditation process assessed all aspects of the security and capability of the Scottish National Safe Haven infrastructure and operations. This accreditation is subject to annual reviews.

Once hosted in the National Safe Haven, the data can be accessed via a Virtual Private Network (VPN) with SSL encryption and two-factor authentication (a pin number is sent to the user phone number along with password verification). The terminals in the Bioquarter and Regional Safe Settings provide a secure connection to the eDRIS server, which means the terminals cannot store local copies of data.


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

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.

NRS performed a public consultation on the Census Outputs which lasted approximately 3 months (October 2022 to February 2023). The results from that Consultation can be found on the Scotland's Census Website here Census outputs consultation | Scotland's Census (scotlandscensus.gov.uk) and the report containing NRS responses can be found here scotland-s-census-2022-sdc-and-outputs-census-outputs-consultation-report.pdf (scotlandscensus.gov.uk).

eDRIS provide direct support to researchers through their Research Coordinators. eDRIS is not a data provider but requires submission of a formal application to the Statistics Public Benefit and Privacy Panel (SPBPP) panel and approval of this application before any project seeking access to census data can commence. NRS, through its Privacy Group, participates in this panel review. SPBPP review includes scrutiny of privacy risks as part of an assessment of research project proposals by SPBPP. Further details of this approvals process are included at Annex A. Individual project applications are also expected to demonstrate how they have consulted with stakeholder groups, and how they will communicate the project outcomes.

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 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) related compliance risks.

	Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk	Likelihood	Severity	Overall Risk
1	Individuals are identified either deliberately or accidentally during analysis and/or accidentally/deliberately identified in the public domain by researchers.	Potential disclosure of personal data (including special category personal data) which could lead to stress and anxiety for the individual(s) identified and potentially their families as well.	Breach of DPA/UK 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/UK GDPR creates potential risk of penalties e.g. notices from the Information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020.	Possible	Severe	High
2	Data breach during transfer from NRS to EPCC.	Potential disclosure of personal data (including special category personal data) which could	Breach of DPA/UK GDPR; breach of Census legislation; 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.	Remote	Severe	Medium

		lead to stress and anxiety for the individual(s) whose data is involved.	compliance with government security policies; possible sanctions.	Breach of DPA/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. . Misuse of information is not allowed under the Census (Scotland) Regulations 2020.			
3	Intruder access to the Edinburgh Bioquarter or Regional Safe Settings	Potential disclosure of personal data (including special category personal data) which could lead to stress and anxiety for the individual(s) whose data is involved.	Breach of DPA/UK 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/ UK GDPR creates potential risk of penalties from the Information Commissioner's Office (ICO). Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.	Remote	Minimal	Low
4	Intruder access to EPCC server room (physical access)	Potential disclosure of personal data (including special category personal data) which could lead to stress and anxiety for	Breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO.	Remote	Minimal	Low

		the individual(s) whose data is involved.	government security policies; possible sanctions.	Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020.			
5	Intruder access to EPCC server (remote access)	Potential disclosure of personal data (including special category personal data) which could lead to stress and anxiety for the individual(s) whose data is involved.	Breach of DPA/UK 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/ UK GDPR creates potential risk of penalties from the (ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020.	Remote	Severe	High
6	Personal data which is not needed is shared with researchers resulting in the processing being viewed as unfair or excessive.	Increases the impact of any loss of personal data. Sharing personal data which is not needed could lead to stress	Sharing personal data which is not needed to achieve the purpose or use of such data is against	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/UK GDPR creates potential risk of penalties from the ICO.	Remote	Significant	Medium

		and anxiety for the individual(s) whose data is involved	DPA/UK GDPR principles.	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 eDRIS services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions from eDRIS services and sanctions from listed funders.			
7	No legal gateway for sharing census data is established and data is still shared (either accidentally or deliberately).	Unlawful disclosure of personal data (including special category personal data) which could lead to stress and anxiety for the individual(s) whose data is involved.	Would be a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Misuse of information is not allowed under the Census (Scotland) Regulations 2020. Researchers could face Safe Haven sanctions – suspension for a fixed period or permanently from eDRIS services, and in serious cases from listed data services and listed funders as well. The responsible organisation may also face fixed period suspensions and sanctions from listed funders.	Remote	Minimal	Low

8	The basis for lawful processing of personal data is not met.	Processing must be legal under DPA/UK GDPR. Unlawful processing of personal data (including special category personal data) which could lead to stress and anxiety for the individual(s) whose data is involved.	Would be a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO.	Remote	Minimal	Low
9	Researchers are not adequately trained in handling personal information, increasing the risk of a breach of privacy.	Increases the risk of an accidental and/or unlawful disclosure of personal data which could lead to stress and anxiety for the individual(s) whose data is involved.	Increases the risk of a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.	Remote	Significant	Medium
10	Data is shared with organisations who will	Increases the risk of a	Increases the risk of a	Reputational, operational and financial risk – trust in NRS and	Remote	Significant	Medium

	not act in a secure, ethical or professional manner increasing the risk of a breach of privacy.	disclosure of personal data – possibly for financial gain by the organisation. This could lead to stress and anxiety for the individual(s) whose data is involved.	breach of DPA/UK GDPR; 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020. Researchers could face Safe Haven sanctions.			
11	There is not enough public benefit associated with the project and therefore there is a risk of public perception that the data is not used proportionately.	Likely that this could be viewed as unfair processing if the public benefit doesn't justify the privacy risks to individuals whose data is involved. This could lead to the stress and anxiety for the individual(s) whose data is involved.	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Researchers could face Safe Haven sanctions.	Remote	Minimal	Low
12	Data is shared unlawfully and/or accidentally with	Increases the risk of an unlawful and/or	Increases the risk of a breach of	Reputational, operational and financial risk – trust in NRS and	Remote	Severe	High

	commercial organisations	accidental disclosure of personal data – possibly for financial gain by the organisation. This could lead to stress and anxiety for the individual(s) whose data is involved.	DPA/UK GDPR; 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020. Researchers could face Safe Haven sanctions.			
13	The security measures around the project are inadequate resulting in a breach of privacy	Increases the risk of an unlawful and/or accidental disclosure of personal data. This could lead to stress and anxiety for the individual(s) whose data is involved.	Increases the risk of a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 https://www.legislation.gov.uk/ukpga/Geo5/10-11/41/contentscarries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.	Remote	Severe	High
14	The data will be used unlawfully to contact	Individuals have not agreed to be contacted and	This would be a breach of personal data	Reputational, operational and financial risk – trust in NRS and	Remote	Severe	High

	individuals which would be a breach of privacy	there is no reason to contact them using our lawful basis. To contact individuals unlawfully could cause distress or detriment to individuals. This would be beyond the purpose of this project and as well as being unlawful would not be fair or ethical.	and would breach DPA/UK GDPR and census privacy undertakings.	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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.			
15	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. This could lead to stress and anxiety for the individual(s) whose data is involved.	Unfair processing, excessive data sharing or use of irrelevant data is against DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO.	Remote	Minimal	Low
16	Individuals involved are not aware of this use of their data increasing the chance that they	If individuals felt the processing was not transparent	not informing individuals of the use of their data,	Reputational, operational and financial risk – trust in NRS and research infrastructure is damaged and, by association, trust in the whole research	Remote	Minimal	Low

	would view the processing to be unfair	(they haven't been informed), unfair or unwarranted it could cause them distress.	unfair processing excessive data sharing or use of irrelevant data is against DPA/UK GDPR principles.	process, reducing our ability to collect and use data in the future. Breach of DPA/UK GDPR creates potential risk of penalties from the ICO.			
17	The project unlawfully uses special category data or data referring to vulnerable groups increasing the impact of any breach of privacy	Unlawful processing of special category data or data referring to vulnerable groups could lead to stress and anxiety for the individual(s) whose data is involved and their families.	If the use of data of this kind is judged to be not needed this would be a breach of DPA/UK GDPR and other UK legislation. .	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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.	Remote	Severe	High
18	There is not adequate governance and controls in place around the project	Increases the likelihood of something going wrong in the project that could result in a breach or unfair or unlawful processing.	Increases the risk of a compliance and/or personal data 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/UK GDPR creates potential risk of penalties ICO.	Remote	Minimal	Low

		This could lead to stress and anxiety for the individual(s) whose data is involved.		Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Researchers could face Safe Haven sanctions.			
19	There is no data sharing agreement in place (between the relevant controllers) for the data processed in this project.	Increases the likelihood of something going wrong in the project that could result in a breach or unfair or unlawful processing. This could lead to stress and anxiety for the individual(s) whose data is involved.	Increases the risk of a compliance breach and/or personal data 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020. Researchers could face Safe Haven sanctions.	Remote	Minimal	Low
20	Changes to physical infrastructure, supply chain or emerging cybersecurity issues compromise security arrangements, e.g. National Safe Haven is no longer DEA accredited.	Increases the likelihood of a data breach. This could lead to stress and anxiety for the individual(s) whose data is involved.	Increases the risk of a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.	Possible	Significant	High

21	Organisational changes within NRS, eDRIS or EPCC affect communication channels	Impedes response to any security incidents or data breaches. This could lead to delayed investigations or communications to individual(s) whose data is involved (if required). This could lead to stress and anxiety for the individual(s) whose data is involved.	Increases the risk of a breach of DPA/UK 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/UK GDPR creates potential risk of penalties from the ICO. Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence.	Probable	Minimal	Low
22	Researcher not complying with standard terms and conditions of accessing	Potential disclosure of personal data (including special category personal data.) This could lead to stress and anxiety for the individual(s) whose data is involved	Increases risk of a Breach of DPA/UK 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	Possible	Significant	Medium

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?	**Residual Risk (Low,Medium,High)**	**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 and/or accidentally and/or deliberately identified in the public domain.	Census extracts provided for linkage studies will be de-identified records, i.e. they will not include any personal identifiers such as name, full 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 A.	Risk Minimised	Low	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. There is an established breach reporting process within NRS. eDRIS also have a breach reporting process. The two organisations would work together to investigate any breaches.			
2	Data breach during transfer from NRS to EPCC.	Encrypted data is transferred using Serv-U Secure File Transfer Protocols.	Risk Minimised	Low	Yes
3	Intruder access to the Edinburgh Bioquarter or Regional Safe Settings resulting in privacy breach	*At the time of publishing this DPIA the physical access to the Bioquarter is not possible for approved research users and approved staff.* Physical access to the Edinburgh Bioquarter or Regional Safe Settings is carefully monitored by trained staff and uses CCTV footage. Only approved researchers named on an approved project may access the safe settings.	Risk Minimised	Low	Yes

		Instance-specific two-factor authentication is required to access data on the eDRIS server. Security at the Edinburgh Bioquarter or Regional Safe Settings is overseen by eDRIS staff.			
4	Intruder access to EPCC server room (physical access) resulting in privacy breach	Physical security at the Safe Haven has been assessed as part of the accreditation process which is based on the security controls in the ISO27001 standard. This DEA accreditation is reviewed annually. Only University staff and approved contractors accompanied by University staff have access to the facility where the data are stored.	Risk Minimised	Low	Yes
5	Intruder access to EPCC server (remote access) resulting in privacy breach	EPCC security has passed DEA accreditation to an ISO27001 certification standard, this is reviewed annually. The secure analytic environment is patched regularly via monthly maintenance windows.	Risk Minimised	Low	Yes

		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.			
6	Personal data which is not needed is shared with researchers resulting in the processing being viewed as unfair or excessive.	Census extracts shared for data linkage studies will include only those variables that have been identified as necessary for the study by researchers. Research proposals will require agreement by the NRS Privacy Group and the Statistics Public Benefit and Privacy Panel (and if required HSC-PBPP) who will make a judgement on whether they are appropriate and proportionate in terms of risk and benefits. Researchers must provide justification for each variable requested. These justifications will be assessed by the Panel members (of	Risk Minimised	Low	Yes

		each panel that needs to give approval) to ensure adherence to data minimisation principles.			
7	No legal gateway for sharing census data is established meaning the processing is not legal.	The legal gateway has been established as being section 4 of the 1920 Census act: **"Preparation of reports and abstracts.** The Statistics Board or Registrar General for Scotland may, if it or he so thinks fit, at the request and cost of any local authority or person, cause abstracts to be prepared containing any such statistical information, being information which is not contained in the reports made by it or him under this section and which in its or his opinion it is reasonable for that authority or person to require, as can be derived from the census returns."	Risk Removed	Low	Yes
8	The basis for lawful processing of personal data is not met.	NRS's lawful basis for processing is UK GDPR Article 6(1) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official	Risk Removed	Low	Yes

		authority vested in the controller ” Our conditions for processing special category information are as follows: UK GDPR Article 9(2)(j) - the processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1), supported by Schedule 1, Part 1, Condition 4 of the Data Protection Act 2018. Researchers that access Census data must have a lawful basis for processing personal data (and if needed special category data). This is reviewed by each of the Panels they apply to for access. Additionally, their lawful basis is stated in the relevant Data Sharing Agreements.			
9	Researchers are not adequately trained in handling personal information, increasing the risk of a breach of privacy.	Researchers will have been approved for the Safe Haven which requires them to have successfully completed ‘safe researcher training’ to allow them to handle personal data and understand what they can and can’t do with it and	Risk Removed	Low	Yes

		sanctions for a breach of the conditions. NRS participates in delivering this training to researchers. Researchers must sign and agree to adhere to the Census Confidentiality Undertaking form. Researchers sign and adhere to remote access conditions within the DSA Appendix. Researchers sign and adhere to the User Agreement form with eDRIS.			
10	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 Census data in the National Safe Haven will have to go through a formal application process, involving scrutiny from independent panels. Further details of this process are included at Annex A. Any sharing of data with parties other than the approved researchers would be a breach of the eDRIS user agreement and would be prevented by the IT security measures in the National Safe Haven.	Risk Minimised	Low	Yes

		Data Sharing Agreements between relevant controllers are completed.			
11	There is not enough public benefit associated with the project and therefore there is a risk of public perception the data is not used proportionately.	Each research project will be assessed by the SPBPP panel to ensure there is adequate public benefit for the use of such data.	Risk Minimised	Low	Yes
12	Data is shared unlawfully and/or accidentally with commercial organisations	Any applications by a private company would be assessed by the SPBPP panel to assess there is enough public benefit inherent in the research. Private companies would be subject to the same security and governance arrangements as any other research institution.	Risk Minimised	Low	Yes
13	The security measures around the project are inadequate resulting in a breach of privacy	The National Safe Haven is managed by eDRIS and its IT infrastructure is provided by EPCC. eDRIS have been accredited for the preparation and processing of data and EPCC for the provision of data, under the DEA. The accreditation process assesses organisations against the security controls	Risk Minimised	Medium	Yes

		required by the ISO 27001 security standard. Accreditation is subject to annual reviews.,			
14	The data will be used unlawfully to contact individuals which would be a breach of privacy	Census extracts provided for data linkage studies will never contain personal identifiers, 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. The technical security of the National Safe Haven would prevent any identifiable data being removed by researchers. NRS has an established breach process which would be followed in the event of unlawful contact. eDRIS also have a breach reporting process. The two organisations would work together to investigate any breaches.	Risk Minimised	Low	Yes
15	The use of the data is incompatible with	Census data is collected for the purpose of producing	Risk Removed	Low	Yes

	the original purpose it was collected resulting in the processing being viewed as unfair or excessive	statistics, therefore this use is compatible.			
16	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 – information is made available via Scotland's Census Website. The results of any research projects which involve access to Census data in the National Safe Haven will be published. The Scotland's Census website will be updated to reflect this.	Risk Minimised	Low	Yes
17	The project unlawfully uses special category 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 protect data of this type, and this minimises the risk of a breach to privacy taking place. NRS has an established Breach process which would be followed in the event of a Breach occurring. eDRIS also	Risk Minimised	Low	Yes

		have a breach reporting process. The two organisations would work together to investigate any breaches.			
18	There is not adequate governance and control in place around the project	For any proposed project, data access depends on completion of all necessary panel approvals, data sharing agreements, data processing agreements, user agreements and census confidentiality undertakings.	Risk Minimised	Low	Yes
19	There is no data sharing agreement in place (between the relevant controllers) for the data processed in this project.	A Data Sharing agreement must be signed and agreed and in place prior to any sharing of data.	Risk Removed	Low	Yes
20	Changes to physical infrastructure, supply chain or emerging cybersecurity issues compromise security arrangements, e.g. National Safe Haven is no longer DEA accredited.	eDRIS will notify NRS at the earliest opportunity of any and all changes to physical infrastructure, supply chain or emerging cybersecurity issues via written email to Information Asset Owner (IAO), the Director of Statistical Services.	Risk Minimised	Medium	Yes
21	Organisational changes within NRS, eDRIS or EPCC affect communication channels.	Regular meetings established between internal and external data linkage partners.	Risk Minimised	Low	Yes

		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.			
22	Researcher not complying with standard terms and conditions of accessing confidential data that they agreed to prior to accessing data.	Breach of confidentiality under Census Act 1920 carries potential of fine and/or prison sentence. Misuse of information is not allowed under the Census (Scotland) Regulations 2020. Researchers could face Safe Haven sanctions. Researchers must sign and agree to adhere to the Census Confidentiality Undertaking form. Research Institution sign and adhere to remote access conditions within the DSA Appendix. Researchers sign and adhere to the User Agreement form with eDRIS. Census extracts provided for data linkage studies will never contain personal	Risk Minimised	Medium	Yes

		identifiers, 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.			

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 National Safe Haven environment by accredited researchers. Any proposed project to analyse the data would be subject to assessment by peers and independent experts to ensure that data minimisation principle is maintained.	The project has been approved in NRS by the Information Asset Owner (IAO) for Census data, (the Director of Statistical Services)
DPIA 2023 Review risks–- As above and also remote access working	DPIA Review – solutions as above	The review has been approved in NRS by the Information Asset Owner (IAO) for Census data, (the Director of Statistical Services) and shared with the DPO for awareness.

Step seven: Integrate the DPIA outcomes back into the project plan (2023)

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

Contact point for future privacy concerns
Data Access team Email: dataaccess@nrscotland.gov.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.

UK GDPR AND EU GDPR Principle (a) (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 Article 6 is met, and

b) in the case of special category personal data, at least one of the conditions in Article 9 is also met.

Have you identified the purpose of the project?

Yes. The proposal aims to improve research access to Scottish Census data for data linkage studies. See step 1 for more information.

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

Information about our uses of Scottish 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. Privacy Notice for 2022 Census: Scotland's Census 2022 - Privacy notice | Scotland's Census (scotlandscensus.gov.uk) Privacy Notice for Custom Microdata: Scotland's Census: Custom Microdata Privacy Statement | Scotland's Census (scotlandscensus.gov.uk)

Have you established which conditions for processing apply?

Yes. NRS's lawful basis for processing is UK GDPR 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." Our conditions for processing special category information are as follows: UK GDPR Article 9(2)(j) - the processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1), supported by Schedule 1, Part 1, Condition 4 of the Data Protection Act 2018.

Researchers who access Census data must have a lawful basis for processing personal data (and if needed special category data). This is reviewed by each of the Panels they apply to for access. Additionally their lawful basis is stated in the relevant Data Sharing Agreements.

The appropriate legal gateway for NRS sharing census data for linkage projects is provided by section 4 of the Census Act 1920. Relevant conditions under the Data Protection Act 2018 and the UK General Data Protection Regulation for processing personal data and special category 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.

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?

Census extracts provided for data linkage studies will be 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 Scotland's Census data for research and analysis, within secure, controlled environments.

UK GDPR AND EU GDPR Principle (b) (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 Scotland's census data for research purposes.

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

No.

UK GDPR AND EU GDPR Principle(c) (Article 5l(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 by NRS to ensure that the census data is fit for purpose and best meet the needs of data users.

For further information please refer to the Scotland's Census Website.
For example: Methodology Enhancements to Secure High Quality Outputs |'Scotland's Census (scotlandscensus.gov.uk), Statistical quality assurance |'Scotland's Census (scotlandscensus.gov.uk) and Statistical methodology |'Scotland's Census (scotlandscensus.gov.uk).

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

All of the data is required.

UK GDPR AND EU GDPR Principle (d) (Article 5(1)(d))– accurate, kept up to date, deletion

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

We are procuring new analytical software for processing census data within NRS, but this will not be used to amend the data being used in linkage projects.

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

Every household in Scotland has a legal responsibility to complete a census questionnaire. This means the census offers a detailed and accurate snapshot of the nation.

Whilst the information is provided by the respondents and accuracy of the information is reliant upon the individual completing the Census, NRS also uses a variety of methods and processes to ensure Census data is accurate.

Information on methods used by NRS to ensure accuracy of the Census Data such as Data Cleansing, Use of Administrative Data, Estimation and Adjustment, Edit and Imputation and Statistical Quality Assurance can be found at Statistical methodology |'Scotland's Census (scotlandscensus.gov.uk).

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

UK GDPR AND EU GDPR Principle (e) (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?

The Census data itself is stored indefinitely by NRS.

Each project has a set end date for data access for analysis and then a period of secure archival retention. The time periods for these are reviewed and agreed by the independent Statistics and Public Benefit Privacy Panel and detailed in the relevant Data Sharing Agreement (which is reviewed annually). On this end date for access for analysis no-one will be able to access the Custom Microdata and all requests for access for the purposes of analysis via the National Safe Haven will be denied. At the end of the archive retention period, typically 5 years, the Custom Microdata will be securely and confidentially destroyed.

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

No. Census Data is kept by NRS forever.
Project data will be deleted by EPCC in line with project retention periods as detailed in the relevant Data Sharing Agreement.

UK GDPR AND EU 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?

Subject Rights that Apply to Custom Census Microdata we process

- ✓ the right to be informed;
- ✓ the right to lodge a complaint with the Information Commissioner's Office.

However, the following rights do not apply to the use of personal data for scientific or historical research purposes or statistical purposes, where responding to these rights would prevent the research or statistical purpose from being achieved.

X Right to access your personal data;
X Right to rectify incorrect data
X Right to have your data erased
X Right to restrict what can be done with your data
X Right to data portability
X Right to object to the use of your data
X Rights in relation to automated decision making (no automated decision making occurs)

Individuals are informed of these rights and advised on how to exercise them in the Scotland's Census Custom Microdata Privacy Notice.

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

UK GDPR AND EU GDPR Principle (f) (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?

NRS Technical and Organisational measures to protect data include:

NRS currently have Cyber Essentials and Cyber Essentials Plus accreditation.

https://www.ncsc.gov.uk/cyberessentials/search

National Records of Scotland
Cyber Essentials - Certificate number: IASME-CE-030754
Cyber E–essentials Plus - Certificate number: IASME-CEP-006839

The NRS Technical Security Standards - https://erdm.scotland.gov.uk:8443/documents/A32279387/details - covers the mandatory baseline technical security standards of NRS storage of data and access within the physical and technical environments, both for our internal systems and for any 3rd parties.
To prevent the infection of NRS computers and networks and avoid the potentially dire consequences of such infection, there are several key controls that will be adopted as policy. These can be found in the NRS end point protection policy - https://erdm.scotland.gov.uk:8443/documents/A33687913/details .

Access to data is limited to individual NRS user accounts that need access.

NRS also has a Data Breach Procedure (see Personal data breaches (nrscotland.gov.uk)) and various relevant internal policies to protect data such as the Data Protection Policy and The IT Security Policy. NRS staff must also adhere to the Civil Service Code of conduct.

NRS Staff all have BPSS Security clearance.

The technical infrastructure at EPCC used to transfer and store the data has been assessed through the DEA accreditation process against the security controls of the ISO27001 security standard. This accreditation is reviewed annually.

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

All members of NRS staff involved in the data transfer and processing are appropriately trained in the safe and secure transfer of confidential Census data and have agreed to and signed confidentiality statements and the Census Confidentiality Undertaking.

All members of eDRIS and EPCC staff involved in the data transfer and processing are appropriately trained and have access to documentation that covers each step of a linked census microdata extract project.

UK GDPR AND EU 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.

Annex A: Approval process for research projects using NRS census data

Background

This annex describes the process to be used when an approved researcher wishes to use an extract of data from the Scottish census (2001 or 2011) for a research project. All projects access research data, stored in the National Safe Haven at the Edinburgh Parallel Computing Centre. The document covers the project life cycle, including the various approval processes required and data transmission to the safe haven and statistical disclosure control of outputs.

The annex is divided into three sections. These cover (1) basic arrangements for processing new projects involving census data, (2) specific arrangements for projects requiring only census data and (3) specific arrangements for projects requiring linkage of census data to other data.

1. Basic arrangements for **all** projects:-

- Researchers should contact eDRIS and be assigned a Research Coordinator, who will support them in developing their project.
- All researchers must either have current ONS safe researcher accreditation or must obtain this before they gain access to data.
- All projects will require approval from the Statistics Public Benefit and Privacy Panel (SPBPP). NRS review these projects through the NRS Privacy Group, which contributes to the SPBPP review.
- The first point of contact in NRS for queries from eDRIS about data variables, feasibility etc. is the Data Access team.
- Specific details about the processes for requesting data for projects that use either only census data or census data linked to other data are described below in sections (2) and (3) respectively.

2. The process to access **only census data** in the National Safe Haven :-

a) Application:

To gain access to a census microdata extract, a researcher must apply through SPBPP. Their eDRIS Research Coordinator will guide them through that process. Only researchers approved through this process will be able to access the data. Only the cohort and variables specified in the application will be extracted and supplied. Analysis is restricted to the purposes and research questions specified in the application.

b) Amendments:

Any amendments to the proposal that may be requested by the researchers after the project has been approved must be submitted in writing to the Statistics PBPP, via their eDRIS Research Coordinator. Such amendments might include addition or deletion of a researcher, or addition or deletion of requested variables, or extension of project end dates.

c) Data Sharing Agreement (DSA)

The Data Sharing Agreement between NRS and the researcher's organisation for each project will be developed and led by the NRS Data Access team. Authorised signatories for NRS are NRS Procurement plus IAO.

d) Data extraction

Data will be extracted by the NRS Data Access team.

e) Data transfer

Data will be transferred from NRS to the National Safe Haven using the eDRIS secure transfer tool servU.

f) Data storage and access for researchers

Data for each project will be checked by a research coordinator in the eDRIS user services team and stored in a specific folder within the National Safe Haven to which the researcher(s) will be given controlled access.

g) Output checking

All outputs requested for release by the researcher(s) will be checked by eDRIS user services (applying the Public Health Scotland (PHS) Statistical Disclosure Control (SDC) policy and any additional rules applying to census data and supplied by NRS). The NRS Data Access team will check all output again before release.

h) Availability of outputs and publications to NRS

Outputs and publications will be supplied by the researcher to NRS on request for the NRS website or similar use.

3. The process to access **census data for a linkage project**:-

This process is similar to (2) above but more complex in terms of data extraction and the requirement for indexing and linkage. There is also additional documentation because permission for the project must be obtained from at least one other data controller.

a) Application

As (2a) above but permission will also be required from the other data controllers from whom data is required. SPBPP form asks for information about all datasets to be linked. Where there is linkage to Scottish Government data sources, those will be included and assessed in the SPBPP application. Where linkage to PHS data is involved, the researchers must also complete an application for the Health and Social Care Public Benefit and Privacy Panel (HSC-PBPP). All research projects must complete a DPIA that describes the privacy impact of the proposed linkage.

b) Amendment

See (2b) above. Any amendments need to be reviewed and approved by SPBPP and HSC-PBPP where appropriate.

c) Data Sharing Agreement (DSA)

Researchers will need to arrange a DSA for any SG data being linked. For health data, their application and access agreement with HSC-PBPP is deemed to constitute a DSA.

d) Cohort construction, data extraction and indexing

Once all approvals are in place, an ‘Indexing Request Form’ should be submitted by eDRIS to the NRS Indexing team. Indexing will be done by the NRS Indexing as a Trusted Third Party (TTP) service, which will supply study specific identifiers to all participating data controllers for linkage purposes.

If the cohort is defined by census variables, the Data Access team will extract the cohort and prepare a set of unique IDs to be passed to the NRS Indexing team. If the cohort is defined by another data source, the relevant data controller will pass the necessary information to NRS Indexing.

NRS Indexing will then use the cohort IDs and probabilistic linkage via their population spine to create a linkage key for each data source in the linkage project. Data source specific keys will be passed to each data controller, and the master linkage key passed to eDRIS. Each data controller will then extract the relevant cohort from their master data set, adding their linkage key.

e) Data transfer and linkage

See (2e) above for data transfer. The eDRIS linkage agent in the National Safe Haven will link datasets using the master linkage key.

f) Data storage and access for researchers

See (2f) above.

g) Output checking

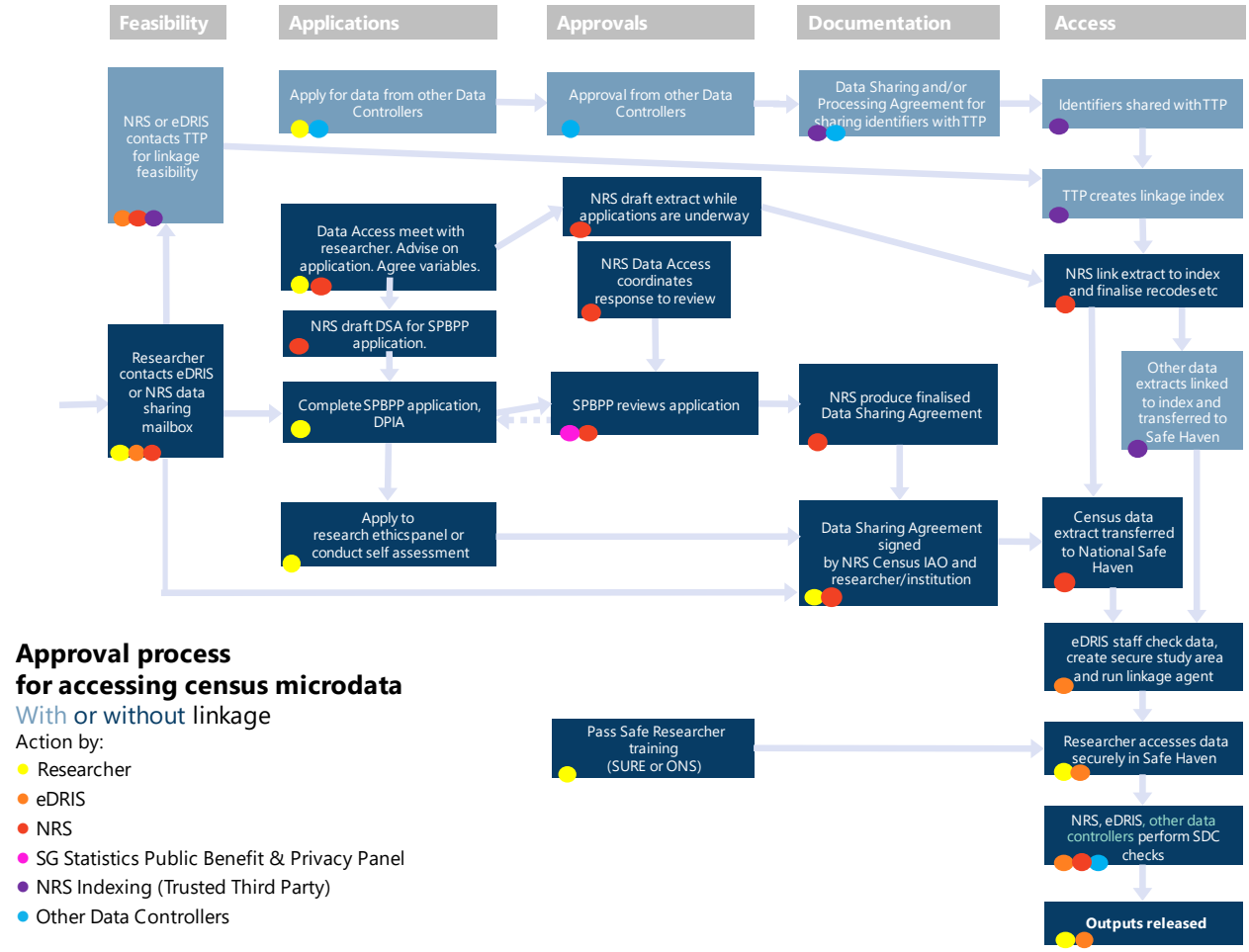
See (2g) above. Another data controller may also have specific requirements for SDC in addition to those in the PHS SDC policy. Any additional requirements will be included in the DSA (see (2c)).

h) Availability of outputs and publications to NRS

See (2h) above.

Step by step process summary

Secure census microdata access process v2



Approval process for accessing census microdata

With or without linkage

Action by:

- Researcher
- eDRIS
- NRS
- SG Statistics Public Benefit & Privacy Panel
- NRS Indexing (Trusted Third Party)
- Other Data Controllers