DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

Version Control

Version	Reason	Date	Author(s)
1.0	**New**	**May 2021**	Sophie Jordan (City of London), Sarah Laws (LB Camden), Lucy Martin(LB Barnet), Alexandra West (LB Redbridge)

Project / Work Stream Name	**Council tax extract data sharing with ONS**	
Project / Work Stream Lead	Name	Mark Stewart
	Designation	Head of Council Tax and Business Rates
	Email	mark.stewart@camden.gov.uk
Overview: **(Summary of the project/work stream)**	For this project ONS will require a monthly extract of Council Tax data from every Local Authority in Great Britain. This extract of the required variables (as detailed below) is taken from the Local Authorities Revenue and Benefit system. For all variables, with the exception of payment details, this is a snapshot from the day of extract.	
Implementation Date:	8 September 2021	

Environmental Scan **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.** *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.*	Checks have been undertaken and this is confirmed as new processing.

Step 1: Complete the Screening Questions			
Q 1	**Category**	**Screening question**	**Yes/No**
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	no
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	no

1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	yes
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	yes
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	yes
Q	**Category**	**Screening question**	
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? See glossary of terms	yes
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	yes
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	yes

1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	yes
1.10	Data	Will the personal data be processed out of the U.K?	no
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	no
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	no
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	no

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.

Step 2: Identify the need for a DPIA										
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??**							New/Changed		
								new		
2.2	**What data will be processed/shared/viewed?**									
	Personal Data									
	Forename	**X**	Surname	**X**	Date of Birth		Age		Gender	
	Address	X	Postal address	X	Employment records		Email address		Postcode	X
	Other unique identifier (*please specify*)		Telephone number		Driving licence number		NHS No		Hospital ID no	
	Other data *(Please state):*		*Details of council tax payments and exemptions and discounts, the full set of fields are contained within the DSA*							
	Special Categories of Personal Data									

Racial or ethnic origin		Political opinion		Religious or philosophical beliefs		
Trade Union membership		Physical or mental health or condition				x
Sexual life or sexual orientation		Social service records		Child protection records		
Sickness forms		Housing records		Tax, benefit or pension records	x	Adoption records
DNA profile		Fingerprints		Biometrics		Genetic data
Proceedings for any offence committed or alleged, or criminal offence record						
Other data *(Please state):*	Physical/mental health records per se are not shared, but some council tax codes will allow inferences about health to be drawn					
Will the dataset include clinical data? (please include)						no
Will the dataset include financial data?						yes
Description of other data processed/shared/viewed?						
N/a						

2.3	**Business sensitive data not in scope**			
	Financial		N/A	
	Local Contract conditions		N/A	
	Operational data		N/A	
	Notes associated with patentable inventions		N/A	
	procurement/tendering information		N/A	
	Customer/supplier information		N/A	
	Decisions impacting:	One or more business function	**Yes/No**	
			N/A	
		Across the organisation	N/A	
	Description of other data processed/shared/viewed (if any).			
	N/A			

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	London Local Authorities	Controller	Yes
	Office of National Statistics	Controller	N/A
3.2	**If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controllers**		Yes/No
			Yes
3.3.	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy, if no, please undertake*		Yes
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** *If yes, provide a copy of the confidentiality agreement or contract?*		No
			N/A

3.5	**Describe in as much detail why this information is being processed/shared/viewed?** *(For example, Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)*
	ONS is aiming to acquire Council Tax data from every local authority in England, Wales and Scotland. This encompasses a monthly snapshot of each Local Authority's Revenue and Benefits system which holds

	information on every property and resident in the respective Local Authority, which is subject to Council Tax. ONS has advised that: "*Council tax data has been identified as an important administrative source for quality assurance of the census. This is due to the level of detail in the data, which will allow ONS to quality check the information collected for census, against information in the Council Tax data, ensuring that the most accurate information is used.* *This will enable the ONS to improve a range of statistics. The data would allow them to produce more accurate local level area population estimates, which would bring improvements to the quality and timeliness of a range of other statistics such as on housing, inequality and poverty. In particular, statistics such as the Consumer Price Index including owner occupiers housing costs (CPIH) would be improved which could have a significant impact on standards of living. These will then inform important changes in policy aimed at reducing poverty and improving people's standard of living. This DPIA covers the ONS acquisition of Council Tax data from every local authority in England, Wales and Scotland.*"
Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?**

	Personal data 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. The authority for ONS to produce, promote and safeguard official statistics is found in the Statistics and Registration Service Act 2007.	**Special Category data** The lawful basis for processing special category data is found in Article 9(2) (g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject Use of Article 9 2(g) requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are: **Statutory etc., and government purposes under Para 6(1)(2)** The authority for ONS to produce, promote and safeguard official statistics is found in the Statistics and Registration Service Act 2007.	
4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	X
		Paper	

4.3	**How will you ensure data quality and data minimisation?**	
Each council is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality. This is part of the ongoing council tax processing. Inaccuracies will be corrected as data is shared in following months. In terms of data minimisation there have been extensive negotiations and discussions between representatives of councils and ONS to ensure that the minimal number of data fields are collected. These will be kept under active review and will be discussed at each review of the Data Sharing Agreement.		
4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to residents on their websites?*	yes
	Privacy notices will be updated before go live as necessary	
4.5	**How will you help to support the rights of individuals?**	
	The council's current processes and procedures will continue to apply to data it holds. In respect of the data to be shared individuals will have the opportunity to opt out of any sharing with ONS by exercising their data subject right of objection. Councils have existing processes to handle these. Once data is received by ONS data subject rights effectively do not apply partly as the data is not held by them in a way that allows individuals to be identified (anonymised or pseudonymised) or is exempt from certain rights due to their processing data for statistical purposes.	

4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?**	
	Each controller remains responsible for their own data subject requests.	
4.7	**Will the processing of data include automated individual decision-making, including profiling?** *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject*	NO
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	NO
	Consent is not the lawful basis for sharing.	
4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the embedded questionnaire.**	The local authorities will not be using cloud based systems, however data may be held on a secure cloud based system by the ONS, who are a separate data controller for this activity
4.10	**Where will the data will be stored** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Council tax data is in existing council tax system. ONS use existing ONS systems. All storage is UK only.	

4.11	**Data Retention Period** *How long will the data be kept?*	
	Council tax data will be retained in accordance with the council's own retention schedule which is based upon council tax law and guidance. ONS inform the council that: "*ONS will keep the data for as long as they continue to be used to produce statistics and undertake research. The retention of the Council tax data until ONS no longer requires it to fulfil our statutory function aligns with the Information Commissioner's Office guidance on GDPR retention for statistical purposes. Further details can be found on the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/. ONS need for the council tax data will be kept under constant review and once it is determined the data are no longer required, they will be destroyed in line with HM Government security guidelines and with relevant data protection legislation*." Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.	
4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No No
Step 5: Information Security Process		

5.1	**Is there an ability to audit access to the information?**	Yes/No
	ONS and Council tax systems have auditable RBAC.	Yes
5.2	**How will access to information be controlled?**	
	RBAC is required with password access as minimum. This will be dependent on local policies in each council and ONS which must meet best practice guidelines and UK GDPR/DPA18	
5.3	**What roles will have access to the information?** (list individuals or staff groups)	
This will be dependent on local policies in each council and ONS which must meet best practice guidelines and UK GDPR/DPA18		

5.4	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**					
	Username and password	X	Smartcard		key to locked filing cabinet/room	
	Secure 1x Token Access		Restricted access to Network Files			x
	Other: *Provide a Description Below*:					

	This will be dependent on local policies in each council and ONS which must meet best practice guidelines and UK GDPR/DPA18		
5.5	**Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:** SLSP is required for new systems. *SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.*	Yes/No	
		Not required	
5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?** *Please explain and give reference to such plan and protocol*	Yes/No	
		No BCP needed for this project as covered by existing BCP for council tax systems	
5.7	**Is Mandatory Staff Training in place for the following?**	Yes/No	Dates
	• Data Collection:	Yes	Continuous
	• Use of the System or Service:	Yes	Continuous
	• Information Governance:	Yes	Continuous
5.8	**Are there any new or additional reporting requirements for this project?**	No	

	• What roles will be able to run reports?	
	N/A	
	• What roles will receive the report or where will it be published?	
	N/a	
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?	
	N/A	
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
	N/A	
5.9	**Have any Information Governance risks been identified relating to this project?** (if Yes the final section will need to be completed)	**Yes/No** Yes

Step 6: Identify and Assess Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Note: risks here are risks of this sharing ONLY. Signatories should have DPIAs for their own individual systems and methods, covering their local risks.			
Loss of data in transfer; Personal data could be obtained by third parties and misused. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Significant	Medium
Loss of data in situ; Personal data could be obtained and misused by malicious parties within the organisation. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Unlikely	Severe	Medium
Misuse of data; Personal data could be used in a manner incompatible with the Data Sharing Agreement. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Minimal	Low

Theft of data; Personal data could be stolen and misused by a malicious third party. Compliance risk; Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Unlikely	Severe	Medium
Further transfer of data; Risk to the safety of personal data if transferred elsewhere. Compliance risk; Personal data shall be obtained for one or more specified and lawful purposes. Appropriate technical and organisational measures shall be taken. Personal data shall not be transferred outside the European Economic Area. Corporate risk; Reputational risk. Loss of trust.	Unlikely	Significant	Low
Disposal of data; If personal data is not disposed of in an appropriate manner, it may be possible for third parties to obtain the data. Compliance risk; Personal data shall not be kept for longer than necessary. Appropriate technical and organisational measures shall be taken. Corporate risk; Reputational risk. Loss of trust. Legal implications.	Possible	Significant	Medium

Inherent privacy intrusion from sharing large quantities of personal information with a third party where the rights to cease processing by the third party are truncated. The purposes for processing provided by ONS have a degree of opacity meaning that data subjects may not be able to ascertain why the data is being processed.	High	Medium/high	Medium/high
Data Retention: Risks that ONS will retain data beyond a defined period given their DPIA and DSA do not give an end date.	High	Medium/high	Medium/high

Step 7: Identify Measures to reduce risk

Identify likely additional measures to reduce or eliminate risks identified as medium or high risk in step 6

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Loss of data in transfer	Council data will be transferred using an agreed, secure, electronic transfer facility which adheres to Government requirements and assurance. ONS will offer to provide each Local Authority with a MoveIT account. MoveIT is a GDPR - compliant solution, the system is hosted on secure LISTX premises and uses data in transit protection and at rest encryption, it is separate from other customers infrastructure and is entirely located within the UK.	Reduced	Low	Yes

	The data transfer from the MoveIT accounts into ONS will be overseen by ONS personnel who have undergone the relevant training, security vetting and are aware of their obligations under Data Protection legislation and Section 39 SRSA 2007. Within MoveIT, the data is anticipated to be dropped into the created folder for each authority within their password protected account. This enables the automatic ingestion utilising SFTP.			
Loss of data in situ	The physical and technical security of the data will be maintained at all times. ONS operate an assured analysis environment that includes the following elements of security control: • Access to high sensitivity data requires appropriate staff security clearance and authorisation by the Information Asset Owner on a case-by-case basis following an ethical assessment and provision of a valid business case. • "Need To Know" is applied with controlled account access using unique credentials based on job role. • User activity is logged and monitored, with operational support processes in place to aid secure data management.	Reduced	Low	yes

	• Logged access of user activity within the environment • Secure build configuration for infrastructure, including Cloud services. • Data from the 380 Local Authorities is received in a format based on their choice but typically being an industry standard or NCSC recommended method. ONS preferred method of transfer is MoveIt, with ONS holding a license and we would set up the user accounts for each authority. As Moveit is a web-browser based portal, there is no need to download anything onto Authority systems. Once accounts have been set-up ONS will send emails with passwords and instructions to those email addresses supplied by the Authority. • Data, as received by each Local Authority, will be stored within the ONS assured environment, with appropriate security controls applied based on its sensitivity and classification. • Vulnerability tested infrastructure with appropriate remediation and patching. • Compliance checks against security enforcing controls are performed by an internal information security audit function. ONS is aligned to the HMG Security Policy Framework			

	and operated a baseline control set that aligns fully with ISO27001. • Architectural review against recognised standards from within Government (Cabinet Office, NCSC, CPNI) and international best practice (ISO 27001, NIST, ISF). GDS Digital Standards are utilised for all new projects or systems acquisition. • Staff security cleared to the appropriate level based on their supervised and/or unsupervised access to sensitive data in accordance with ONS clearance policies and data access processes. • Education and awareness of environment users covering security policies and secure working practices. • Operational support processes to securely manage the environment. • Risk assessment to identify security risks and mitigation actions to reduce this risk. User access to Council Tax data is through ONS standard laptops or desktops connecting to the ONS network that then connect to a separate virtual desktop infrastructure, logically within the ONS boundary, through a controlled channel that does not provide for any network connection or data transfer outside the environment.			

	ONS premises are secured to Government standards. All ONS sites are UK-based (London, Titchfield and Newport). Site access is controlled and audited supported through regular reviews of technical, procedural and CCTV records.			
Misuse of data/ Theft of data	ONS ensure that their staff, including any contractors, understand and guarantee to maintain the confidentiality requirements of this data supply and will ensure that ONS employees involved with the processing of this data supply, have undergone staff training and appropriate security vetting and are working according to established Security Operating Procedures (SyOPs). In summary, the security controls in place include: • physical – the data are held, and all research using them takes place within a cloud-based, virtual desktop infrastructure segregated from the ONS organisational network with dedicated separate accounts for user and IT management access. Only authorised and security cleared ONS researchers are permitted to access the data, and all access is recorded, monitored and audited by ONS Security and Information Management on a regular basis, through regular review of technical and procedural records.	Reduced	Low	Yes

	• procedural – the data acquisition, import, linking and export processes are subject to strict procedural controls. When linked, data will be used for statistical and statistical research purposes only. • personnel – access to data is managed on a need to know basis. Individuals are only given access to what they require for their business purposes. Staff undergo a national vetting clearance process if they have a business need to access sensitive data.			
Further transfer of data	Any ONS publication or output using Council Tax data undergoes an appropriate level of disclosure control to ensure that the identity of individuals or businesses cannot be deduced, either by being specified in the output, deduced from the output, or can be deduced from the output taken together with any other published outputs. No identifiable council tax data will be shared outside of ONS without prior consent of Local Authorities and the updating of this DPIA accordingly. Aggregate information will meet our statistical disclosure control guidelines. Council Tax data will not be transferred outside of GB.	Eliminated	Low	yes

Disposal of data	Specific business and technical processes have been developed to delete data and validate that this has been performed without the prospect of recovery. These cover the deletion of raw data, working files and derived data. Data deletion is confirmed by the Security Manager and is signed off by the Information Asset Owner for the data, and evidence of deletion is provided to the data supplier where necessary	Reduced	Low	Yes
ONS retention beyond stated period	Regular review of the DSA and what is shared and its necessity and proportionality to reduce what is shard and therefore retained. Once shared with ONS they process data under legal basis around statistics and research and retention is controlled by them with many safeguards around retention not applying. As a data controller this is their responsibility and not a risk that councils can control.	Unchanged	Medium/high	Accepted
Inherent privacy intrusion	Training and appropriate policy. Data minimisation, sharing only what is needed. Knowledge of DSA/ISA and its limits. Regular review of the DSA and what is shared and its necessity and proportionality. Regular review of privacy notices and that appropriate notification is given to data subjects.	Reduced	Medium	Yes

Overall residual risk level: Medium

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:	Mark Stewart, Head of Council Tax and Business Rates 7 September 2021	
Residual risks approved by:	Mark Stewart, Head of Council Tax and Business Rates 7 September 2021	
DPO advice provided:	Lucy Martin(LB Barnet), Alexandra West (LB Redbridge), Sophie Jordan (City of London), Sarah Laws (LB Camden)	

Summary of DPO advice for each council (Note that local DPOs for each organisation need to produce their own DPIAs, or consciously adopt this suggested DPIA). I have carefully considered this form and the underlying facts. I am happy that this is an acceptable and proportionate use of the data for proper purposes. Andrew Maughan DPO		
DPO advice accepted or overruled by:	N/A	If overruled, you must explain your reasons
Comments: N/A		
Consultation responses		If your decision departs from individuals' views, you must explain your reasons

reviewed by:		
Comments:		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA

Glossary of terms

1. 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. 'Special Categories of Personal Data' mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
3. 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, '
4. 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
5. 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

6. ‘Data Subject’ – an individual who is the subject of personal information.
7. Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.
8. ‘Pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
9. ‘Anonymised Data’ - means data in a form where the identity of the individual cannot be recognised i.e. when:
    - Reference to any data item that could lead to an individual being identified has been removed;
    - The data cannot be combined with any data sources held by a Partner with access to it to produce personal data.