

DPIA - Ealing council and HMRC Digital Economy Act Data Sharing Pilot.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves for Council Tax data. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Ealing council has a strategic objective to improve the council tax collection rate.

For 2017/18, Ealing council issued approx. 134,000 bills (at annual billing) to resident households demanding £156M council tax in year, with an average collection rate of 97.34% in year (national average is 97.1%). Debt remaining for the 2017/2018 financial year was at £4.15M.

Within 2017/18 Ealing council obtained 17,583 Liability Orders at the Magistrates Court (inclusive of multi/prior years), of which over 68% of these liability orders were eventually passed to Enforcement Agents, with only just over 1% resulting in Attachment of Earnings (AoE) - a process where direct deductions are made from salary at a percentage set by Local Government Finance Act 1992 (LGFA 1992).

Ealing council have identified that sharing council tax debt data with Her Majesty's Revenues and Customs (HMRC) to obtain PAYE and self-assessment information could support:-

- managing overall council tax arrears and further developing its recovery procedures, by analysing the employment and income information of individuals provided by HMRC to:-
 - identify customers whose circumstances make them vulnerable and providing appropriate support;
 - contact customers identified as having a propensity to pay and offering them the opportunity to pay, and ;
 - For those that still do not engage and are in employment, recovering individual council tax debts by Attachment to Earnings Orders
 - overall reducing use of Enforcement Agents and associated costs to customers (approx £75.00 per customer at compliance stage, with additional £235.00 if enforcement necessary)

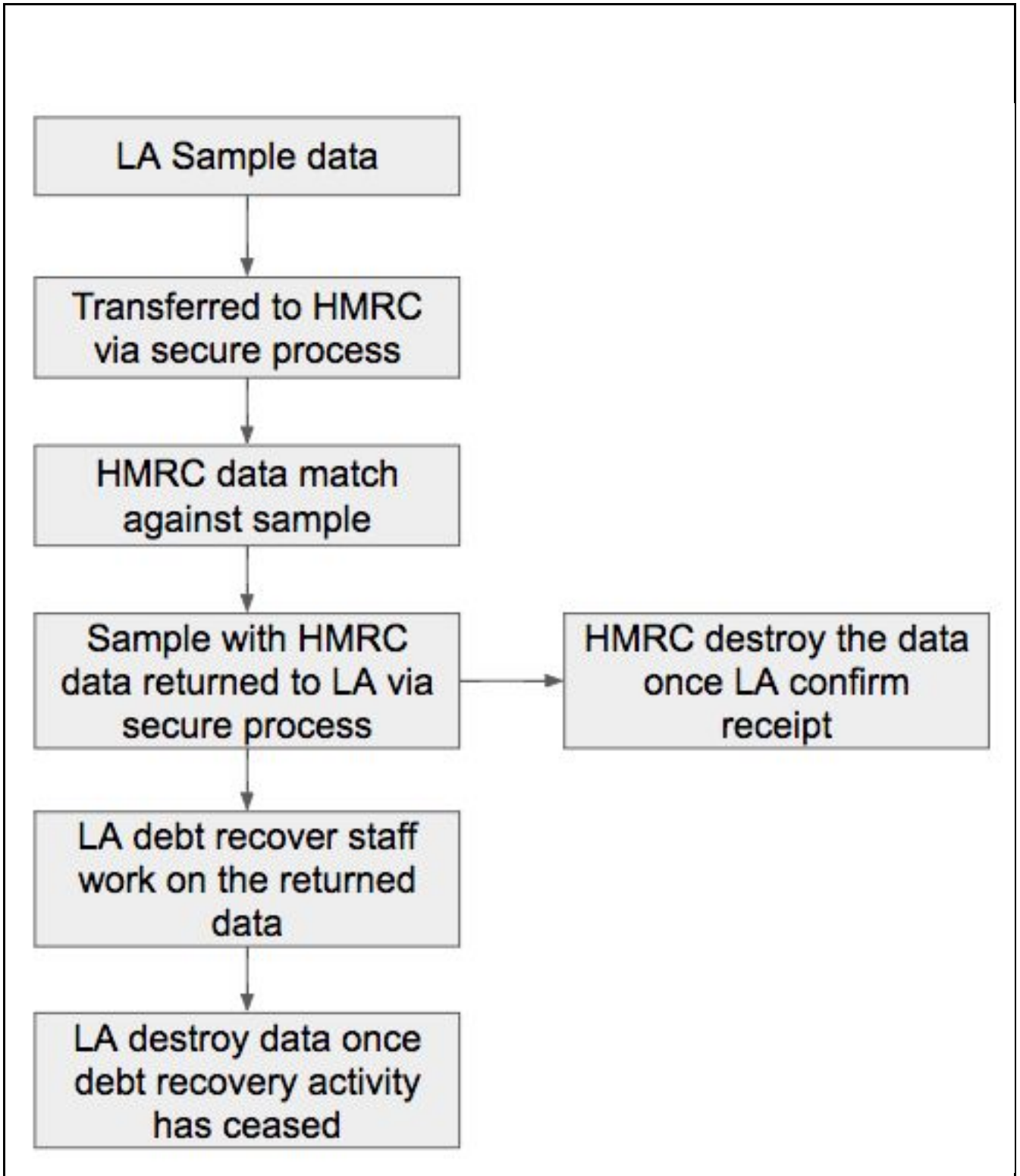
Ealing council and Her Majesty's Revenues and Customs are both joint data controllers.

The purpose of the pilot is to gather evidence that the data shared from HMRC will increase Ealing council's council tax recovery rate.

The DPIA is needed as we will be collecting new information from HMRC to enable council tax to enable recovery which may have a significant impact on the individuals concerned, for example:-

- Financially vulnerable individuals may be identified and offered debt support
- AoE's may be implemented where the individual will have no choice regarding payment of the debt.
- Individuals may be contacted to discuss the new information provided by the HMRC

This may also raise privacy concerns as this data was originally collected for the purposes of calculating income tax liability.



Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Ealing council will supply to HMRC, account numbers, customer names, addresses and Liability Order dates for a sample of up to 4,000 Ealing council customers, who are subject to Liability Orders. The data will be supplied via the Digital Gateway through TLS- potentially via an Egress passworded file. HMRC will match against HMRC data and matching cases will be supplied to Ealing council with PAYE and self-assessment data. The file will be through the Digital Gateway through TLS- potentially via an Egress passworded file.

The additional data from HMRC will be:

- Employer Name(s)
- Employer Address(es)
- Debtor Income (if under £300.00 net earnings attachment not applicable – national rates)
- If Self-Employed if no PAYE data

HMRC turnaround check must be quick for data accuracy, to ensure the data supplied by Ealing remains contemporary, namely the debtor is in arrears as at file transfer. That said checks by Ealing Local Taxation officers will be carried out prior to the actioning of any attachment of earnings to verify Liability Order debt remains outstanding.

The data will be used to enable management and recovery council tax debt, via:-

- Where financial vulnerability is identified, discussions around the use of debt support
- AOE where employment information has been provided
- Further discussion with the individual where self-assessment information has been provided

Officers in the Local Taxation Back Office will review the HMRC file and look at the accounts stated and see if the Liability Order arrears are still owed. If so then attachment from earnings will be requested and on the weekly creation of the document then a further check will be carried prior to dispatching of documents to both the debtor and employer.

As employment data is held for the purpose of recovery of the statutory owed Council Tax then this data is retained on accounts until such time it is clear the

employment has changed. Therefore further attachment of earnings can be made against Liability Orders subsequent to those stated within the HMRC file.

The data will be stored in secure folder within Ealing council. For

HMRC will destroy their data once Ealing council have confirmed receipt.

HMRC will destroy the records supplied by Ealing council after processing and return to Ealing council and confirmation of receipt by Ealing council. Data to be destroyed within the ICT procedural timeframe.

The council will not retain any unprocessed data relating to the project once the pilot has completed. Unprocessed data will be employment data unused due to all Liability Order debts having been paid subsequent to file transfer.

Information processed through Council's revenues and benefits systems will be retained in line with Ealing council's local data retention policies relating to the billing and processing of Council Tax.

The standard data retention period for the pilot is one year. However, data that is being used operationally to recover debt, e.g. via an Attachment of Earnings, bankruptcy action or supporting identified vulnerable customers will be retained in line with local Council Tax data retention policies for each pilot authority and deleted in accordance with said policies.

The data will be held for one year on the transferred file by Ealing, for verification and accuracy purposes, in case of query from the customer/employer. The file will be destroyed by the Ealing ICT Team in line with their procedures.

The data will not be shared with anyone else.

Those with full view and update access to the Northgate system are:

- Local Taxation Back Office Staff
- Customer Services Contact Centre Staff

Those with full view access to the Northgate system are:

- Housing Benefit Staff
- Local Welfare Staff

Other Sections with View Access to Northgate i.e. Social Services and Regulatory Services will be have Recovery Parts restricted from view which includes employment data

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is customer name, address and liability order date from Ealing council and for matching records and if applicable, PAYE and self-assessment information from HMRC.

There are no special categories or criminal offence data.

A sample of up to 4,000 records will be collected and used.

This is a one off pilot to inform the next phase. For the next phase a new DPIA will be required.

Up to 4,000 individuals may be affected

The geographical area covers Ealing council boundary.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The individuals reside within the Ealing council boundary or did reside at the time of liability and are liable to pay council tax to Ealing council and have not paid.

The individuals will have no control as the legal basis for processing is statutory obligation and not consent. Specific referral is made to the Local Government Act 1992, statutory Instrument 613 Regulation 37.

Council tax is covered by the Local Government Finance Act 1992 and individuals are required to pay their council tax and would expect Ealing council to pursue recovery of their debt.

Data will only be requested for those who have proven liability. The data received from HMRC may identify customers who could be deemed vulnerable which will enable Ealing council to assist them (i.e. Benefit assessment, Local Welfare Assistance, Social Services) and also by signposting to third sector agencies i.e. StepChange.

There are no prior concerns over this type of processing and security flaws.

It is novel in that this is the first piloted use of data in this manner; however, the use of data sharing to manage and reduce debt is well established throughout the debt industry.

There is no new technology in this area for this type of pilot.

There are no issues of public concern to be factored in.

Ealing council and HMRC are required to adhere to the DEA Code of Practice, DPA 2018 and LGFA 1992 (as amended).

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The pilot is aimed at:-

Increasing recovery of council tax debt from individuals who have not paid and debt support for those individuals identified as financially vulnerable.

The intended effect on individuals will be to for those who are able to pay and choose not to pay is to manage and recover their debt. For those who are identified as vulnerable, the effect will be to help them via debt support. It will also be fairer for those who do pay their council tax.

The benefits of the processing are:-

- Identified financially vulnerable debtors can be signposted for assistance within or without the council.
- Increase in Council Tax debt recovered
- Increase take up of reliable Attachment of Earnings,
- Increase in debt recovery due to knowledge of customers self-assessment information
- Reduce failure rate of Attachment of Earnings,
- Reduce need for using enforcement agents as a first port of call and increasing debt with fees.
- A fairer approach to reducing debt with ability to pay over a regular period.
- Improve our effectiveness in debt recovery reduces pressure on budgets
- Those in regular employment will avoid expensive and stressful enforcement agent visits.
- Customers knowing that we have access to HMRC data will encourage earlier take up in contacting us and making arrangements to pay.
- Efficiency savings by reducing time/court hearings on committal or insolvency cases.
- Efficiency savings on not transferring cases to enforcement agents.
- Swifter repayment of debt to the council

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Individuals views will not be sought for this pilot, the council already has the power to request employment details from individuals when a liability order has been obtained under Regulation 36 of the Council Tax (Administration & Enforcement) Regulations 1992 and employment details are already held in many cases where an attachment of earnings order has been served. Consultation is not therefore necessary on this occasion.

Additionally the Digital Economy Act 2017 has undergone a public consultation process.

Within Ealing council, the DPO, SIRO, senior decision makers, Local Taxation Recovery Manager. and Customer Services Contact Centre staff need to be involved.

Local Taxation Back Office staff will be asked to assist.

Security, data protection and analyst experts will be involved and consulted.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The statutory gateway is:-

- Local Government Finance Act 1992
- Digital Economy Act 2017, part 5, Chapter 3.

The lawful basis for processing is the:-

Performance of a task carried out in the public interest or in the execution of official authority vested in the controller

The processing will achieve the purpose and there is no other way of obtaining the same outcome.

The pilot will adhere to the DEA Code of Practice, DPA 2018 and LGFA 1992 and the project aim and processing will prevent function creep. Function creep is not applicable as consent is not required.

Data minimisation is achieved by adhering to the LGFA 1992, in that only the information supplied by the individual can be supplied to HMRC. The information in the file to HMRC are:

- Account Number
- Full Name,
- Property Address,
- Contact Address (if now outside borough)
- Liability Order Date

Data quality will be achieved by in-house processing by HMRC to ensure only matched individual data is returned to Ealing council that reaches HMRC matching criteria. HMRC will ensure:

- A quick turnaround of data
- Flag data not matched due to uncertainty due to name comparison
- A summary of the data match criteria used in comparing to tax records

Information given to the individual will take the form of signposting to the Council Tax Privacy Notice outlining the potential uses that may be made of their data for the purposes of Council Tax collection and in the event of non-payment. The Privacy Notice will also include details, or reference to details, of how to exercise data subject rights under the legislation. The Privacy Notice will be on the Ealing website and will state that potential sharing of Council Tax data to third parties including HMRC.

Information given to individual as a consequence of the matching activity will depend on the match data returned by HMRC, and for those with:-

- PAYE data supplied, they will be informed that an AoE will commence
- Self-assessment data, they will be informed by letter or phone conversation.
- For those identified as financially vulnerable they will be helped by debt support

Ealing council will apply it's fairness principles to the pilot.

All staff involved in the pilot have been suitable trained and have signed relevant data security policies.

Data will not be sent outside the UK.

Step 5: 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
<p>Source of Risk: Non-compliance with Principle A (Lawfulness, Fairness and Transparency) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018. Data not used for the purpose of the Local Government Act 1992 Statutory Instrument 613 Regulations 37 to 43. Data not used for the intention of the Digital Economy Act 2017, Part 5.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> • The data subjects will feel deceived or misled when they realised that their personal data is shared with HMRC without their knowledge • Payment not received towards debtor’s arrears <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage. HMRC will close the Digital Gateway for bulk employer information. Compromising national sharing agreements with Billing Authorities,</p>	Likely	Low	Low
<p>Source of Risk: Non-compliance with Principle B (Purpose Limitation) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Potential Impact on Data Subject</p> <ul style="list-style-type: none"> • Lack of trust by the members of the public especially the data subjects. 	Probable	Medium	Medium

<ul style="list-style-type: none"> Public distrust about how information is used can damage the council's reputation HMRC will not supply data under an agreement <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>			
<p>Source of Risk: Non-compliance with Principle C (Data Minimisation) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> Decisions are made about the data subject based on an incomplete understanding of the facts and the most suitable recovery path is missed Data which then held is unnecessary <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	Probable	High	High
<p>Source of Risk: Non-compliance with Principle D (Data Accuracy) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> Financial loss Vulnerability not identified Delay in payment plan and continued arrears <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	Probable	High	High

<p>Source of Risk: Non-compliance with Principle E (Data Storage) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> • Dispute over data as old information held • Supply of data not efficiently made on request <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>Probable</p>	<p>High</p>	<p>High</p>
<p>Source of Risk: Non-compliance with Principle F (Data Security – Confidentiality & Integrity) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Not having appropriate security control measures (physical, procedural and technical) in place to protect the personal data in transit and at rest.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> • Data comes into unauthorized possession • Vulnerability not identified due to invalid data • Not able to access Ealing processes and procedures <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	<p>Probable</p>	<p>High</p>	<p>High</p>

<p>Source of Risk: Non-compliance with Chapter 3 Article 12 – 23 (Rights of the data subject) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> • Supply of data not efficiently actioned on request • Data held is shown to be unnecessary <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	Probable	High	High
<p>Source of Risk: Non-compliance with Chapter 3 Article 12 – 23 Principle A (Restricted Transfer) of the EU General Data Protection Regulations 2016 and UK Data Protection Act 2018.</p> <p>Transferring of personal/special category data outside the protection of the GDPR</p> <p>Potential Impact on Data Subject:</p> <ul style="list-style-type: none"> • Fraud and misuse of data national and internationally • No or difficult legal remedy <p>Compliance and corporate risk: Non-compliance with the GDPR/DPA or other legislation can lead to sanctions, fines and reputational damage.</p>	Occasional	High	High

Step 6: Identify measures to reduce risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk - Eliminate, Reduce or Accept	Residual risk – Low, Medium or High	Measure approved Yes or No
Lack of or use of inappropriate legal basis for sharing the data with HMRC.	Lawful basis already identified – Legal Obligation under Local Government Finance Act 1992 and Digital Economy Act 2017	Reduce	Low	Yes
Data subjects not aware that their data is shared with HMRC and Employer	The Council Tax Privacy Notice to be updated/created.	Reduce	Low	Yes
Not sure of the purpose(s) for collecting the data at onset.	Already established the purpose which is embedded in the lawful basis – collection of Council Tax Debt	Reduce	Low	Yes
The new purpose for sharing the data with HMRC is not compatible with the original purpose(s) for collecting the data	The lawful basis for sharing and processing the data from HMRC and the employer is compatible with the statutory obligation to collect Council Tax from people in London Borough of Ealing	Reduce	Low	Yes
Not updating the privacy notice with	The Council Tax Privacy Notice will be updated by incorporating the sharing	Reduce	Low	Yes

the new purpose(s).	with HMRC and the employer.			
Non-compliance with documentation and transparency obligations to specify purpose(s).	The Council Tax Privacy Notice will be updated by incorporating the sharing data with HMRC and the employer.	Reduce	Low	Yes
Transferring insufficient or more data (to HMRC or employer) than it is necessary to fulfill the purpose(s) for processing.	<p>Agree standard file format based on a national standard with Ealing's identifier in the title.</p> <p>Agree spreadsheet style csv or excel</p> <p>Joint controller agreement is signed for clarity of the data required and to be transferred within the digital gateway.</p> <p>Agree most efficient secure file transfer between HMRC and Ealing and modify as appropriate during pilot.</p>	Reduce	Low	Yes
Software Update and Security	<p>ICT to updates software for file transfers with HMRC</p> <p>Ealing Network to up software as providers advise</p> <p>Northgate to be upgraded as notified by supplier</p>	Reduce	Low	Yes

<p>Some of the personal data shared with HMRC is incorrect or misleading. HMRC provide misleading or incorrect data</p>	<p>Act on incorrect deductions by requesting a stop of attachment of earnings and refund payments. Attachment from earnings made against wrong liable party leading to financial loss. Accept HMRC data on income but make an indicator on Northgate where information from in event of employer providing contrary data concerning low income (sign-post to assistance) or is self-employed. Be clear in date whether PAYE or self-employed.</p>	<p>Reduce</p>	<p>Low</p>	<p>Yes</p>
<p>Keeping the information longer than it is necessary</p>	<p>Compliance with data retention periods that apply to service HMRC to confirm their deletion of files or storage after each file transfer Retention of HMRC data file is only for a year (for query purposes) or up to when the pilot has completed. Ealing standard of file destruction used. Agree with ICT a secure data storage area Keep the employment data on Northgate in line with statutory retention</p>	<p>Reduce</p>	<p>Low</p>	<p>Yes</p>
<p>Manual Transfer of HMRC employment</p>	<p>Training and testing is carried out and clear understanding of the data extracted via HMRC and</p>	<p>Reduce</p>	<p>Low</p>	<p>Yes</p>

data to Northgate personal accounts	where it is placed on Northgate Council Tax software.			
Inappropriate, unauthorized or accidental disclosure of data.	Restrict access to data through system usernames/ passwords GDPR training delivered to all existing staff and incorporated in induction procedures for new staff provided.	Reduce	Low	Yes
Inappropriate or unauthorized access to data.	Restrict access to data through system usernames/ passwords GDPR training delivered to all existing staff and incorporated in induction procedures for new staff provided.	Reduce	Low	Yes
Loss or damage to data at rest and in transit.	Agree with HMRC receipt and transfer protocols. Test with quasi data prior to pilot real-world. Data file not transferred to right authority due to inaccurate header/title	Reduce	Low	Yes
Inability to make accurate decision for potential payment or vulnerable assessment	Agree with HMRC the data content, inclusive of income, and in the agreement the comparison match process used.	Reduce	Low	Yes

Unauthorised modification of data	Agree the communication lines, who are the specified person/teams up to file going to Local Taxation Team for manual entry	Reduce	Low	Yes
Unavailability of data to the authorised user when it is needed. Data availability only to those authorised	Check the authorised users have access such as members in Local Taxation, Housing Benefit, Investigation and Audit and Customer Services. Those with view access should have restricted access. When unavailable ensure recovery processes and rollbacks procedure are in place for Newtwork and Northgate	Reduce	Low	Yes
Inability to meet data subject right requests within the timeframe.	Agree protocol between Local Taxation office and Ealing ICT of where data is stored for ease of access. Staff trained as to where employment details are stored on Northgate accounts	Reduce	Low	Yes
A transfer of personal data outside the protection of the GDPR/DPA	Not transferring data outside EEA Attachment requests can be made on individual accounts to companies registered abroad	Reduce	Low	Yes


Step 7: Sign off and record outcomes

Item	Name/date	Notes
------	-----------	-------

Measures approved by:	[REDACTED]	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	[REDACTED]	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Official Sensitive

Signature



Head of Service.

Impact/Consequences/Severity		Likelihood/Probability		Risk	
Category	Description	Category	Description	Category	
1	Insignificant/Trivial	1	Rare	1	Minimum
2	Minor	2	Unlikely	2	Low
3	Significant/Moderate	3	Possible	3	Medium/Moderate
4	Major	4	Likely	4	High
5	Severe/Critical	5	Very Likely/Almost Certain	5	Extreme

Impact	Description
1. Insignificant/Trivial	<ul style="list-style-type: none"> • Insignificant impact to the service • Unauthorised access to, loss or damage to ordinary personal data of up to 10 living individuals, cost impact £0 to £25,000
2. Minor	<ul style="list-style-type: none"> • Minor impact to the service or XYZ • Localised decrease in perception within service area – limited local media attention, short term recovery • Unauthorised access to, loss or damage to ordinary personal data of 11-999 individuals, cost impact £25,001 to £100,000
3. Significant/Moderate	<ul style="list-style-type: none"> • Moderate impact to the service or • Decrease in perception of public standing at local level – media attention highlights failure and is front page news, short to medium term recovery • Unauthorised access to, loss or damage to sensitive data of 11-999 individuals, cost impact £100,001 to £400,000
4. Major	<ul style="list-style-type: none"> • Major impact to the service • Decrease in perception of public standing at regional level – regional media coverage, medium term recovery from incident

	<ul style="list-style-type: none"> • Unauthorised access to, loss or damage of sensitive data to over 1000 individuals, cost £400,001 to £800,000
5. Severe/Critical	<ul style="list-style-type: none"> • Catastrophic impact to the service • Decrease in perception of public standing nationally and by the Government – national media coverage, long term recovery from incident • Significant long-term damage or distress to large numbers of people, cost £400,001 to £800,000.

Descriptor	Likelihood Guide
1. Improbable/Rare	<ul style="list-style-type: none"> • Virtually impossible to occur 0 to 5% chance of occurrence.
2. Unlikely/Remote possibility	<ul style="list-style-type: none"> • Very unlikely to occur 6 to 20% chance of occurrence
3. Possible	<ul style="list-style-type: none"> • Likely to occur 21 to 50% chance of occurrence
4. Likely/ Probable	<ul style="list-style-type: none"> • More likely to occur than not 51% to 80% chance of occurrence
5. Very Likely	<ul style="list-style-type: none"> • Almost certain to occur 81% to 100% chance of occurrence