NORTH HERTFORDSHIRE DISTRICT COUNCIL

Data Privacy Impact Assessment ('DPIA')

Data Protection Impact Assessments (DPIAs) are a legal requirement *in certain circumstances*. You are required to carry out a DPIA for every processing operation which is "***likely to result in a high risk***". The DPIA should be carried out "prior to processing". Consider whether you need to do this as part of any new project and/ or procurement. Further guidance can be obtained from information management, Legal, the Data Protection Officer or via the ICO website.[1]

Remember this checklist before completing the DPIA:

- You will need to describe the nature, scope, context and purposes of the processing.
- Ask any data processors to help complete the DPIA for any joint processing activities.
- If a DPIA is necessary, consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- The advice of the Data Protection Officer must be sought.
- Check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- Assess the likelihood and severity of any risks to individuals' rights and interests.
- Identify measures we can put in place to eliminate or reduce high risks.
- Record the outcome of the DPIA, *including any difference of opinion of the DPO* or individuals consulted.
- Implement any measures identified, and integrate them into a project plan and, if relevant, the data protection clauses in any contract.
- Consult the ICO before processing *if we cannot mitigate high risks*.
- Keep any DPIA under review and revisit it/ amend it if necessary.

STEP ONE: Identify the need for a DPIA

Explain what the project aims to achieve and what processing it involves. You may find it helpful to link to other relevant documents related to the project, for example a project proposal.
Also summarise why you identified the need for a DPIA.

The aim of this project is to obtain employment, self-employment and income details from Her Majesty's Revenue and Customs (HMRC) to enable the efficient collection of council tax debt, using the least punitive method of recovery available to it.

In cases of non-payment, after obtaining a liability order at the magistrates' court the council has a number of options for recovering the debt including: attachment of earnings or benefits, removal of goods by enforcement agents (bailiffs), insolvency, charging order or committal to prison, depending on customer circumstances and information the customer has provided.

Further details can be found in the business case that has been prepared for the Cabinet Office

The DPIA is needed as we will be collecting new information from HMRC to enable council tax to be taken by deduction from debtors earnings which will have a significant impact on the individuals concerned (albeit a lesser impact than the alternatives) as they will have no choice regarding payment of the debt. This may also raise privacy concerns as this data was originally collected for the purposes of calculating income tax liability.

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

STEP TWO: Describe 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 another way of describing data flows. What types of processing identified as likely high risk are involved?

A sample of up to 4000 customers who are subject to Liability Orders will be cross referenced against HMRC data and matching cases will be supplied with employment, self employment and income details. This information will be sent directly to HMRC via encrypted email (TLS) by the individual Authorities who are active in the pilot.

Where employment details are received, and income is at a legislated level to enable an attachment to earnings, the council will contact the employer and require them to make deductions from their employee's earnings at the rate prescribed in the Council Tax (Administration and Enforcement) Regulations 1992 until the debt is cleared.

Where self-employment and income data has been supplied, further communication with the customer may be made with a view to arranging repayment.

Data supplied by NHDC will not be retained by HMRC once they receive confirmation that their appended data has been received.

The data will be held until six years after the debt has been cleared, in accordance with the Council's retention schedule.

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 data collected will consist of employment details in relation to customers who have unpaid Council Tax and where the debt has already been through the court process and a Liability Order obtained. Currently the Council has a number of unpaid debts at Liability Order stage, which have potentially exhausted the methods of recovery action, barring committal action, which is costly and resource hungry. The debts relate to all areas within the district.
The data collected will be based on the employment details held by HMRC.

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)?

This exercise will include all groups within the NHDC area, but information gathered will not be used in every case, for instance in cases where income is particularly low; but this will give the Council the opportunity to be able to filter out those that may be potentially vulnerable.
Customers will have a degree of control if they contact the Council, we do have the power to 'cap' the attachment level if customers genuinely cannot afford the percentage deduction contained within the legislation, but they have no control over the method of recovery as this is an available method of recovering unpaid Council Tax.

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 aim of this project is to collect unpaid Council Tax using attachment of earnings.
The Cabinet Office and HMRC are using The Digital Economy Act to ultimately enable Council's to ascertain information held by another Government body – if the project is successful, the intention is to attempt to change primary legislation.
The Council has duty to collect unpaid Council Tax for the benefit of those tax payers that do pay in a timely manner.

STEP THREE: Consultation requirements/ 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?

By completing this DPIA we will identify and address all privacy risks

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 previously been served. Consultation is not therefore necessary on this occasion.

The DEA has undergone a public consultation process.

The pilot will adhere to the DEA Code of Practice, Data protection 2018 and the Local Government Finance Act 1992 and the project aim and processing will prevent function creep.

Data Protection Act 2018, Schedule 2, Part 2(1).

STEP FOUR: 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?

STEP FIVE: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include	**Likelihood of harm** (Remote,	**Severity of harm**	**Overall risk** (Low, medium

associated compliance and corporate risks as necessary.	possible or probable)	(Minimal, significant or severe)	or high)
1. Data is shared with other sections or organisations for which there is no authorisation or legal justification	Remote		Low
2. The data being collected may be considered sensitive as it shows employment details including levels of earnings, self employment and income	Remote		Low
3. Data concerning vulnerable customers may be divulged without authorisation putting individuals at risk	Remote		Low
4. Data held may be out of date	Possible		Medium

STEP SIX: Identify measures to reduce risk

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, reduced or accepted). If there is residual is it low, medium or high	**Measures approved?** Yes/ no
1	• Restrict access to data through system usernames/ passwords • GDPR training delivered to all existing staff and incorporated in induction procedures for new staff provided	Reduced Restrictions on access already in place and GDPR training delivered	Yes
2	• Data only used by staff responsible for administering attachment of earnings • Legislation prescribes deduction percentages depending on income (section 6 of CT (Administration & Enforcement)Regulations 1992	Reduced Restrictions on access already in place	Yes
3	• Restrict access to data through system usernames/ passwords	Reduced Restrictions on access already in place	Yes

4	• GDPR training delivered to all existing staff and incorporated in induction procedures for new staff provided • Compliance with data retention periods that apply to service	Eliminated Data retention module in Information@Work already activated	No

STEP SEVEN: Sign off and record the DPIA outcomes

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

Item	Name/ date	Notes
DPIA prepared by (including any processor)	[redacted]	Contact details including any processor's nominated contact details
Measures approved by & deadline for completion	[redacted] **Data to HMRC by Jan 2019/ 1 year monitoring- feedback to Cabinet Office**	- Put in project plan and/ or contract - Responsibility and deadline for completion
Residual risks approved by:		If accepting residual risk and this is still high, *consult ICO*
DPO advice must be obtained		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:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA