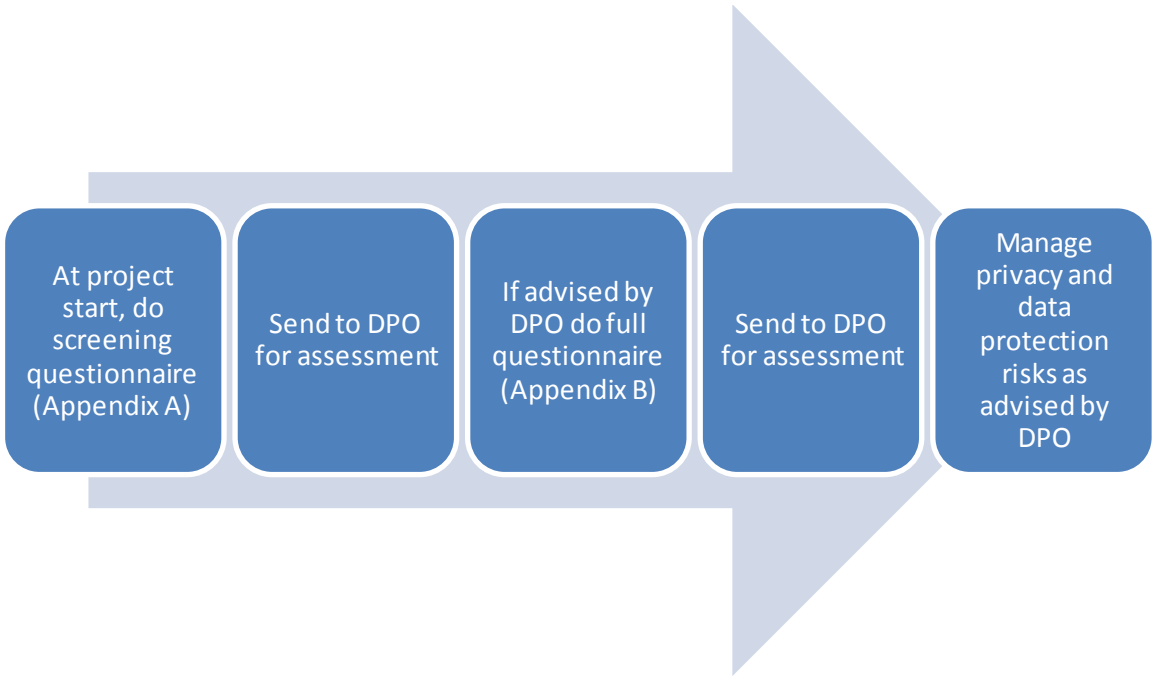
Data Protection Impact Assessment Guidance and Policy

Introduction

The General Data Protection Regulation requires organisations to understand privacy risks and to reduce them. A key method is to carry out a data protection impact assessment (DPIA). The DPIA is a questionnaire that can be applied to a project, a new activity or a large IT project. The outputs of the questionnaire are an assessment of the privacy risks, which can be managed and reduced in a timely manner, before the project progresses too far.

Outline Process



When do we need to do a DPIA?

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals. You can do this by filling in the screening questionnaire at Appendix A.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. Appendix C provides a non exhaustive list of examples where the Council is legally obligated to carry out a Data Protection Impact Assessment.

You should do the DPIA screening questionnaire at the earliest stage possible in your project or activity. It can be very costly to have to change a project if you consider privacy at too late a stage.

Appendix A: Screening Questionnaire

Answering 'yes' to any of these questions is an indication that a DPIA is required. You can expand on your answers as the project develops if you need to. Once complete, this document should be returned to the Data Protection Officer - infogov@3csharedservices.org

Project title	Taxi CCTV within vehicles
Date	
Author(s)	Myles Bebbington
Director or Information Asset Owner	Licensing manager
Date sent to DPO	
Is full DPIA needed? (for DPO to fill out)	

Please summarise the project here briefly, so that the DPO can give bespoke advice.

Installation of CCTV in licensed vehicles to assist in evidence for disputes between drivers and passengers and other incidents and accidents, to be a deterrent to would be troublemakers.

	Yes / No	Further information
1. Will the project involve the collection of new, additional or updated information about individuals? Factors that heighten risk: • process special category or criminal offence data on a large scale • systematically monitor publicly accessible places on a large scale • profile individuals on a large scale • process biometric data • process genetic data • collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') • profile children or target services at them	Yes	

2. Will the project require individuals to provide information about themselves? Factors that heighten risk: • use systematic and extensive profiling with significant effects • process special category or criminal offence data on a large scale • systematically monitor publicly accessible places on a large scale • use profiling or special category data to decide on access to services • profile children or target services at them	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? Factors that heighten risk: • process special category or criminal offence data on a large scale • systematically monitor publicly accessible places on a large scale • use profiling or special category data to decide on access to services • collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')	Yes In specific matters only such as detection,prevention of crime.	
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? Factors that heighten risk: • process special category or criminal offence data on a large scale • use profiling or special category data to decide on access to services • process biometric data • process genetic data • match data or combine datasets from different sources	No Enforcement matters	

5. Does the project involve you using new technology? Factors that heighten risk: • use systematic and extensive profiling with significant effects • systematically monitor publicly accessible places on a large scale • process biometric data • process genetic data • collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')	No CCTV with relevant notices	
6. Will the project result in you making decisions, or taking action against individuals in ways that can have a significant impact on them? Factors that heighten risk: • use systematic and extensive profiling with significant effects • process special category or criminal offence data on a large scale • systematically monitor publicly accessible places on a large scale • use profiling or special category data to decide on access to services • match data or combine datasets from different sources • profile children or target services at 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. Factors that heighten risk: • use systematic and extensive profiling with significant effects • process special category or criminal offence data on a large scale • systematically monitor publicly accessible places on a large scale • process biometric data • process genetic data • match data or combine datasets from different sources • collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') • profile children or target services at them	Yes CCTV on all the time, audio restricted	
8. Will the project require you to contact individuals in ways that they may find intrusive? Factors that heighten risk: • Contacting by email • Contacting by social media, including targeted advertising • Contacting by phone	No	

A record of the DPO decision is made here - On the basis of the screening above is a full data protection impact assessment required?	Choose an item.	Give reasons for decision here

Appendix B: Full Data Protection Impact Assessment

You should be aware that if you have unmitigated high risks that the DPO may need to send this DPIA to the regulator, the Information Commissioner's Office (ICO). The ICO can take up to 14 weeks to issue advice, including serving a notice to prevent the activity.

If you are asked by the DPO to fill one of these full assessments out, please do so and return to infogov@3csharedservices.org. The DPO is obligated to monitor this process and provide advice.

Project title	Taxi CCTV within vehicles
Date	
Author(s)	Myles Bebbington
Director or Information Asset Owner	Head of Licensing
Date sent to DPO	
Advice from DPO received on	

Article 5(a) Processing Condition: personal data is shall be processed lawfully, fairly and transparently.

A1. What is the data? Please list each data field or type (such as name, DOB, case notes, etc). Please provide a screen shot of the fields if it is easier.

Visual images and potential audio recordings of customers and drivers

A2. Please list the councils (or, if no organisation, individuals) involved (including third party or other entities).

South cambs district council

A3. Which way is the data flowing (please indicate if it flows in or out of the council and if it's both ways; explain what goes where). Feel free to draw a picture and insert.

Data collected in vehicle – held for 28 days in harddrive in boot of vehicle, then recorded over. Can down load to laptop if required to use as evidence only, otherwise held in vehicle

A4. What is the purpose of collecting this data and why is it flowing in this particular way? Why is this being done?

For security and safety of the driver and the travelling public

A5. Is there a statutory requirement to process this data in this way? No

A6. Is this:

- personal data (data that uniquely identifies living individuals) or

  Yes ☒
  No ☐

- special categories/sensitive personal data (mark if YES)

Ethnicity / Race	☐
Religious beliefs	☐
Political opinions	☐
Trade union membership	☐
Sexual life	☐
Sexual orientation	☐
Health (including Mental Health)	☐
Relating to an offence	☐
Relating to proceedings for an offence	☐
Biometric data	☐
Genetic data	☐

A7. Will you be collecting and/or processing the data of anyone under the age of 13?

Yes ☒
No ☐

If Yes:

Will they be required to sign up to a website or the use of an app or a smart device?

Yes ☐
No ☒

If Yes:

- Have you provided a privacy notice in plain English? Please attach this here.
- Tell us how you are providing age verification

A8. Please tick a processing condition that seems best to you; more than one may apply:

You have a contract with the data subjects (money must change hands)	☐
Legitimate interests (you must do a further test for this – not recommended)	☐
You have a legal obligation (there is a direct law telling you to do it)	☐
You have a statutory responsibility (there is no direct law, but you have legal obligations and the processing will aid you in achieving them)	☒
You are trying to protect the life or very serious actual danger to an individual (such as loss of a limb)	☐
You will ask for consent and the individual can freely refuse and still get the service	☐

If there is sensitive personal data, please also tick one. If there is no sensitive personal data, please indicate: There is no sensitive personal data ☒.

To fulfil employment, social security or social protection law obligations	☒
You are trying to protect the life or very serious actual danger to an individual (such as loss of a limb)	☐
Processing relates to personal data manifestly made public by the data subject	☐
Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	☐
Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	☐
Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of UK law or a contract with a health professional.	☐
Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	☐

If you cannot find what you need above, please ask the IG Team for advice – there are other processing conditions available.

A9 If you need consent from individuals, please complete the following (if you don't need consent, please move on to the next question):

Consent was explicit because…	
Consent was freely given because…	
Consent was informed because…	

A10. Will you be sending mass emails or making telephone calls to individuals as part of this work? If yes, how often and why?

A11. Is there likely to be any breach of the Human Rights Act, especially Article 8, the right to a private life? For info: https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

No

Article 5(b) Personal data is shall have a 'purpose limitation'

B1. Where data has already been collected, it should have been collected for a specified purpose. Does the use in the current project align to that original purpose?

Yes ☒

No ☐

Data not collected yet ☐

Please explain your answer is Yes or No.

B2. Is this the only use of this data? If data is being shared*, what other uses might the other organisation(s) or parts of the council want to make of it? Can we stop this in contract or data sharing agreements?

Only shared for statutory purposes

*note: Sharing may include access by a third party company to give support / ability to access by administration. Third party company taking anonymous statistics.

Article 5(c) Personal data is shall be adequate, relevant and limited to what is necessary – 'data minimisation'.

C1. Is the information being processed necessary?

Please go back to A1 and for each data type, justify why it is being used - can you get away with anonymising some (e.g. replacing a name with a number, using only the first half of a post code) of it or aggregating (instead of giving age or DOB, giving age range such as 20-24; 25-29, etc).

Yes, for enforcement processes and identifying relevant individuals

Article 5(d): personal data is shall be accurate, kept up to date, have regard for which they are processed (Article 6 and 9) and be erased or rectified without delay ('accuracy')

D1. How will this information be kept up to date? If there is no need (because the information is being shared and is supposed to be a snapshot, please say)

Recorded for 28 days and then recorded over on a continuous loop

Article 5(e): information should not be kept longer than necessary

E1. How long does the information have to be kept for the purpose of the project? Can information be anonymised or aggregated later and kept?

28 days and then recorded over

E2. Are there any statutory retention periods for the information? 28 days as recommended by ICO

E3. Do the parties have up-to-date retention schedules and policies?

Yes

Article5(f): Processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

F1. Where will all the data be held?

Please give locations of all drives, systems (internal and external), including back up locations, and any physical storage.

Recording takes place in vehicle held in hard drive in boot. Recordings taken by EH designated laptop will be stored on secure drive, restricted access

F2. Will there be encryption? Please consider information in storage and information in transmission, as well as any need to travel with information. Please include details of encryption standards used.

Yes to the current FILPS 140-2 (level 2) standard or equivalent

F3. Please give a list of all people that will have access to the data and the need for the access if it is not obvious.

Myles Bebbington – Head of Licensing, John Goodwin – Enforcement Officer

F4. If data is leaving the council, is there a contract and/or a data sharing agreement in place?

Not applicable

What due diligence did you perform to make sure the partner organisation can be trusted with the data?

Not applicable

F5. Who is the data controller and who is the processor? (a controller has control over the data and is responsible for how it uses it - a processor is usually undertaking the work on behalf of a controller and can only do what is specified in contract).

South Cambridgeshire District Council

F6. If data is leaving the council, is the receiving organisation's physical security and security auditable? Is it ISO 270001 or NHS IG Toolkit compliant?

Not applicable

F7. If data is leaving the council, has a penetration test of the receiving organisation's systems been considered?

Not applicable

F8. Once the work is complete how will data be destroyed? Please provide details of how information is shredded (included specifications), how information is removed from cloud servers and local servers.

In the vehicle it is recorded over, on the lap top, will be deleted in line with retention policy

F9. What systems are in place to ensure detection or prevention of unauthorised access to data? This might include passwords, smartcards, etc.

Laptop password protected, hard drive in vehicle has a seal and key for access

F10. What policy is in place to report data incidents or breaches? How are these handled?

Data breach reporting as per IG policy

F11. Is data being transferred outside the EEA? Please consider your own back ups and other companies who have access and whether their storage and back ups are. If so, how is this being handled and assured?

Not applicable

Accountability

How are you proving that you are compliant with the data protection principles?

Alongside the above principles, the GDPR also provides the following rights for individuals:

1. The right to be informed (Article 13 and 14)

If you receive the data directly from the individual: Do you have a privacy policy in place that informs the individual in a concise, transparent, intelligible and easy accessible way? And contains in the list here. Not applicable

If you are collecting data that was not given to you by the subject matter directly and has been obtained by other methods, how are you telling individuals whose personal data we want to use about this? e.g.

- is there any other communication?
- are you running a consultation?
- Are you going to write to them?

Do you have a process in place for contacting them and ensuring they are given all details required? List here.

Signs will be clearly displayed in vehicles

2. The right of access (Article 15)

Do **all** parties have clear procedures for data subjects to submit subject access requests to be able to see their personal data?

Yes

3. The right to rectification (Article 16)

If asked to, can you physically delete the data? If the information is being shared; do you have a process in place to ask the council's to also delete the data?

is there a contract clause that advises they must delete the data and/or hand it back at the end of the contract within 30 days of contract ceasing?

Yes

If asked to, can you physically delete or destroy the data out of your system on a record by record basis? i.e. not destroying the whole data base/system/information collection.

Yes

On deletion or destruction, how long will it take to leave the network and a system to be complete expunged? E.g. Consider backs up and how long before backups are over written. Consider the information to be on your network if it can be restored.

Not applicable

If the information is being shared; do you have a process in place to ask the council's to also delete the data?

is there a contract clause that advises they must delete the data and/or hand it back at the end of the contract within 30 days of contract ceasing?

Not applicable

5. The right to restrict processing (Article 18)

Do **all** parties have clear procedures for data subjects to submit subject access requests to be able to know whom to contact to ask for their data to stop being processed?

6. The right to data portability (Article 20)

Are you able to pull the data from the system in a machine readable format that enables transfer of the data to another provider?

7. The right to object (Article 21)

Will you be undertaking any direct marketing to the individual? If so, do you have a process in which the direct marketing can cease if the individual objects?

Will you be processing any scientific or historical research purposes or statistical purposes?

8. Rights in relation to automated decision making and profiling. (Article 22)

Will any decisions about the data subject be made on the basis of a solely automated process or the data linking or matching with other data sets?

How will you ensure that automated decision making or profiling data is accurate when being linked or matched?

Will you be profiling individuals to gain a 'bigger picture' about them?

Identify the privacy and related risks The DPO will issue advice here			
Privacy issue	**Risk**	**Recommended Actions**	**Outcome**

Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project?

What solutions need to be implemented?

Is there dissent from the advice provided or opinion of the DPO? If so record here.

Further information: read pages 30-31 of the ICO Code of Practice.

Risk	Approved solution	Approved by

7: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the privacy impact assessment 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?

Further information: read page 32 of the ICO Code of Practice.

Action to be taken	Date for completion of actions	Responsibility for action

Appendix C: Examples of when a Data Protection Impact Assessment is Required.

We're thinking of:

☐ using systematic and extensive profiling or automated decision-making to make significant decisions about people.

☐ processing special category data or criminal offence data on a large scale.

☐ systematically monitoring a publicly accessible place on a large scale.

☐ using new technologies.

☐ using profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.

☐ carrying out profiling on a large scale.

☐ processing biometric or genetic data.

☐ combining, comparing or matching data from multiple sources.

☐ processing personal data without providing a privacy notice directly to the individual.

☐ processing personal data in a way which involves tracking individuals' online or offline location or behaviour.

☐ processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.

☐ processing personal data which could result in a risk of physical harm in the event of a security breach.

☐ evaluating or scoring.

☐ automating decision-making with significant effects.

☐ systematically processing sensitive data or data of a highly personal nature.

☐ Processing on a large scale.

☐ Processing data concerning vulnerable data subjects.

☐ Innovating technological or organisational solutions.

☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ If we decide not to carry out a DPIA, we document our reasons.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

☐ Describe the nature, scope, context and purposes of the processing.

☐ Ask Information Asset Owners to help you to understand processing activities and identify any associated risks.

☐ Consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ Ask for the advice of the data protection officer (DPO)

☐ Check that the processing is necessary for and proportionate to your purposes, and describe how you will ensure data protection compliance.

☐ Do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ Identify measures you can put in place to eliminate or reduce high risks.

☐ Record decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ Implement the measures we identified, and integrate them into our project plan.

☐ Ask the DPO to consult the ICO before processing, if we cannot mitigate high risks.

☐ Keep DPIAs under review and revisit them when necessary.