



**SURVEILLANCE CAMERA
COMMISSIONER**

ico.
Information Commissioner's Office

Data protection impact assessments
template for carrying out a data
protection impact assessment on
surveillance camera systems



Project name: Body worn video cameras

Data controller(s): Coventry City Council

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA¹:

- | | |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data |
| <input type="checkbox"/> Public monitoring | <input type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input checked="" type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input checked="" type="checkbox"/> Other (please specify) |

Coventry City Council's Civil Enforcement Officers will capture video footage which will include members of the public who physically or verbally threaten / assault Civil Enforcement Officers.

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

No - an existing system
DPA 2018

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

Information will be collected using Body Worn video cameras that will record images and sound of any interactions between the Council's Civil Enforcement Officers and members of the public whilst undertaking parking enforcement operations.

Body worn video cameras record sound and vision of incidents and therefore, they have the potential to invade the privacy of those involved in an incident. The purpose of recording is to safeguard Civil Enforcement Officers and members of the public during enforcement operations and to provide good

¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/>

evidence for all parties in the event of complaints or investigations lodged with the Council or any other investigation into incidents, accidents or alleged assaults. The recording of offences and incidents may result in a higher number of members of the public being prosecuted or receiving warnings and a reduction in the number of assaults against Council employees.

The equipment will be used in an overt manner at all times and devices will be visible to the public. Devices will not be switched on whilst the Civil Enforcement Officer is travelling to / from their work location or during rest and comfort breaks.

Recordings will only be held for as long as an incident is being investigated.

Any attempt to delete a recording will be clearly identifiable through the device's audit trail.

Control records will be maintained to show which officers are using specific devices at any given date / time.

The use of body worn video cameras by Council staff must be proportionate, legitimate, necessary and justifiable, and Coventry City Council is satisfied that it is.

Recordings are retained for a 30 day period unless they are being used as evidence as part of an on-going investigation. Recordings will be automatically deleted and overwritten after 30 days.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

Information will be collected using a Body Worn video camera which will record images and sound of any interactions between the Council's Civil Enforcement Officers and members of the public, [which potentially may include children or other vulnerable groups], whilst undertaking enforcement operations.

The purpose of recording is to safeguard Civil Enforcement Officers and members of the public and to provide good evidence for all parties in the event of complaints or investigations lodged with the Council or any other investigation into incidents, accidents or alleged assaults.

BWC recordings will constitute personal data and its creation, retention and use has been considered under the provisions of the Data Protection Act 1998. Recordings can be requested through subject access requests by following the Council's Access for Personal Information procedure.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Parking Manager

Information may be shared with the police in line with any investigations and potential prosecutions.

6. How is information collected? (tick multiple options if necessary)

- | | |
|---|---|
| <input type="checkbox"/> Fixed CCTV (networked) | <input checked="" type="checkbox"/> Body Worn Video |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Redeployable CCTV |
| <input type="checkbox"/> Other (please specify) | |

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Officer starts BWV recording when enforcing parked vehicles.

Information is stored on the device.

The device is docked at the end of shift and the video footage is automatically uploaded onto the Council's network where it is stored on a secured server as an encrypted file.

Authorised officers with the relevant permission can review the footage if necessary.

Officers with relevant permission can create incidents for use as evidence by the police or in line with internal investigations.

Information cannot be amended or tampered with.

Information will be automatically deleted in line with the deletion policy (30 days) unless the information is needed as evidence for an ongoing investigation.

Any incidents that are created pending further investigation will be deleted by the Authorised Officer when the incident investigation has been closed and the footage is no longer required.

8. Does the system's technology enable recording?

- Yes No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

On-site - body worn video camera
Audio recording is enabled

9. If data is being disclosed, how will this be done?

- Only by on-site visiting
 Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)
 Off-site from remote server
 Other (please specify)

Encrypted link of the video to the intended recipient.

10. How is the information used? (tick multiple options if necessary)

- Monitored in real time to detect and respond to unlawful activities
- Monitored in real time to track suspicious persons/activity
- Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.
- Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
- Linked to sensor technology
- Used to search for vulnerable persons
- Used to search for wanted persons
- Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
- Recorded data disclosed to authorised agencies to provide intelligence
- Other (please specify)

The information may be used by the police in line with investigations into assaults against Council employees or to help prevent other criminal activity, or as part of an internal investigation into a complaint against an employee.

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Staff	Meetings	Personal privacy could be compromised. Likely to in-flame situations rather than de-escalate.	Operational procedure note developed and adopted.
Trade union colleague	Meetings		Operational procedure note adopted and implemented

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

Personal data shall be obtained only for the specified purposes, and shall not be further processed in any manner incompatible with that purpose.

The information is to safeguard Civil Enforcement Officers and members of the public during enforcement operations and to provide good evidence for all parties in the event of complaints or investigations lodged with the Council or any other investigation into incidents, accidents or alleged assaults.

Data Protection Act 2018, Human Rights Act

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

Civil Enforcement Officers wear armbands indicating that CCTV recording is in progress.

Body worn cameras indicate when a camera is recording.

Civil Enforcement Officers are required to verbally inform members of the public that they are being recorded.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

Operational procedures have been developed and staff have been trained.

Cameras are only switched on when officers are undertaking the enforcement of a vehicle.

15. How long is data stored? (please state and explain the retention period)

Information is stored in line with the system's deletion policy setting which is normally 30 days.

Any information relating to assaults or incidents that are subject to investigation will be stored until the incident has been investigated and the matter closed. At that point the information is deleted.

16. Retention Procedure

- Data automatically deleted after retention period
- System operator required to initiate deletion
- Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

Data is automatically deleted after 30 days retention period.

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The information is stored on secure servers.

Once the information has been uploaded it will be kept securely on a password protected laptop which can only be accessed by authorised personnel.

The data will be processed only for the specified purpose in accordance with the Data Protection Act 1998.

The use of data by the Police or in court proceedings will be subject to written documented requests which will be signed for by the person receiving the data.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

Subject Access Requests are received, managed and responded to by the Council's Information Governance department in line with the Council's policy.

Information requested in line with an SAR will be provided in line with a request from Information Governance to the Parking Manager.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

.Not applicable

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

- The agencies that are granted access
- How information is disclosed
- How information is handled

Are these procedures made public? Yes No

Are there auditing mechanisms? Yes No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

Data Privacy Statement published on the Council's website.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

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
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

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
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
	Eliminated reduced accepted	Low medium high	Yes/no

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
	Eliminated reduced accepted	Low medium high	Yes/no

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. [Further information](#) is on the ICO website.

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		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:		

Date and version control: 19 May 2020 v.4

This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.
---	--	--

APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Town centre	All	250	24hrs	24hrs (only maximum 3 operators) – likely average patrol high hourly	The privacy level expectation in a town centre is very low; our town centres are well signed with appropriate signage for CCTV its use and purpose with contact details.
Public car park	1, 5, 6	100			
Parks					HD camera only include due to proximity to town HD cam
Play areas					
Housing blocks internal	1, 2	200	24hrs (calendar month)	Limited due to the fact that most are static cameras	High level asb historical problems (please see statistical assessment in annual review)
Housing estate (street)					
Residential street					Cameras are installed here to respond to high crime trends, deal with the fear of crime

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



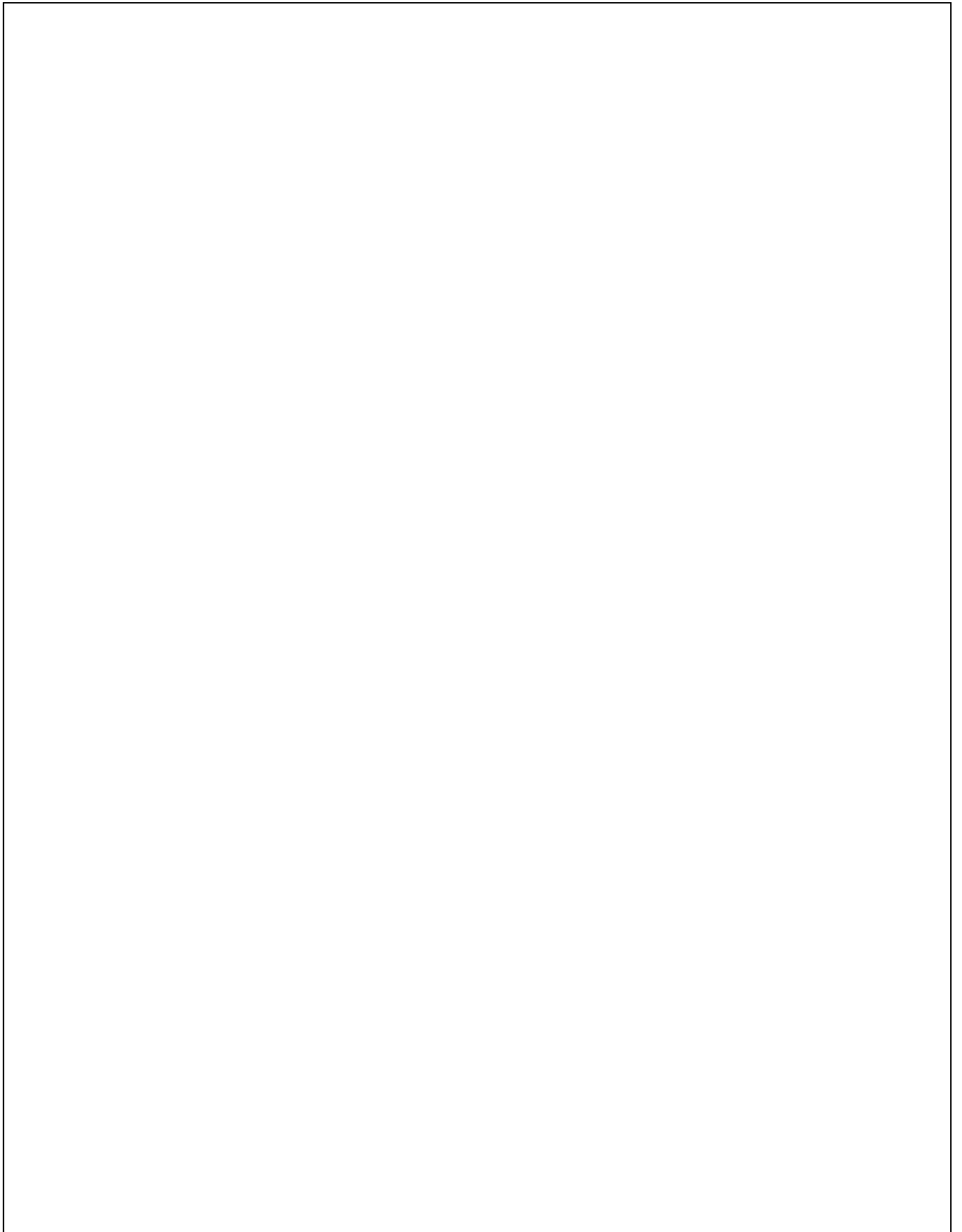
APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:

	Camera Types (low number low impact – High number, High Impact)									
	→									
Location	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Types	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
A (low impact)	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Z (high impact)	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red

NOTES

A large, empty rectangular box with a thin black border, intended for taking notes. It occupies most of the page below the 'NOTES' header.

Date and version control: 19 May 2020 v.4

