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: CCTV - Body Worn Video

Data controller(s): London Borough of Waltham Forest

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 DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☐ Targeting children / vulnerable adults
☒ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

BWV is to be used by staff deployed in public spaces to negtate a risk of harm or abuse and to capture evidence if this occurs which could be used in civil or criminal proceedings

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 expansion to the system just an update and review of policies associaited with its use. Processing is carried out under the guidelines of 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.

BWV will be used by Council Nighbourhood and Enforcment Teams to protect them while carrying out their statutory duties, locations of use will include Council property such as libraries and open spaces as well as public areas such as high streets. BWV is being used to reduce abuse or harm to Council staff and forms part of their Personal Protective Equipment. It is also hoped the presence of BWV de-escalates a potention conflict situation for the safety of the public as well as Council staff

[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/

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?

The system records both images and audio of anyone within its field of view so has the potential to capture live images of people and anything they may say, the system is reactive to each individual situation and will not be used to gather large amounts of data such as being left on record for a whole day while the staff member is working. The data subjects will be anyone the staff member feels they need to record due to the situation they are in at the time which would mostly be members of the public. If a recording is activated it will be stopped once the situation is over

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.

The system is in use by the Neighbourhood and Enforcement Departments, they may need to share data gathered by BWV with outside agencies such as the Police for evidential purposes if a crime has been record on a device

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

- ☐ Fixed CCTV (networked)
- ☒ Body Worn Video
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Redeployable CCTV
- ☐ 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.

Any recording on a BWV device will include images and audio this stays on the device until placed into a docking station attached to a computer. Each individual is issued their own BWV device and a user account on a Digital Evidence Management Systen, when the device is placed in the docking station any recordings it contains are uploaded onto the D.E.M.S where only that user can view them. Unless marked as evidential all recordings are auto-deleted after 30 days. Evidential recordings are retained for a period of up to 2 years. No watch lists or facial recognition is integrated into the system and it does not have the ability to be watched live.

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.

Images and audio are recorded on site

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)

Police would need to attend the Office where the BWV is docked to retrieve any recordings

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 system is in place to deter assualt or abuse of staff and capture evidence if it does occur this would only be released to assist in investigations or court proceedings.

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

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.

The system is used under Section 115 of the Crime and Disorder act 1998 to enable evidential release of any incidents
GDPR Article 6 (1) E Processing is necessary for the performace of a task carried out in the public interest, or in the exercise of official authority vested in the Controller
Under section 163 of the Criminal Justice and Public Order Act 1994

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.

The BWV device is located in a prominent area on the users clothing and not concealed in anyway, if a member of staff begins to record they are trained to verbally tell the person being recorded that a BWV video is now recording them including any audio

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?

Any staff issued BWV are trained on its use and associated Council policies. The evidence of whether the system is providing benefits is the reduction or eradication of assaults and abuse on staff

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

The standard retention period is 30 days this increases to two years if the recording is marked as evidential

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)

The Digital Evidence Management System will auto delete non evidential recordings after 30 days. If a recording is marked as evidential it is stored for up to 2 years automatically by the system, evidentials recordings can be manually deleted if not needed anymore or will be auto deleted by D.E.M.S after the 2 year retention. The 2 year retention period is to allow adaquet time for any court proceedings to be finalised in case the recording is needed

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?

Staff issued with BWV are trained in its use and how to correctly transfer and store data to D.E.M.S individual staff members also only have access to the recordings they make and cannot see any other devices recordings. The system is obtained from Pinnacle who are an industry leader and ensure all necessary processes are protected through their software. The D.E.M.S system also resides within the Councils ICT systems and firewalls adding a further layer of protection from outside intrusion, Council staff must also undergo mandatory Cyber Security training. The Operations Centre Manager can test compliance with processes and policies through visits to personnel utilising BWV

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.

The Council has policies and proceedures for Subject Access Requests and Data Requests which are followed if a request is received, each request is reviewed on a case by case basis and if data is held on a Council system and can be lawfully released to the requester it will be

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.

The Council operates a CCTV system across the Borough but cannot see all areas, a BWV system would allow for increased protection of staff while not increasing surveillance on a permanent basis in wider areas of the community. Due to the nature of its use in protecting staff from assault or abuse the need to record audio is also a requirement which is why a BWV system was chosen.

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)

All associated processes are reviewed annually.

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**
Privacy	Remote, possible or probable Possible	Minimal, significant or severe Severe	Low, medium or high Medium
Recording of personal data	Probable	Severe	medium
Retention and deletion of data	Probable	Severe	medium
Excessive or inappropate monitoring	Possible	Severe	Low

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**
Data handling and provision	Remote, possible or probable Possible	Minimal, significant or severe Severe	Low, medium or high Mediun
Sharing of information	Possible	Severe	Medium

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?**
Privacy - BWV will only be used to capture any potential harm or abuse to staff and will not record at all times. It will have a field of view similar to that of the staff member to minimise unneccessary data capture	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Recording of personal data - Images and audio recordings will be captured but only for the purpose of evidence gathering. Access to this information is restricted to trained and authorised staff.	Reduced	Low	Yes
Retention and deletion of data - Data is retained for 30 days then auto deleted unless marked as evidential then it can be retained for up to 2 years	Reduced	Low	Yes

Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Excessive or inappropiate monitoring - Staff are governed by the LBWF Code of Practice and BWV Operatinal Procedures. Appropiate monitoring and use of equipment will be in accordance with the relevant procedures	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Data handling and provision - Data handling and issuing is governed by the Code of practice. The process in which data is handled and issued is outlined within the procedure and only conducted by authorised trained staff in accordance with policy and procedure.	Reduced	Low	Yes

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:	Heidi Balci - Deputy DPO 23.02.2022	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by:	N/A	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)	John Hubbard, Director of Commercial & Innovation. 23.02.2022	If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.

Date and version control: 19 May 2020 v.4

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

Date and version control: 19 May 2020 v.4

APPENDIX ONE

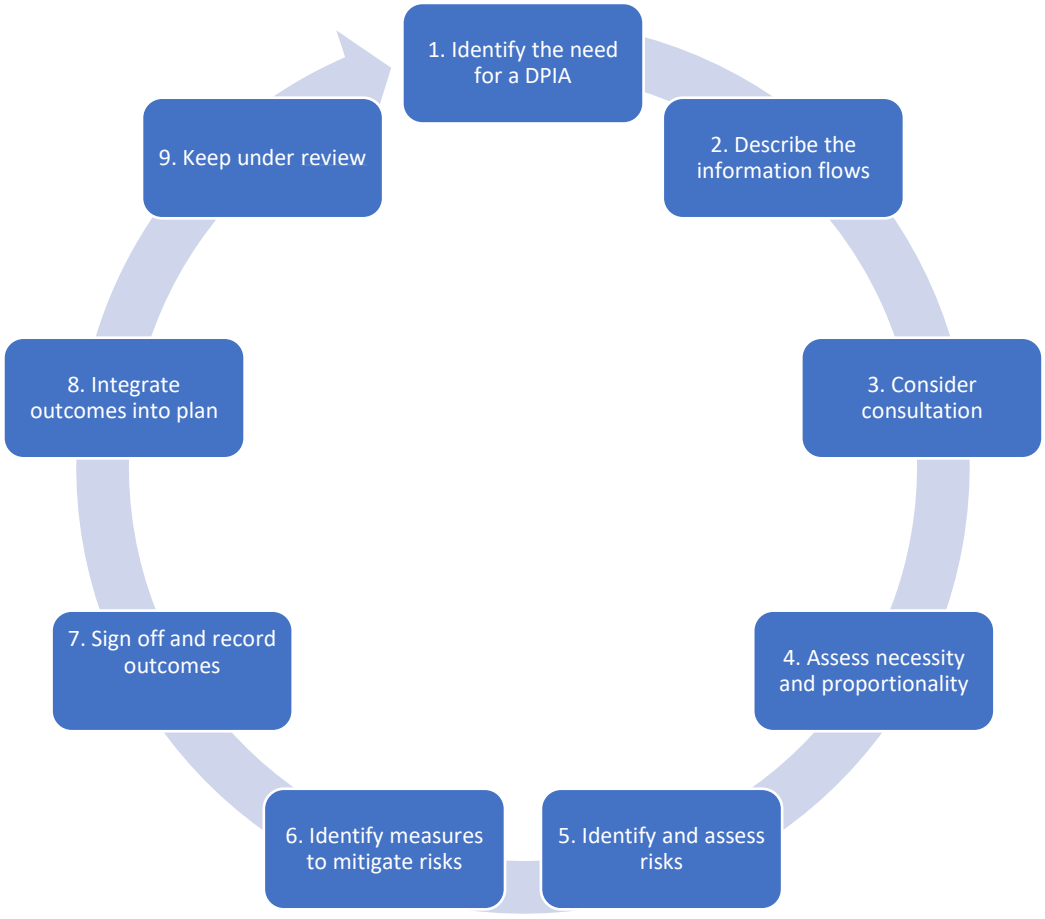
This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

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)
Neighbourhoods Department	Pinnacle PR6	30	Images and audio	No	Prevent and deter assualt or abuse of staff
Enforcement Department	Pinnacle PR6	8	Images and audio	No	Prevent and deter assault or abuse of staff

Date and version control: 19 May 2020 v.4

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

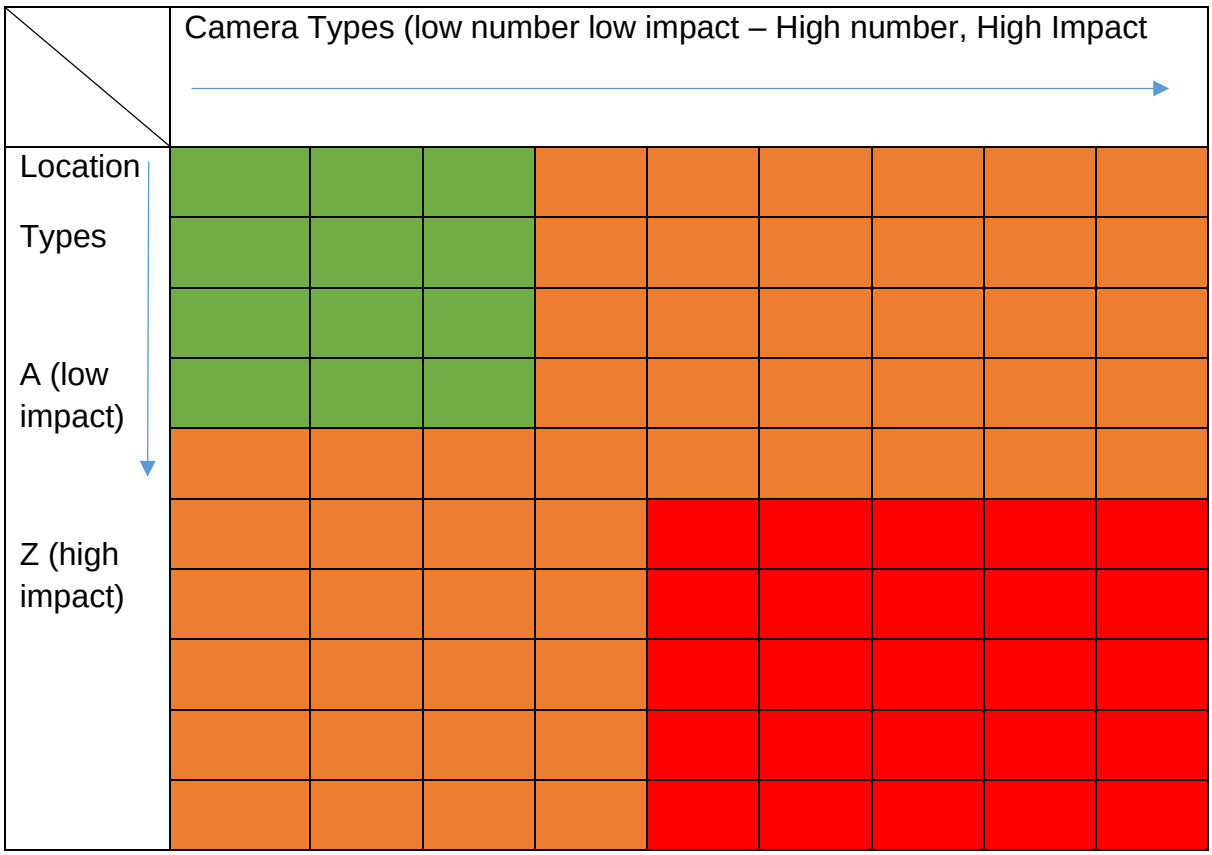


Date and version control: 19 May 2020 v.4

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:



Date and version control: 19 May 2020 v.4

NOTES

Date and version control: 19 May 2020 v.4

Date and version control: 19 May 2020 v.4