

Data protection impact assessments

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



Project name: Verkada CCTV Project

Data controller(s): North Tyneside 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:

- | | |
|---|---|
| ☐ 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) |

Provide a cloud CCTV and security management platform and the provision of CCTV and security devices. Public space and town centre monitoring for crime prevention and detection of crime and public safety.

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)?

Upgrade of the current CCTV system to replace an existing system to provide a cloud CCTV and security management platform and the provision of CCTV and security devices in accordance with the SCC code of practice. Lawful basis for processing under GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

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.

CCTV cameras have been installed in areas of the town centres and public places to assist in the prevention and detection of crime, improve public safety and reduce anti-social behaviour. Information is collated from local crime and anti-social behaviour statistics which are provided by the police and monthly performance indicators produced by the CCTV control room which detail reactive and proactive incidents, arrests recorded on camera, reviews of footage and the production of evidence.
Crime Prevention and Detection:

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/>

The primary use of CCTV data is for crime prevention, identifying and deterring criminal activity, and providing evidence for investigations and prosecutions.

Public Safety and Order:

Monitoring public spaces to ensure the safety of residents, manage crowd control, and prevent public disorder.

Monitoring and Investigating Complaints:

Reviewing footage in response to specific complaints or concerns raised by the public or law enforcement agencies.

Incident Reporting: Using CCTV data to verify and report incidents such as accidents or disputes in public areas.

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 Authority will process personal data of persons in public places such as town centres, car parks, Authority property and residential streets. The data collected and processed is in the form of recorded video footage. There will be images of children, vulnerable persons, people from minority ethnic groups and religious beliefs however this will not be known at the time of recording unless the cameras are being proactively used by staff.

Any proactive monitoring of the public must be justified by the operator. A full audit trail is maintained and inspected by the system manager on a regular basis. Images of individuals will only be released to investigating authorities in accordance with the objectives listed in the code of practice. The system will be used in an overt manner and signage informing the public that cctv is in operation will be displayed throughout the borough.

The CCTV system, does not discriminate in any way, nor does it have any analytical software which could be used to discriminate people.

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 data owner and data controller is North Tyneside Council. The Authority may share data with third parties for law enforcement purposes, statutory investigations, fraud and prosecution of offenders.

No other organisation will have access to the data other than consideration of individuals exercising their rights in relation to subject access requests where appropriate.

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.

The proposed CCTV solution has the flexibility to choose the region where data is stored and processed. This allows the Authority to select specific geographical locations for data storage and processing, enhancing performance and ensuring compliance with regional data protection regulations. Data is securely held within Amazon AWS cloud infrastructure hosted in the EU.

Verkada Customer Data Processing Agreement - <https://legal.verkada.com/#cdpa>

Verkada Data Residency & Processing - <https://help.verkada.com/en/articles/9709469-data-residency-processing>

Data that will be shared will ensure purpose limitation, data minimisation and have a lawful basis for sharing data. A Verkada account will be created and managed by the authority, and then provisioned accordingly. Live feeds or archived footage can be shared, but full control and audit logs remain with the authority. Further information can be found here - <https://help.verkada.com/en/collections/2452515-sharing-video>

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.

CCTV Control Centre, visual recording only

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/statutory prosecuting authorities will access data on site. Subject Access requests, requests from Insurance Companies and solicitors will be dealt with on a case by case basis where appropriate and released by using encrypted media and this is recorded with the Authority Information Governance Team.

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)

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
Northumbria Police	Monthly Meeting	Location of CCTV cameras, quality of images, damaged camera, re-deployment of cameras, new CCTV camera locations	Procurement of new CCTV system, re-mapping of CCTV locations
Northumberland Fire and Rescue Service	Monthly Meeting	Location of CCTV cameras, quality of images, damaged camera, re-deployment of cameras, new CCTV camera locations	Procurement of new CCTV system, re-mapping of CCTV locations
Council Members	Quarterly Meeting	Adequate signage, internal ownership of processes, information to be published to the public, how to handle complaints	CCTV Steering Group, CCTV Policy, changes to signs and websites
Child Services	Monthly Meeting	Location of CCTV cameras, quality of images, damaged camera, re-deployment of cameras, new CCTV camera locations	Procurement of new CCTV system, re-mapping of CCTV locations
Housing Associations	Monthly Meeting	Location of CCTV cameras, quality of images, damaged camera, re-deployment of cameras, new CCTV camera locations	Procurement of new CCTV system, re-mapping of CCTV locations

--	--	--	--

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.

GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

Local authorities establish their CCTV systems under the GDPR/DPA 2018 and Section 17 Crime and Disorder Act 1998 which places an obligation on local authorities and the police to work in partnership to develop and implement a strategy for tackling crime and disorder. Section 17 outlines how and why local services may impact on crime and disorder and indicates the reasonable actions that might be put in place to ensure a co-ordinated approach to crime reduction. Evidence shows the opportunity for crime and disorder may be reduced and the safety and reassurance of the public improved when there is adequate CCTV coverage and it is used with other interventions. Using CCTV remains a strategic, financial and operational choice in exercising crime reduction partnership responsibilities between the police and other relevant supporters.

In addition, Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare

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 Authority website provides information on location of cameras, statistics, privacy notice. SCC Self Assessment Tool, Code of Practice and DPIA Appropriate signage in and around the area where surveillance is taking place. Data subjects will reasonably expect to be under surveillance, confirmed via public notices in CCTV locations.

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?

The Authority has installed CCTV (Closed Circuit Television) cameras in various locations within the conurbation for the purposes of reducing crime, disorder, anti-social behaviour and the fear of crime by helping to provide a safer environment for those people who live and work in the area and for visitors travelling through the area.

CCTV is also installed on highways for monitoring traffic on a permanent or temporary basis. In all locations, signs are displayed notifying you that CCTV is in operation and providing details of who to

contact for further information about the scheme. The purpose and use of the CCTV system are to provide the Police and enforcement agencies with assistance to detect, deter and prevent crime and disorder; to help identify, apprehend and prosecute offenders; to provide the Authority and Police agencies with evidence to enable criminal and/or civil proceedings to be brought in the courts; and to maintain public order.

Some examples of how we use data are provided below;

- Providing evidence in criminal proceedings (police and criminal evidence act 1984 and criminal procedure and investigation act 1996)
- Providing evidence in civil proceedings
- The prevention and reduction of crime and disorder
- The investigation and detection of crime
- Identification of witnesses

Effectiveness of the system is measured in performance indicators along with information supplied by the police and other authority departments. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and SC Code of Practice, GDPR/DPA is measured through SCC Certification process.

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

The proposed solution is not reliant on the existing CCTV solution. New data fields will be processed under the proposed CCTV solution, as indicated above. Footage from the existing CCTV solution will be retained for 30 days to ensure the completion of any investigations. Any data that is required for more than 30 days will be archived in line with the new operating procedure developed for the new CCTV solution. Cost implications will be taken into consideration for this approach.

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)

Footage may be retained for more than 30 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceedings and Subject Access Requests.

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?

Access is restricted to the control room and system. The system is password protected and use is subject to regular audits. The system is security tested regularly. Continue strict access controls, encryption, MFA and audit trails for CCTV data. Regularly train staff on security. Consolidation of multiple systems into a single platform. Removal of any generic accounts.

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 Authority CCTV policies and procedures are fully compliant with the GDPR/DPA 2018 for general disclosure access requests and CCTV related subject access requests. Information on subject access can be found on the North Tyneside Council website and all requests are initially dealt with by the Information Governance Team and then passed to the CCTV Manager.

Any complaints are dealt with through the councils corporate complaint procedure.

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.

Intrusiveness, monitoring of non-criminal activity, handling of personal data, data retention, access control, abuse of power, unfair targeting. All have been mitigated by DPIA, CCTV Policy review, security measures and minimisation of data collection.

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)

Any CCTV operation is audited. This includes the use of cameras, reviewing and downloading images, access, storage and incidents recorded. Regular audits are carried out by the CCTV administration staff.

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
Non Compliance of GDPR/DPA 2018. The GDPR/DPA sets out seven key principles which CCTV System owners must comply with: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability Non compliance may result in prosecution, financial penalties and severe damage to the reputation of the local authority	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Compliance with articles 6, 8 and 14 of the Human Rights Act. The Act applies to public authorities and other bodies, which may be public or private, when they are carrying out public functions Article 6: the right to a fair trial Article 8: right to a private and family life Article 14: protection from discrimination	Possible	Significant	Medium

A breach of any article may impede on the subjects rights and result in the prosecution of the local authority resulting in financial penalties and severe damage to its reputation			
Compliance with Code of Practice and the Protection of Freedoms Act 2012. The code of practice is issued by the Secretary of State under Section 30 of the 2012 Protection of Freedoms Act. Relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales must have regard to the code when exercising any functions to which the code relates. A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings. The surveillance camera code is admissible in evidence in any such proceedings. (A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings. This is reflected in the Crown Prosecution Service Disclosure Manual Reputational damage to Local Authority. The court may take inference in an authorities non compliance.	Possible	Significant	Medium
Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalties and severe damage to the reputation of the local authority.	Possible	Significant	Medium
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

Unauthorised Disclosure that may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority	Possible	Significant	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?
Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Compliance with articles 4, 6 and 13 of the Human Rights Act Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff.	Reduced	Low	Yes
Compliance with Code of Practice and the Protection of Freedoms Act Management of system. SCC Full certification.	Reduced	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Unauthorised Disclosure Release of data is strictly controlled by the Authority. Information Sharing Agreement/SLA in place with Police. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Misuse of Data Release and use of data is strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Financial Loss. Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. SCC Full certification achieved and regular audits are carried out by the system manager.	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:		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: Emma Phillips	Emma Phillips 29/01/25	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Surveillance is proportionate and appropriate, with the relevant COP, DPIA and management of risks in place. Relevant protocols followed in relation to data handling and disclosure. CCTV policy regularly reviewed, alongside operational guidance and industry best practice.		
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:		

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)
					.
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)
					Cameras are installed here to respond to high crime trends, deal with the fear of crime
Public Spaces/Town Centres	PTZ & ANPR	61	24 Hours	Monitored throughout each 24 hour period at different times of the day/night	To monitor, prevent and detect crime. The privacy level expectation is very low; our town centres are well signed with appropriate signage for CCTV its use and purpose with contact details
NTC Buildings	Mini Dome (Internal and external), fish eye and ANPR	58	24 hours	Monitored throughout each 24 hour period at different times of the day/night	Cameras are installed to protect staff safety, public safety and the security of the building.
██████████	1 x mini dome	1	24 hours	No allocated/set monitoring schedule	Installed on a temporary basis following safe guarding concerns of residents in the communal area due to risk of violence
██████████	Internal & External Mini Domes	6	24 hours	Limited due to the fact that all are static cameras	To protect staff and building security and to safeguard vulnerable tenants.
					I

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 Types A (low impact) Z (high impact)											

