



**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: NORTH AYRSHIRE COUNCIL PUBLIC SPACE SURVEILLANCE CCTV SYSTEM,

Data controller(s): NORTH AYRSHIRE 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 checked="" 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 checked="" type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input type="checkbox"/> Other (please specify) |

Public space 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)?

The system is an existing estate management monitored, maintained and certified in accordance with the SCC code of practice. and governing guidance. 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, housing estates 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 on recorded on camera, reviews of footage and the production of evidence. The key performance indicators along with an annual report are published on the councils website. These can be found at www.north-ayrshire.gov.uk

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 council will process personal data of persons in public places such as town centres, car parks, the promenade 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 Ayrshire Council.. The council will share data with

1. Data subjects
2. Statutory prosecuting authorities
3. Clients and authorised investigators

The Data Sharing Agreements are in place with Law Enforcement, North Ayrshire Council Environmental Enforcement Team and North Ayrshire Council Housing Services. No other organisation will have access to the data other than general individuals exercising their rights in relation to subject access requests.

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

- Fixed CCTV (networked)
- ANPR
- Stand-alone cameras
- Other (please specify)
- Body Worn Video
- Unmanned aerial systems (drones)
- Redeployable CCTV

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.

Data will be captured in video format. The system is hard wired. There is live monitoring by trained and vetted CCTV operators from the main CCTV control room. There is no AFR or audio recording. Staff will be provided with intelligence by the police relating to crime hotspots, wanted and missing persons. The retention periods is 31 days after which there is an automatic deletion of the footage. Procedures, data sharing and security are in line with Council policy and procedures. Authorised staff have received relevant training in legislation, procedures and use of the system. Footage may be retained in an evidence locker for more than 31 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceedings and Subject Access Requests. The evidence locker is reviewed by the manager on a monthly basis. The principles of GDPR/DPA 2018 will be adhered to at all times.

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 Server Room

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 will access data on site. Subject Access requests, requests from Insurance Companies and solicitors will be dealt with differently depending on any data protection issues that may arise. All parties are required to sign a disclosure form for any media.

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)

Released to council departments investigating ASB, Licensing and Fly Tipping.

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 |
|---|----------------------------|---|---|
| Police Scotland | Email, meetings | Requests for images to address crime hotspots or increased ASB | Process application, Site assessment, public consultation, signage, measure effectiveness |
| North Ayrshire Council Community Safety Team | Email, meetings | Requests for images to address crime hotspots or increased ASB. Discuss funding for future developments | Consultation with police, analysis of existing data, impact of new development on community safety, liaison with planning department and developers |
| North Ayrshire Council Housing Offices | Email, meetings | Existing camera system. | Meetings with business groups, maintenance of cameras, signage updated. |
| North Ayrshire Council Environmental Enforcement Team | Email, meetings | Existing camera system. Requests for images to address fly tipping hotspots and increased fly tipping. | Regular Email contact with Environmental Enforcement Team to address any concerns or requests |
| Public/Councillors | Email, meetings | Support for CCTV System to tackle on going issues in the area. | Maintain funding and operation of CCTV system. Make performance data available through yearly reports. |
| | | | |
| | | | |

| | | | |
|--|--|--|--|
| | | | |
|--|--|--|--|

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.

Letters circulated to residents to advise cameras are being monitored through the CCTV and CS team. North Ayrshire Council website provides information on location of cameras, statistics, privacy notice, Code of Practice and DPIA

Appropriate signage in and around the area where surveillance is taking place

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?

North Ayrshire Council 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. 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 Police/Council 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 your 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 monthly performance indicators along with information supplied by the police and other council departments. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012, SC Code of Practice and GDPR/DPA.

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

Footage is retained for 31 days and then automatically deleted unless stored in the evidence locker. This should give investigating authorities and Data Subjects sufficient time to request footage. Please see below.

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 in an evidence locker for more than 31 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceedings and Subject Access Requests. The evidence locker is reviewed by the manager on a monthly basis.

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 has multi layer password protected and use is subject to regular audits. The network has been upgraded and the system is security tested regularly.
DVD's are released to police officers, DVD's are released to third parties such as Insurance companies and solicitors via recorded delivery and email confirmation prior to disclosure of the encryption code. No international transfers are made.

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 Public Space 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 Ayrshire 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 complaints procedures.

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.

Other solutions are always considered including the use of additional council resources such as ASB officers, lighting changes and the use of private security before CCTV is used. Every deployment of CCTV is accompanied by a DPIA, public and stakeholder consultation Privacy zones can be programmed to cameras along with operator training and regular audits can help to mitigate any intrusion.

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 operation to do with Public Space CCTV 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 manager. North Ayrshire Council RIPSAs audit is carried out every three years.

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 |
|---|--|---|---------------------------------------|
| <p>Non Compliance of GDPR/DPA 2018. The GDPR/DPA sets out seven key principles which LA CCTV System owners must comply with whilst operating a Public Space Surveillance System:</p> <ul style="list-style-type: none"> • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability <p>Non compliance may result in prosecution, financial penalties and severe damage to the reputation of the local authority</p> | <p>Remote, possible or probable Possible</p> | <p>Minimal, significant or severe Significant</p> | <p>Low, medium or high Medium</p> |
| <p>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</p> <p>Article 6: the right to a fair trial</p> <p>Article 8: right to a private and family life</p> <p>Article 14: protection from discrimination</p> | <p>Possible</p> | <p>Significant</p> | <p>Medium</p> |

| | | | |
|---|----------|-------------|--------|
| <p>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</p> | | | |
| <p>Compliance with SC 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. Scottish Local Authorities will adopt these same rules. 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</p> <p>Reputational damage to Local Authority. The court may take inference in an authorities non compliance.</p> | Possible | Significant | Medium |
| <p>Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalites and severe damage to the reputation of the local authority</p> | 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 |
|---|---|--|--|
| <p>Unauthorised Disclosure Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the local authority</p> | <p>Remote, possible or probable Possible</p> | <p>Minimal, significant or severe Significant</p> | <p>Low, medium or high Medium</p> |
| <p>Misuse of Data 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</p> | <p>Possible</p> | <p>Significant</p> | <p>Medium</p> |
| <p>Harm to an individual Information unlawfully disclosed outwith Law Enforcement may result harm to any individuals identified if legislation was not followed.</p> | <p>Possible</p> | <p>Significant</p> | <p>Medium</p> |
| | | | |
| | | | |

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. | 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 SC Code of Practice and the Protection of Freedoms Act Management of system. | Reduced | Low | Yes |

| Options to reduce or eliminate risk | Effect on risk | Residual risk | Measure approved? |
|---|--|--------------------------------|-----------------------|
| <p>Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.</p> | <p>Eliminated reduced accepted Reduced</p> | <p>Low medium high Low</p> | <p>Yes/no Yes</p> |
| <p>Unauthorised Disclosure Release of data is strictly controlled by the council. Information Sharing Agreement 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.</p> | <p>Reduced</p> | <p>Low</p> | <p>Yes</p> |
| <p>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.</p> | <p>Reduced</p> | <p>Low</p> | <p>Yes</p> |
| <p>Financial Loss. Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. Regular audits are carried out by the system manager.</p> | <p>Reduced</p> | <p>Low</p> | <p>Yes</p> |
| | | | |

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: | Graham Emans, CCTV Co-ordinator 21/07/2020 | Integrate actions back into project plan, with date and responsibility for completion. |
| Residual risks approved by: | Linda Taylor, Legal Services 02/09/2020 | 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: | Kirsty Hamilton, Information Governance Team 21/07/2020 | DPO should advise on compliance and whether processing can proceed. |
| Summary of DPO advice : No concerns after updating Risks to include "harm to individual" | | |
| DPO advice accepted or overruled by: (specify role/title) | Janeine Barrett, Community Safety Senior Manager | If overruled, you must explain your reasons. |
| Comments: | | |

| | | |
|--|--|---|
| <p>Consultation responses reviewed by: Graham Emans, CCTV Co-ordinator</p> | | <p>If your decision departs from individuals' views, you must explain your reasons.</p> |
| <p>Comments: All consultation meetings positive.</p> | | |
| <p>This DPIA will be kept under review by: CCTV Manager</p> | | <p>The DPO should also review ongoing compliance with DPIA.</p> |

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 Estate | PTZ, FIXED | 119 | 24hr | 24hrs – regular camera patrols based upon risk and intelligence information | The privacy level expectation in residential streets is medium. These areas have appropriate signage for CCTV, its use, purpose and contact details. All recording and evidence downloads are secure and managed by the CCTV Manager and Police Staff. Regular audit checks are carried out on camera use in these areas. Privacy zones are programmed as and when required |
| Town Centre Shopping areas Public Car Parks | PTZ, FIXED | 29 | 24hrs | 24hrs – regular camera patrols based upon risk and intelligence information | The privacy level expectation in a town centre and public car parks is very low. These areas have appropriate signage for CCTV its use, purpose and contact details. All recording and evidence downloads are secure and managed by the CCTV Manager and Police Staff. . |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



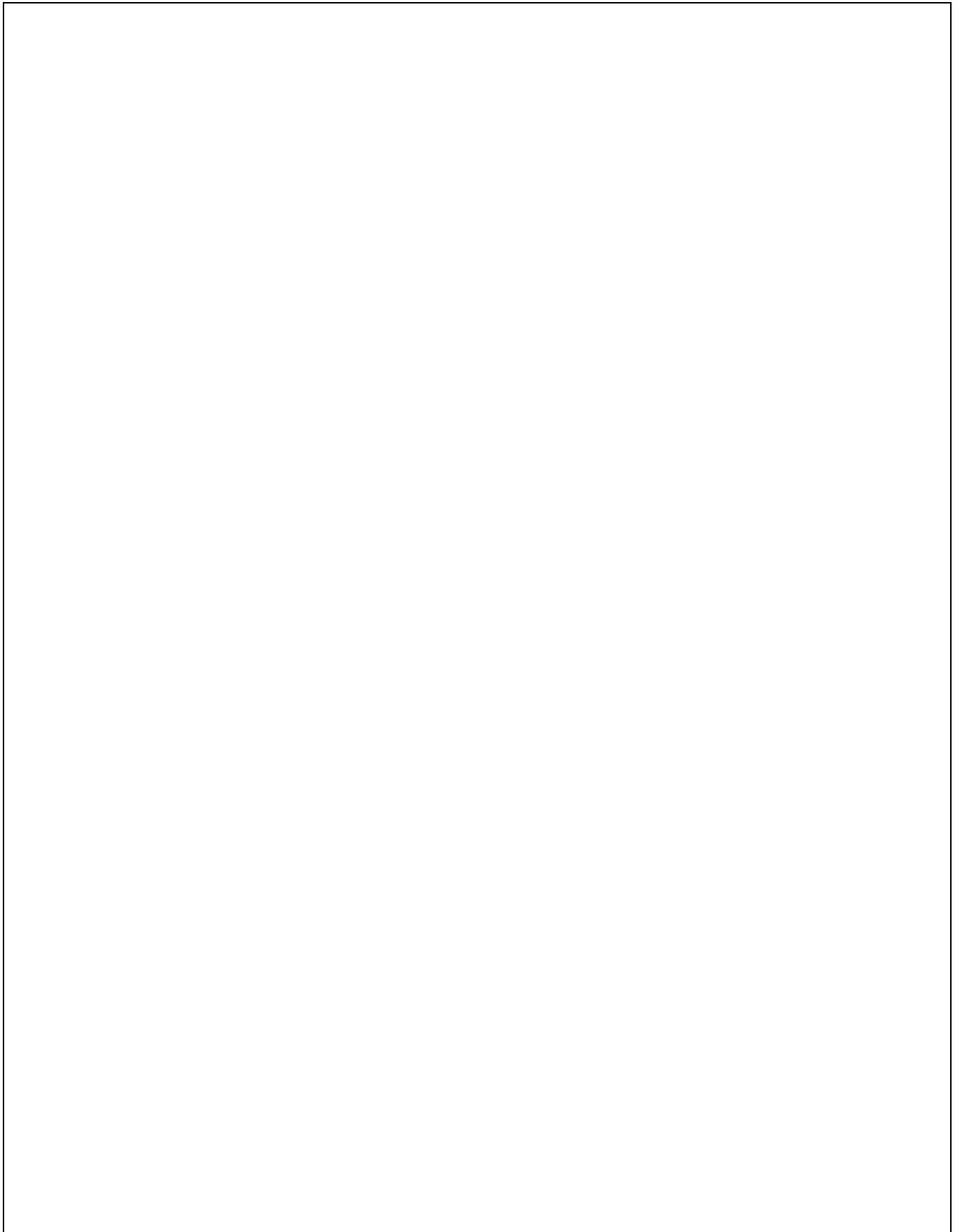
APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

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) | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

NOTES

A large, empty rectangular box with a thin black border, occupying most of the page. It is intended for handwritten or typed notes.

Date and version control: 19 May 2020 v.4

