National Cyber Security Authority

DPO DATA PROTECTION OFFICE

GUIDELINES ON THE USE OF CCTV AND AI-ENABLED VIDEO SURVEILLANCE SYSTEMS

- 2026 -

www.dpo.gov.rw

dpp@dpo.gov.rw

Toll free: 9080

Contents

1. Introduction 2
2. Scope and Application of these Guidelines 3
3. Lawful Basis, Necessity, and Proportionality 3
3.1 Purpose Limitation and Justification 3
3.2 Necessity and Proportionality 4
3.3 Legal Basis 4
3.4 Limitation of Scope 5
4. Camera Placement and System Configuration 5
4.1 Use of Private CCTV Systems and Impact on Neighbours 6
5. Transparency and Information 7
Standard CCTV Warning Sign (examples) 8
6. Retention, Access, Use and Disclosure of Footage 9
6.1 Retention 9
6.2 Access and Use 9
6.3 Disclosure 10
7. Rights of Individuals 10
8. AI-Enabled CCTV Systems 12
8.1 Differentiating levels of risk 12
8.2 Restrictions on Certain Practices 13
8.3 Enhanced Obligations for Controllers 14
9. Risk Assessment and DPIA 14
10. Security and Measures 15
11. Use of Data Processors in CCTV Surveillance (Outsourced Operations) 16
11.1 Determining roles and responsibilities 16
11.2 Data controller obligations when using processors 17
11.3 Minimum requirements for processor agreements 17
11.4 Security and access control in outsourced environments 17
11.5 Use of AI service providers 18
11.6 Ongoing oversight and monitoring 18
12. Accountability and governance 19
13. Supervision and Enforcement 20
Annex 1 – CCTV Compliance Checklist 21
Annex 2 – Data Processor Due Diligence Checklist 23

1. Introduction

The use of CCTV constitutes the processing of personal data under Law Nº 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (DPP Law). As such, it may have a direct and significant impact on individuals' rights and freedoms, including their privacy, autonomy, and ability to move freely without being subject to unjustified monitoring.

For the purpose of these Guidelines, Closed-Circuit Television (CCTV) refers to a system of cameras and associated equipment used to capture, transmit, monitor, or record images of individuals within a specific area. Such systems may operate continuously or at specific times and may include systems that allow live viewing, recording, storage, or analysis of video footage.

The presence of video surveillance, particularly in publicly accessible spaces, may influence how individuals act and interact. Accordingly, its deployment requires careful assessment and responsible use.

The increasing use of AI-enabled video surveillance systems further intensifies these concerns. Technologies enabling automated analysis—such as facial recognition, behavioural detection, and tracking—may result in systematic monitoring, profiling, and inference about individuals, often without their knowledge. Such processing carries heightened risks, including errors, bias, and disproportionate interference with fundamental rights, and therefore requires enhanced scrutiny and robust safeguards.

Under the DPP Law, the use of video surveillance systems must comply with the core data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, and accountability. The deployment of video surveillance must not be automatic or based solely on general security concerns. Controllers must be able to demonstrate, in each particular circumstance, that the use of CCTV serves a specific and legitimate purpose, is supported by a valid legal basis, and is necessary and proportionate to achieve that purpose, taking into account whether less intrusive measures could reasonably achieve the same objective.

The installation and operation of CCTV systems constitute the processing of personal data where individuals are identified or identifiable, directly or indirectly, including through the combination of footage with other data or through technological capabilities. This applies equally where identification results from AI-enabled functionalities, even in the absence of explicit recognition.

While video surveillance may serve legitimate purposes, such as ensuring safety and security, its use must remain targeted, limited, and proportionate, avoiding excessive or unjustified interference with individuals' rights.

These Guidelines are issued by the Data Protection and Privacy Office of Rwanda and aim to:

- clarify the application of the DPP Law to CCTV and AI-enabled video surveillance systems;
- provide practical and operational guidance to data controllers and processors; and
- support consistent, lawful, and accountable use of video surveillance in practice.

At the same time, these Guidelines are designed to be practical and operational, enabling controllers and processors to understand and implement their obligations in real-world contexts.

2. Scope and Application of these Guidelines

These Guidelines apply to the use of **CCTV and AI-enabled video surveillance systems (**hereafter referred to as "video surveillance systems") where such use involves the processing of personal data. This includes live viewing without recording, temporary or mobile cameras, doorbell cameras, dashcams, and CCTV systems operated through mobile applications.

They apply to all **data controllers and data processors operating in Rwanda**, across both public and private sectors, regardless of the technology used or the organisational setting in which processing takes place.

These Guidelines cover a wide range of real-life environments, including:

- commercial premises and retail environments;
- public-facing facilities and infrastructure;
- workplaces and office environments;
- residential buildings and shared spaces;
- public or semi-public environments where individuals may reasonably expect a degree of privacy.

This list is illustrative and not exhaustive.

These Guidelines do not apply to:

- **Body-worn cameras**, including those used by law enforcement, which are subject to specific legal and regulatory frameworks;
- **Covert surveillance** carried out for criminal investigations or national security purposes, which is governed by separate legal frameworks;
- **Purely personal or household use of CCTV**, provided that:
  - ✓ the use remains strictly within a personal or domestic context; and
  - ✓ it does not extend to monitoring individuals outside the household, including neighbours, shared spaces, or public areas.

Where such use affects individuals beyond the household context, data protection requirements may apply, as further addressed in Section 4.1 of these Guidelines.

3. Lawful Basis, Necessity, and Proportionality

The use of CCTV must always be grounded in a clearly defined purpose and a valid legal basis. The use of video surveillance systems is inherently intrusive and must therefore be treated as an exceptional measure, not a routine or default solution.

3.1 Purpose Limitation and Justification

Data controllers must first identify the specific problem or risk they aim to address and clearly define the specific purpose for which CCTV is intended before deployment. Video surveillance may only be deployed where there is a real, specific, and evidenced need, such as:

- repeated security incidents;
- identifiable vulnerabilities;

- documented risks to individuals or property.

The mere possibility of risk or general preventive monitoring is not sufficient to justify the use of CCTV.

CCTV may only be used for specific, explicit, and legitimate purposes, including:

- protection of individuals and property;
- security of premises;
- prevention or detection of clearly identified risks or criminal activity;
- public safety in defined contexts.

Broad or undefined purposes (e.g. general monitoring, behavioural observation, or "oversight") are not acceptable.

3.2 Necessity and Proportionality

Before installing CCTV, data controllers must assess whether:

- the use of video surveillance is necessary to achieve the intended purpose; and
- less intrusive measures (e.g. physical security, lighting, access controls) could reasonably achieve the same objective.

Where less intrusive alternatives are available and effective, CCTV must not be used.

3.3 Legal Basis

The use of CCTV must be based on a valid legal ground under Article 46 of the DPP Law, identified prior to deployment.

Typically:

- **Public authorities** rely on legal obligations or public interest (Article 46.5 of the DPP Law);
- **Private entities** rely on legitimate interests (Article 46.7 of the DPP Law).

Where legitimate interests are relied upon, data controllers must conduct and document a balancing test, demonstrating that:

- The interest pursued is legitimate and clearly defined;
- CCTV is necessary to achieve that interest;
- The impact on individuals' rights and freedoms does not override the controller's interest, taking into account the nature of the area monitored, the level of intrusion, and expectations of individuals;
- appropriate safeguards are in place;

As a general rule, **consent will not be an appropriate legal basis** for CCTV, given that individuals are rarely in a position to freely refuse surveillance in most environments.

3.4 Limitation of Scope

CCTV deployment must be strictly limited:

- **geographically** – to areas where risks are identified;
- **temporally** – to periods where monitoring is necessary;
- **functionally** – to the specific purpose defined.

Practical guidance

Do

✔ Clearly define the purpose before CCTV installation

✔ Base CCTV deployment on evidence (e.g., incidents, risk assessments)

✔ Complete and retain a CCTV purpose and necessity assessment, documenting the intended purpose, evidence of need, legal basis, consideration of less intrusive alternatives, and proportionality of the proposed surveillance.

Don't

✘ Install CCTV as a precautionary or default measure

✘ Use CCTV for vague or undefined purposes

✘ Rely on consent where individuals cannot freely refuse

Practical examples

Acceptable: CCTV installed at a warehouse entrance following repeated theft incidents, supported by a documented risk assessment.

Not acceptable: CCTV used for continuous monitoring of employees without specific justification or evidence of risk.

4. Camera Placement and System Configuration

In accordance with the principle of data minimisation, and the requirements of necessity and proportionality set out in Section 3, video surveillance systems must be designed and configured to limit processing to what is strictly necessary for the defined purpose.

Cameras must:

- be directed only at areas relevant to the specified purpose;
- avoid capturing neighbouring properties or public spaces, unless this is strictly necessary and justified;
- be positioned and adjusted to reduce unnecessary or excessive monitoring.

Certain areas must **never** be subject to video surveillance, including:

- sanitary facilities and changing rooms;
- private or sensitive spaces where individuals have a high expectation of privacy (e.g. hotel rooms or private living areas).

Data controllers must also ensure appropriate technical configuration of systems, including:

- applying masking or blurring to exclude irrelevant areas;
- limiting or disabling features such as zoom, tracking, or continuous monitoring where not necessary;
- disabling audio recording, unless it is clearly justified, lawful, and proportionate.

Audio can be more intrusive than video and may capture conversations unrelated to the security purpose. Consider stating that audio should be switched off by default and, where exceptionally proposed, the controller should separately document the necessity, legal basis, proportionality, notice and safeguards. Please ensure this wording is consistent with the applicable law.

Practical guidance

Do

✔ Focus cameras on entry points, exits, and critical areas

✔ Configure systems to minimise data collection

Don't

✘ Capture entire streets, residential windows, or unrelated areas

✘ Use high-intensity monitoring (zoom/tracking) without necessity

Practical examples

Acceptable: Camera at shop entrance after incidents or CCTV in parking areas for safety

Not acceptable: Continuous employee monitoring; capturing neighbouring homes or facial recognition in public spaces

4.1 Use of Private CCTV Systems and Impact on Neighbours

The use of CCTV systems by individuals for personal or household purposes must respect the privacy and rights of others. Even where such use falls within a personal or domestic context, positioning and operation of cameras should not unnecessarily intrude into neighbouring properties or shared spaces.

Individuals using private CCTV systems should:

- position cameras to monitor only their own property, entrances, or immediate surroundings;
- Avoid capturing neighboring homes, private gardens, balconies, or windows. Ensure cameras are not used in ways that could be perceived as neighbor surveillance;
- limit the field of view to what is strictly necessary for security purposes;
- use technical measures (e.g. masking, blurring, restricted angles) to exclude areas not relevant to the intended purpose;

Where surveillance of areas beyond one's property is unavoidable (e.g. shared entrances or common spaces), individuals should:

- assess whether such monitoring is necessary and proportionate;
- minimise the scope and duration of recording;

- consider informing affected individuals where appropriate.

Practical guidance

Do

✔ Install cameras facing your own entrance, gate, or driveway.

✔ Adjust angles to minimise incidental capture of neighbouring areas and #use privacy masking features where available.

Don't

❌ Direct cameras toward neighbours' windows, gardens, or private spaces.
❌ Monitor shared spaces in a way that is excessive or unjustified.

❌ Use CCTV for purposes beyond security (e.g. observing or tracking neighbours).

Practical Examples

Acceptable:

A homeowner installs a CCTV camera to monitor their front entrance. Due to the layout of the property, a small portion of a shared entrance is also captured. The homeowner adjusts the camera angle and applies privacy masking to minimise the area captured, limits recording to what is necessary, and informs affected individuals where appropriate.

Not acceptable: A camera is directed toward a neighbour's backyard or window, enabling observation of their daily activities.

5. Transparency and Information

Transparency is a fundamental requirement for the lawful use of video surveillance systems. Individuals must be informed, in a clear and timely manner, that they are subject to video and, where applicable, audio surveillance.

Data controllers must ensure that:

- signage is visible, clear, and positioned before individuals enter the monitored area;
- individuals can easily understand that surveillance is taking place and identify the data controller responsible.

As a minimum, CCTV signage must include:

- a clear indication that video surveillance is in operation;
- the identity of the data controller.

In addition to signage (first-layer information), data controllers must make further information available through accessible means (second-layer information), such as websites or on-site information points. This should include:

- the purpose of the surveillance;

- contact details of the data controller (and, where applicable, the data protection officer);
- information on individuals' rights;
- retention period or criteria used to determine it.

Practical guidance

Do ✔ Place clear signage at all entrances to monitored areas ✔ Ensure information is easy to understand Don't ✘ Use hidden cameras in ordinary contexts

Standard CCTV Warning Sign (examples)







6. Retention, Access, Use and Disclosure of Footage

Footage generated by video surveillance systems must be managed under strict control throughout its lifecycle, including storage, access, use, and disclosure, in accordance with the principles of data minimisation, storage limitation, and integrity and confidentiality.

6.1 Retention

Footage must be retained only for as long as necessary to fulfil the purpose for which it was collected, in accordance with the principle of storage limitation.

Retention periods must be:

- limited, defined, and justified;
- proportionate to the purpose of processing;
- based on a case-by-case assessment of necessity.

In practice, short retention periods will generally be sufficient for most video surveillance systems. As a general benchmark, this is not a statutory retention period or automatic safe harbour. Controllers should determine and document a period based on the purpose, risks and operational context;

- retention periods of **7 to 14 days** will often be appropriate in standard security contexts;
- shorter periods (e.g. a few days) may be sufficient where risks are limited.

Retention periods approaching **30 days** are not prohibited, but will require **specific, clear, and documented justification**, based on concrete circumstances (e.g. nature of risks, operational needs, or legal obligations).

Where an incident occurs, only the relevant footage may be retained for a longer period, for purposes such as investigation, legal proceedings, or compliance with legal obligations.

Data controllers must implement automatic deletion mechanisms to ensure that footage is not retained longer than necessary.

6.2 Access and Use

Access to video surveillance systems and stored footage must be strictly controlled.

Access must be:

- restricted to authorised personnel only;
- based on clearly defined roles and responsibilities;
- granted on a need-to-know basis;
- logged and auditable to ensure full traceability.

Data controllers must implement procedures to ensure that access is regularly reviewed and revoked where no longer necessary.

Footage must be used only for the purpose for which it was originally collected and must not be used for unrelated or incompatible purposes.

6.3 Disclosure

Disclosure of footage to third parties is permitted only where it is:

- required by law (e.g. lawful requests from law enforcement authorities); or
- necessary and proportionate for a legitimate and clearly defined purpose, in line with the original purpose of collection.

All disclosures must be:

- documented and traceable;
- based on a clearly identified legal basis;
- limited to what is strictly necessary.

Footage must not be:

- shared informally or without proper authorisation;
- used for personal purposes;
- disclosed publicly (e.g. through social media or other public channels).

Practical guidance

Do
- ✔ Define retention periods (e.g. 7–14 days for routine footage)
- ✔ Automatically delete footage when no longer needed
- ✔ Restrict access and maintain logs
- ✔ Share footage only upon lawful request

Don't
- ✘ Retain footage indefinitely
- ✘ Allow unrestricted access
- ✘ Use or share footage for unrelated purposes

7. Rights of Individuals

The lawful and justifiable use of video surveillance systems must not undermine individuals' ability to exercise their data protection rights effectively. Given the nature of video surveillance—where individuals may not always be aware of when or how they are recorded—data controllers must take proactive and practical measures to ensure that these rights can be exercised in a meaningful and accessible manner.

At a minimum, individuals have the right to:

- obtain access to their personal data, including footage in which they appear;
- request erasure of footage, where the legal conditions are met (e.g. where retention is no longer necessary, or the processing is unlawful);
- object to processing, particularly where surveillance is based on legitimate interests.

To ensure the effective exercise of these rights, data controllers must establish appropriate procedures and technical capabilities.

In accordance with Articles 18, 19 and 23 of the DPP Law, individuals may exercise their rights to access their personal data, object to processing, and request erasure, where the legal conditions are met. Data controllers must respond to requests within thirty (30) days of receipt, in accordance with the applicable provisions of the Law and the relevant guidance issued by the supervisory authority.

Data controllers should assist individuals in identifying the relevant footage where the information initially provided is insufficient. They may request additional information where reasonably necessary to locate the footage or verify the requester's identity. However, such requests must be proportionate and must not create an unnecessary or excessive burden on the individual.

In particular, data controllers must:

- define clear internal workflows for handling requests, including roles and responsibilities;
- implement systems that enable efficient searching, identification, and extraction of relevant footage (e.g. based on time, location, or other reasonable criteria);
- verify the identity of the requester in a proportionate manner;
- respond within applicable legal timeframes;
- provide footage in a format that is accessible and secure;
- maintain records of requests and responses for accountability purposes.

Controllers must not place an unreasonable burden on individuals, such as requiring excessive detail, disproportionate proof, or impractical steps to exercise their rights.

Where footage contains images of multiple individuals, data controllers must balance the rights of the requesting individual with the rights and freedoms of others.

To enable disclosure while protecting third parties, controllers must implement appropriate technical measures, such as:

- blurring or masking other individuals;
- redacting or limiting parts of the footage where necessary.

In exceptional cases, access may be refused or restricted where:

- disclosure would disproportionately affect the rights of others; and
- no reasonable technical solution (e.g. anonymisation) is available.

Practical guidance

Do

✔ Facilitate requests in a practical and user-friendly manner

✔ Use technical tools (e.g. blurring) to enable disclosure

✔ Keep records of requests and responses

Don't

✘ Refuse requests solely because footage contains other individuals

✘ Require excessive or unnecessary information from the requester

✘ Delay responses due to lack of internal procedures or system capability

8. AI-Enabled CCTV Systems

The use of AI-enabled video surveillance systems represents a significant evolution in surveillance practices, moving from passive recording to automated analysis and, in some cases, decision-making. While such technologies may enhance security and operational efficiency, they also introduce substantially higher risks to individuals' rights and freedoms.

In particular, AI-enabled functionalities may enable:

- continuous or large-scale monitoring;
- inference about individuals' behaviour, characteristics, or intentions;
- identification or tracking of individuals across locations or over time.

These capabilities significantly increase the risk of intrusive and disproportionate surveillance, as well as the likelihood of:

- errors and inaccurate outcomes;
- bias and discriminatory effects;
- reduced transparency and limited ability for individuals to understand or challenge the processing.

These risks are particularly acute where individuals are unaware of, or unable to meaningfully contest, such processing.

As a result, the use of AI in video surveillance systems requires:

- a higher threshold of necessity and justification;
- the implementation of enhanced safeguards; and
- stronger accountability and oversight measures.

8.1 Differentiating levels of risk

Not all AI-enabled functionalities present the same level of risk. Data controllers must assess and distinguish between different types of AI use, taking into account their impact on individuals' rights and freedoms.

Lower-risk uses (generally acceptable with safeguards)

Lower-risk uses typically involve non-identifying or aggregated analyses, in which individuals are not identified or profiled. However, the fact that a system produces anonymous, aggregated, or non-identifying outputs does not necessarily mean that no personal data is processed. Data

controllers must assess the entire processing operation, including the initial collection of video footage, any intermediate analysis or data generated, and the final outputs. This assessment should establish whether individuals are identified or identifiable at any stage of the processing, including through the use of additional information or technological capabilities. Where personal data is processed, the requirements of the DPP Law continue to apply. Examples include:

- motion detection;
- counting individuals;
- analysis of crowd density or queue management, without identifying individuals.

Such uses may be acceptable, provided that:

- they do not enable identification, tracking, or profiling of individuals; and
- appropriate technical and organisational safeguards are in place.

Higher-risk uses (requiring strict scrutiny)

Higher-risk uses involve identification, tracking, or behavioural inference, including:

- facial recognition;
- behavioural profiling or anomaly detection;
- tracking individuals across different locations, cameras, or over time.

These uses are inherently more intrusive and may result in systematic monitoring or profiling, with significant impacts on individuals' rights and freedoms.

As such, they require:

- strict necessity and proportionality;
- a clear and valid legal basis;
- enhanced safeguards and oversight.

8.2 Restrictions on Certain Practices

In line with international best practice, and unless explicitly authorised by law, certain uses of AI in video surveillance will generally be considered disproportionate.

In particular:

- the use of real-time facial recognition in public or publicly accessible spaces should not be deployed, given its highly intrusive nature and potential to enable mass surveillance;
- large-scale or continuous tracking of individuals across locations should not be carried out, particularly where it enables profiling or behavioural analysis.

Data controllers must approach such use cases with extreme caution and should assume that, in most contexts, they will not meet the threshold of necessity and proportionality.

8.3 Enhanced Obligations for Controllers

Where AI-enabled video surveillance systems are deployed, data controllers must implement additional safeguards, including:

- conducting a Data Protection Impact Assessment (DPIA) prior to deployment, with specific attention to risks arising from automated analysis and inference;
- ensuring meaningful human oversight, so that decisions are not based solely on automated processing;
- validating the accuracy, reliability, and performance of the system, including through regular testing and monitoring;
- identifying and mitigating risks of bias, discrimination, or unfair outcomes, particularly where individuals are classified or assessed;
- ensuring an appropriate level of transparency regarding the use of AI functionalities, where feasible and proportionate.

Practical guidance

Do

✔ Use AI for non-identifying, aggregated purposes (e.g. counting visitors, managing queues)
✔ Carry out a DPIA that specifically addresses AI-related risks
✔ Regularly test systems for accuracy and unintended bias

Don't

✘ Use AI to identify or track individuals without a clear legal basis and strong justification
✘ Deploy systems that enable continuous or large-scale profiling
✘ Rely solely on automated outputs without human review

Practical examples

Acceptable: A shopping center using AI to count visitors entering the premises and optimise staffing levels is acceptable.

Not acceptable: A system that identifies individuals and tracks their movement across multiple locations to analyse behaviour represents a high risk and is likely unlawful.

9. Risk Assessment and DPIA

Given the inherently intrusive nature of video surveillance, controllers are expected to adopt a risk-based approach, assess the impact of CCTV systems before deployment, and, where necessary, throughout their lifecycle.

A DPIA is required where processing is likely to result in a high risk to the rights and freedoms of individuals. This will typically be the case where:

- CCTV monitors public or publicly accessible spaces;
- AI-enabled or advanced analytics technologies are used;

- monitoring is systematic, continuous, or large-scale;
- Individuals may not reasonably expect to be monitored.

In practice, most deployments involving public environments or AI functionalities should be presumed to require a DPIA.

A DPIA is not a purely formal exercise, but a practical decision-making tool. It should enable controllers to determine whether the intended use of CCTV is justified and, if so, under what conditions.

At a minimum, the DPIA must:

- clearly describe the intended processing (location, scope, technology used);
- assess the necessity and proportionality of CCTV in relation to its purpose;
- identify and evaluate the risks to individuals, including risks of intrusion, misuse, or unjustified monitoring;
- define concrete mitigation measures to reduce those risks.

Where the DPIA indicates that high risks cannot be sufficiently mitigated, controllers should reconsider or refrain from deploying the system. For further information, check the guidance note on the DPIA at https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_dpia-guide-and-form.pdf

Practical guidance

Do
- ✔ Conduct the DPIA at an early stage, before installing cameras
- ✔ Consider realistic risks (e.g., misuse, over-monitoring, identification)
- ✔ Use the DPIA to adjust system design (e.g., camera angles, retention periods)

Don't
- ✘ Treat the DPIA as a formal or "tick-box" exercise
- ✘ Proceed with deployment where high risks remain unaddressed
- ✘ Copy generic DPIAs without assessing the specific context

10. Security and Measures

The use of video surveillance systems requires data controllers to implement appropriate technical and organisational measures to ensure the security of personal data and to demonstrate compliance with data protection requirements, in accordance with the principles of integrity, confidentiality, and accountability.

Security measures must be proportionate to the nature, scope, context, and risks of the processing, and must address both technical vulnerabilities and human factors, including the risk of internal misuse.

At a minimum, data controllers must ensure:

- secure storage of footage, including protection against loss, alteration, or unauthorised access;
- strict access controls, based on clearly defined roles and responsibilities;
- implementation of audit logs, ensuring traceability of access, use, and disclosure of footage;
- protection against unauthorised access, including cybersecurity risks and insider threats.

Particular attention must be paid to higher-risk configurations, including:

- remote access systems, especially where access is provided over external networks;
- cloud-based storage or processing, including risks related to external hosting and cross-border access;
- shared or outsourced operations, where multiple parties may have access to footage or systems.

Where such arrangements are in place, data controllers must ensure that appropriate safeguards are implemented, including secure authentication, encryption, and ongoing monitoring of access and system activity.

11. Use of Data Processors in CCTV Surveillance (Outsourced Operations)

In many cases, CCTV systems are not operated solely by the data controller, but involve external service providers, such as:

- security companies monitoring live feeds;
- IT providers managing storage or infrastructure;
- cloud service providers hosting footage;
- vendors providing AI-enabled analytics or system maintenance.

Where such third parties process personal data on behalf of the data controller, they act as data processors and must comply with the applicable data protection requirements.

Data controllers remain fully responsible and accountable for the processing, including where operations are outsourced.

11.1 Determining roles and responsibilities

Before engaging any external provider, data controllers must assess the role of that provider based on the actual activities performed and the extent to which it determines the purposes and essential means of processing personal data.

A provider is not automatically considered a data processor merely because it supplies, installs, maintains, or services CCTV equipment. Where a provider only supplies equipment or provides technical support without accessing or otherwise processing personal data on behalf of the controller, it may not qualify as a data processor.

However, where the provider accesses, views, stores, or otherwise processes CCTV footage on behalf of the controller and under the controller's instructions, it may qualify as a data processor and must comply with the applicable data protection requirements.

Where a provider processes personal data for its own purposes, its role must be assessed accordingly. Data controllers must clearly establish and document the roles and responsibilities of each provider before engaging them.

11.2 Data controller obligations when using processors

Where a data processor is engaged, the data controller must:

- select processors that are registered as such with the DPO and provide sufficient guarantees of compliance, including technical and organisational security measures;
- ensure that processing is governed by a written contract or legal act;
- provide documented instructions on how the CCTV data may be processed;
- maintain oversight and ensure that processing remains aligned with the original purpose.

Outsourcing does not reduce the data controller's obligations. The data controller must be able to demonstrate compliance at all times, including in relation to processor activities.

11.3 Minimum requirements for processor agreements

Contracts between data controllers and data processors must clearly define:

- the subject matter and duration of processing;
- the nature and purpose of CCTV processing;
- the types of data processed (e.g., video footage);
- the obligations and rights of the controller;
- confidentiality obligations for personnel;
- security measures to be implemented;
- conditions for engaging sub-processors;
- procedures for assisting the controller in:
    - responding to data subject requests;
    - handling data breaches;
    - conducting DPIAs where required.

Data processors must act only on documented instructions from the controller and must not use CCTV data for their own purposes.

For further information, consult the guide on contractual provisions for processing at https://dpo.gov.rw/fileadmin/DPO/ComplianceTools/-_Guide-On-Contractual-Provisions-For-Processing-Of-Personal-Data__2_.pdf

11.4 Security and access control in outsourced environments

Where CCTV processing is outsourced, particular attention must be paid to:

- remote access to live feeds or recordings;

- storage of footage in external or cloud-based systems;
- cross-border access or transfers (where applicable);
- the risk of unauthorised access by processor personnel.

Data controllers must ensure that:

- access is strictly limited and role-based;
- all access is logged and auditable;
- appropriate encryption and security safeguards are in place;
- Data processor staff are subject to confidentiality obligations and training.

11.5 Use of AI service providers

Where AI-enabled video surveillance systems are provided or managed by external vendors, data controllers must exercise heightened due diligence, including:

- understanding how the system processes and analyses data;
- ensuring that the data processor does not use the data for its own purposes (e.g. training algorithms without authorisation);
- verifying safeguards related to accuracy, bias, and transparency;
- ensuring that meaningful human oversight remains with the controller.

11.6 Ongoing oversight and monitoring

Data controllers must not treat outsourcing as a one-time compliance step. Instead, they should ensure continuous oversight, including:

- periodic review of data processor performance and compliance;
- audits or checks where appropriate;
- updating contractual arrangements where systems or risks change;
- ensuring alignment with DPIAs and internal policies.

Practical guidance

Do

✔ Use written contracts with clear data protection clauses
✔ Choose processors with proven registration as a processor and relevant security and compliance capabilities
✔ Monitor and review processor activities regularly
✔ Ensure clear instructions and limitations on data use

Don't

✘ Assume that outsourcing transfers responsibility
✘ Allow processors to use CCTV data for their own purposes
✘ Grant unrestricted or unmonitored access to footage
✘ Use providers whose processing cannot be explained or audited

Practical examples

Acceptable: A company contracts a security provider that is registered with the DPO as a processor to monitor CCTV. The contract clearly defines roles, restricts access to authorized staff, and requires logging and confidentiality.

Not acceptable: A company uses a cloud provider to store footage without checking if it is registered as a processor and without clear contractual safeguards. This provider allows broad internal access and utilizes the data to enhance its own AI systems.

12. Accountability and governance

Beyond implementing the security measures set out in Section 10, data controllers must be able to demonstrate compliance in practice, in accordance with the principle of accountability.

This requires the establishment of appropriate governance frameworks, ensuring that the use of video surveillance systems is properly documented, controlled, and subject to oversight.

At a minimum, data controllers must:

- maintain a CCTV register, documenting key elements such as system locations, purposes, retention periods, and main system characteristics;
- conduct and retain Data Protection Impact Assessments (DPIAs) where required;
- adopt and implement internal policies and procedures governing the use of video surveillance systems, including access control, use of footage, and handling of incidents or requests;
- ensure that all personnel with access to video surveillance systems are appropriately trained, aware of their responsibilities, and subject to confidentiality obligations.

Accountability also requires that video surveillance systems are subject to regular review, to ensure that:

- their use remains necessary and proportionate in light of the original purpose;
- system configurations and safeguards remain effective and appropriate;
- any changes in context, risk, or technology are properly assessed and reflected in updated measures, including DPIAs where applicable.

Practical guidance

Do

✔ Restrict access to a limited number of trained personnel
✔ Regularly review who has access and why
✔ Keep clear records (register, logs, policies)

Don't

✘ Allow shared or uncontrolled access to CCTV systems
✘ Neglect security of remote or cloud-based systems
✘ Treat CCTV as a "set and forget" system without review

13. Supervision and Enforcement

The Data Protection and Privacy Office of the NCSA is responsible for overseeing the application of these Guidelines and ensuring compliance with the data protection framework.

In exercising its mandate, the DPO may:

- conduct inspections and investigations, including on-site assessments of video surveillance systems;
- request information and documentation (e.g. DPIAs, CCTV registers, policies, and procedures);
- issue recommendations and require corrective measures, including modifications to system configuration or operation;
- order the restriction, suspension, or cessation of processing where it is found to be unlawful, disproportionate, or otherwise non-compliant;
- impose administrative sanctions, in accordance with the law.

Data controllers must cooperate fully with the supervisory authority and must be able to demonstrate compliance with these Guidelines and the applicable legal requirements upon request.

Annex 1 – CCTV Compliance Checklist

Before installation

- **Purpose of surveillance:** What specific purpose is the CCTV system intended to achieve?
- **Evidence of need:** What incidents, risks, or vulnerabilities justify the use of CCTV?
- **Area to be monitored:** Which specific areas will be covered by the cameras?
- **Legal basis:** What legal basis under Article 46 of the DPP Law supports the processing?
- **Less intrusive alternatives:** What alternative measures have been considered, and why are they insufficient?
- **Necessity and proportionality:** Why is CCTV necessary, and how will its impact on individuals' rights be minimised?
- **Safeguards:** What measures will be implemented to protect the personal data collected?
- **Review:** When will the necessity and continued use of the CCTV system be reviewed?
- Legitimate interest assessment conducted (where applicable)
- DPIA conducted where required

System design and configuration

- Cameras limited to areas strictly necessary for the purpose
- No monitoring of private or sensitive spaces
- Field of view minimised to avoid capturing irrelevant areas
- Masking or blurring applied where appropriate
- Audio recording disabled, unless clearly justified and lawful
- High-risk features (e.g. tracking, AI functionalities) assessed and limited

Transparency

- Clear and visible signage installed at all entry points
- Signage includes minimum required information
- Additional (layered) information available (e.g. website, reception)
- Contact details and rights information accessible

Operation and retention

- Retention period defined, justified, and documented
- Retention aligned with purpose (e.g. typically short-term)
- Automatic deletion mechanisms implemented
- Incident-related footage handled separately and securely

Access and Use

- Access restricted to authorised personnel
- Role-based access controls implemented

- Access and use logged and auditable
- Use limited strictly to defined purposes

Rights of Individuals

- Procedure for handling access/erasure/objection requests in place
- Ability to search, identify, and extract relevant footage
- Identity verification procedures defined and proportionate
- Technical tools available (e.g. blurring/masking)
- Requests and responses documented

Security

- Secure storage of footage ensured
- Protection against unauthorised access (internal and external)
- Authentication and access controls implemented
- Audit logs maintained
- Additional safeguards for remote/cloud systems

Governance and Accountability

- CCTV register maintained and regularly updated
- DPIAs documented and reviewed where necessary
- Internal policies and procedures adopted
- Staff trained and bound by confidentiality
- Periodic review of necessity and proportionality conducted

Annex 2 – Data Processor Due Diligence Checklist

1. Role and Qualification of Data Processor

- Data processor role clearly defined (controller vs processor distinction confirmed)
- Data processor provides sufficient guarantees of compliance
- Data processor's experience and technical capability assessed

2. Legal and Contractual Framework

- Written contract or legal act in place
- Roles and responsibilities clearly defined
- Purpose and scope of processing specified
- Instructions documented and binding
- Sub-processing conditions clearly regulated

3. Data Protection Safeguards

- Data processor does not use data for its own purposes
- Confidentiality obligations imposed on staff
- Assistance with data subject rights ensured
- Assistance with data breaches and DPIAs included

4. Security Measures

- Technical and organisational measures verified
- Access controls and authentication mechanisms in place
- Logging and monitoring capabilities ensured
- Encryption and secure storage applied (where appropriate)

5. Access and Control

- Access limited to authorised personnel
- Remote access controlled and secured
- Cross-border access assessed (if applicable)

6. Oversight and Accountability

- Audit rights included in contract
- Monitoring and review mechanisms in place
- Data processor performance periodically assessed
- Clear procedures for termination and data return/deletion