An Post CCTV Policy

Prepared by	Data Privacy Office
Date first issued	May 2017
Last updated	February 2024
Version	1.5
Document Classification	For Publication on An Post Intranet

Document Control

Version History

Version	Date Released/Reviewed	Contributor(s)	Description
1.0	May 2017	An Post Legal, Security Services and HR department in conjunction with the An Post Group of Unions	CCTV Policy – Policy on the use of CCTV in An Post and its Contractors
1.1	July 2019	Data Privacy Office	Added cover sheet – Updates required for GDPR
1.2	June 2020	Data Privacy Office, An Post Security Services	Revised Policy to take account of the 'open counter environment' and the siting of CCTV cameras behind the counters
1.3	October 2021	Data Privacy Office	No further updates
1.4	October 2022	Data Privacy Office	Updated with Grant Thornton Suggestions
1.5	February 2024	Security Services, HR and Data Privacy	Updated following engagement with Unions

Document Approval

Approved by	Position	Date
Frank Ennis	An Post Data Protection Officer	July 2019
Frank Ennis	An Post Data Protection Officer	June 2020
Frank Ennis	An Post Data Protection Officer	October 2021
Frank Ennis	An Post Data Protection Officer	October 2022
John Twomey Frank Ennis	Head of Security Services An Post Data Protection Officer	February 2024

Distribution List

Distributed to	Organisation	Position	Date
Company Secretary's Office	An Post	Company Secretary	February 2024
Legal	An Post	Company Solicitor	February 2024
Security Services	An Post	Head of Security	February 2024
HR	An Post	Head of Employee Relations	February 2024
Intranet	An Post	N/A	February 2024

POLICY ON THE USE OF CLOSED CIRCUIT TELEVISION (CCTV) SYSTEMS IN AN POST AND ITS CONTRACTORS

INTRODUCTION

Closed circuit television (CCTV) systems are installed in Retail, Mails and other premises under the remit of An Post. The rules applicable to the processing of information about individuals recorded on CCTV are covered under applicable data protection laws ("Data Protection Legislation"). Data Protection Legislation contain obligations regarding the use of CCTV and also give individuals certain rights in connection with their personal data.

1. PURPOSE OF THE POLICY

The purpose of this policy is to regulate the use of An Post owned and third party owned CCTV and its associated technology under the remit of An Post and its Postmasters in the monitoring of all the internal and external environs of premises both where An Post business is conducted and whether the premises is owned by An Post or a Postmaster (the "Premises"). The policy sets out the clear and lawful basis for the processing of any personal data gathered on CCTV and the handling of that data. Any personal data which is obtained by An Post as a result of the operation of the CCTV system will be treated in accordance with Data Protection Legislation.

CCTV systems are installed both internally and externally in premises for the purpose of enhancing security of the building and its associated equipment as well as creating an awareness among the occupants, at any one time that a surveillance security system is in operation within and/or in the external environs of the premises.

2. PROCESSING PURPOSES

CCTV systems are installed both internally and externally at the Premises for the following legitimate business purposes of An Post:

- **Security and prevention of crime.** For the purpose of enhancing security of the premises and the associated equipment and for the detection and investigation of crime, the apprehension and prosecution of offenders and the protection of property.

- **Promotion of safety and customer service.** For the purpose of monitoring and resolving traffic management issues

- **Ensuring** public and staff safety, investigating accidents and near misses and dealing with customer complaints about service.

CCTV will not be used for the day to day supervision of employees and any material which has been viewed may only be referred to in the context of the objectives set out above. An Post CCTV systems do not contain audio recording facilities.

3. SCOPE

This policy applies to the use of CCTV footage on An Post premises and relates directly to the location and use of CCTV systems and the monitoring, recording and subsequent use of such recorded material.

The policy also covers the use of camera related surveillance equipment such as Automatic Number Plate Recognition (ANPR). The ANPR only uses licence plates to facilitate the lifting of the barrier for automatic entry to certain mail centres.

This policy also applies to CCTV footage and systems contained in company vehicles as well as the use of CCTV footage for investigation of accidents and related claims.

4. GENERAL PRINCIPLES

An Post is committed to ensuring that recording and monitoring is conducted in a professional, ethical and legal manner and in accordance with data protection principles under Data Protection Legislation.

Information obtained through CCTV recording may only be released when authorised by An Post Head of Security, a Business Development Manager, an Area Manager, a HR Manager or Level One or Two Manager as appropriate to the circumstances under enquiry.

CCTV monitoring is limited to uses that do not violate the reasonable expectation to privacy. It will be conducted in a manner consistent with all existing policies adopted by An Post including Equality & Diversity Policy, Disciplinary Policies and the Dignity at Work Policy.

Information accessible on CCTV Monitors and/or recorded on CCTV will be retained in secure designated locations. Access to this information is restricted to authorised personnel only, which may where necessary in connection with installation, servicing, maintenance or support include personnel of the contractor that installs, services or maintains the CCTV systems. Location of CCTV monitors should be chosen, as far as reasonably practicable, to ensure they cannot be inadvertently viewed by those not authorised to access them. Where this is not possible, monitors should be turned off until the authorised viewer is satisfied it can be viewed by them confidentially.

Where access is given to information recorded on CCTV, the manager responsible for granting access will record to whom it is given and why access is granted. An audit will be carried out from time to time by An Post Internal Audit, to check that procedures are being complied with and whether any procedures need to be updated.

From time to time matters of a serious nature arise which may be appropriate to be dealt with as a breach of contract or pursuant to the Company's Grievance or Disciplinary policy. In dealing with these matters, An Post may seek to establish if any relevant material is held on CCTV systems operated under its control. In seeking to establish if any such material exists the manager in charge of the enquiries will make an application to the Head of Employee Relations to have the relevant CCTV footage made available for viewing. The application will state the reason(s) the footage is being sought and the names and titles of the managers who will be viewing the footage. Where any potential relevant material is identified the Company may retain and use it as part of any proceedings (civil or criminal) relating to a customer, contractor or an employee in accordance with applicable law.

5. LOCATION OF CAMERAS

CCTV cameras will be positioned in areas that are deemed appropriate by the Company to support the objectives as outlined at paragraph 2 above and also to ensure that there is an awareness among outside occupants that a surveillance security system is in operation within and / or in the external environs of the premises. Cameras are located where they will provide the coverage in order to protect the lives of employees and contractors, to protect all mails and to protect valuable property.

An Post have introduced some Post Offices which incorporate the use of the 'open office environment'. There are risks associated with such environments. These risks include jump overs and sleight of hand transactions. In order to mitigate these risks and to ensure the health and safety of the staff An Post has decided to locate some CCTV cameras behind the counter. These cameras will not record any personal information from documents handed over the counter nor will it record any information displayed on PC monitors. The rest of this policy applies equally to the use of these cameras as it does to cameras situated elsewhere in the post office.

CCTV contained in company vehicles will be directed externally for safety and security reasons. The policy applies equally to the use of these cameras as it does to cameras situated elsewhere in An Post.

6. COVERT SURVEILLANCE

Covert surveillance is only permitted on a case by case basis where it is required for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies the actual or potential involvement of An Garda Síochána or other prosecution authorities for potential criminal investigations arising as a consequence of an alleged committal of a criminal offence(s). The An Post Investigation Branch may use Covert Surveillance from time to time as specified below.

The use of covert cameras will be on an exceptional basis and may only be used under the following circumstances:

- An application is made to the Head of Security for the use of the camera(s) and justified reasons put forward for the requirement to utilise covert camera(s).
- Written authorisation for the use of the cameras is given by the Head of Security.
- The decision to use covert recording will be fully documented and sets out why the recording was necessary, how the decision to use covert CCTV was reached and by whom and the duration of the recording.

An Post will use covert cameras for the above purposes in circumstances including, but not exclusively limited to, the following;

- where there are grounds to suspect that unauthorised or illegal activity is taking place or is about to take place;
- where informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; or
- where the recordings will only relate to the specific suspected unauthorised activity.

The use of the covert camera(s) will only be carried out for a limited period of time and be consistent with the objectives of making the recording. The camera(s) will be removed when the set period of time has elapsed.

7. COMMUNICATION, NOTIFICATION – SIGNAGE

Notices will be placed in prominent locations on the premises indicating that CCTV cameras are in use. The signage will advise that CCTV is in operation and the reason for the operation.

In some instances, the CCTV notification will be accompanied by other security signage such as notifications in relation to the use of time locks at Retail Offices and requirements to remove helmets.

All employees will also be provided with access to a copy of this policy.

8. STORAGE & RETENTION

CCTV recordings are stored on digital recorders which are installed in secure areas and should generally be contained in offices where access is limited to managers authorised to view CCTV images.

Where possible the recorder shall be retained in a secure unit and be further protected under the local alarm system.

Typically, data retained through the CCTV system is recorded on a loop and will be retained for no longer than is necessary for the purpose for which it is collected, or as required or permitted for legal, regulatory, fraud prevention and/or legitimate business purposes. In general, data recorded on CCTV will be retained for no longer than 31 days, but will be retained for longer periods where required in connection with criminal investigations and disciplinary proceedings, or where An Post requires the data in connection with legal proceedings or has a legal obligation to retain the data for a longer period. Where the Payment Card Industry Data Security Standard (PCIDSS) so requires for sensitive areas, a retention period of three months will apply.

Recordings are automatically erased when the operational time period has passed. Where recordings are retained for the purposes of an investigation, the images will be securely retained for a period of time as appropriate to the particular case.

9. ACCESS AND SUPPLY OF RECORDINGS TO MANAGEMENT, AN GARDA SÍOCHÁNA AND OTHER INVESTIGATORY BODIES

Access to the CCTV recordings is restricted to;

- Local Management;
- Level 1,2 or 3 Line Management;
- Security Services personnel;
- Internal audit personnel; and
- HR Management as appropriate in each case including Head of Employee Relations as provided under this Policy or their nominee.

An Post may share personal information obtained through the CCTV system with authorised agencies including law enforcement, regulatory authorities or other third parties when required as a matter of applicable law or when there is a legitimate purpose (e.g., an emergency where the health or security of a data subject is in danger, to prevent imminent physical harm or financial loss, to report suspected illegal activity or to protect corporate assets or their use).

Requests from authorised agencies, such as An Garda Síochána or the Department of Social Protection, for copies of recorded CCTV in the investigation of a suspected criminal offence must be notified to Security Services who will liaise with that agency and arrange with the

appropriate manager/Postmaster on site to take copies, subject to applicable Data Protection Legislation. Any requests from such authorised agencies should only be acceded to where a formal written request is provided to An Post. For practical purposes, and to meet a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. Any verbal request must be directed to the Head of Security Services. A record of any such requests (written and verbal) is maintained by the Head of Security Services.

In instances where CCTV data relating to an employee is requested, the Head of Employee Relations or their nominee must be notified. In the event that the application is deemed in order and that it is necessary that the recordings be duly transferred, a record of the event will be retained.

10. RESPONSIBILITIES

Due to the extensive Retail, Mail and administrative networks and divisions in operation within An Post, responsibilities for the management of CCTV systems falls on different managers, both locally and centrally. These responsibilities extend to ensuring compliance with this policy as is applies to the use of CCTV in their respective areas.

Head of Security Services

The Head of Security Services will: -

- Oversee and co-ordinate the use of CCTV systems and recordings for safety and security purposes.
- Ensure that the CCTV monitoring in An Post is consistent with the highest standards and security protections.
- Maintain a record of access requests received by him for release of recorded images or any material recorded or stored in the system.
- Be responsible, for the release of any information or material stored on digital recorders in relation to security issues in compliance with this policy.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to staff, contractors, contractor's staff and customers regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of a reasonable expectation of the privacy of individuals.
- Ensure adequate signage, at appropriate and prominent locations is displayed as detailed above.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy".
- Ensure that recorders are stored in a secure place.
- Ensure that images recorded on Digital Video Recorders (DVRs) / digital recordings or mobile devices or other Company equipment are stored for periods not longer than appropriate and will then be erased unless required as part of a criminal investigation or court proceedings (criminal or civil); for accident investigations; or for staff grievance and disciplinary procedures as approved by the relevant manager.

Local Manager/Postmaster

- Ensure access by authorised personnel only.
- Be responsible for the release of any information or material stored on digital recorders and maintain a record in compliance with this policy.
- Co-operate with the relevant Level 3 Line Manager in regard to the provision of CCTV data required.
- CCTV footage should generally not be recorded onto private devices. Exceptions to be approved by Level 3 line managers in writing.
- Ensure monitors are located so that unauthorised persons cannot view the monitor, insofar as this is practicable. Where this is not possible, ensure the monitor is turned off until the authorised viewer is satisfied it can be viewed by them confidentially.

Level Three Manager

- Be responsible, as appropriate, for the release and storage, deletion of any information or material stored on digital recorders in compliance with this policy.

Head of Insurance Services

- Be responsible, as appropriate, for obtaining copies of CCTV footage and the release and storage and deletion of any information or material stored on Company equipment for claims management. The CCTV footage is held to defend claims against An Post and/or the underwriter.
- Be responsible for the supply of CCTV footage to approved service providers who are data processors who require the footage to provide their service to An Post (e.g. claims assessors; An Post Legal Services; Barristers). Ensure the service providers have appropriate retention and disposal procedures for the CCTV shared with them.
- Ensure that images downloaded for defence of actual and potential claims on Company equipment are not held for longer than appropriate and will be erased unless they are required for claim management including PIAB cases; mediation and court proceedings.

Head of Employee Relations

- Provide input to decisions directly or through a nominee regarding the release of CCTV data held in respect of employees.
- Periodically review the use of CCTV data in the application of the Company's Discipline and Grievance Procedures.
- Ensure that images required for staff grievance or disciplinary procedures are stored for periods not longer than appropriate and are then erased.

HR Management

Access, retain, erase and use CCTV data in accordance with Data Protection Legislation and where appropriate, in addressing matters with employees under the Company's Discipline and Grievance Procedures.

11. SECURITY COMPANIES

The installation, service and maintenance of CCTV systems is provided by contracted security companies ("contractors") to An Post. Agents of the relevant contractors are required to operate in accordance with Data Protection Legislation and An Post policies.

Contractors that place and operate cameras on behalf of An Post are considered to be "data processors" as defined in applicable Data Protection Legislation. As data processors, they operate under the instruction of data controllers (in this case, An Post). Data Protection Legislation place a number of obligations on data processors. An Post ensures that contractors retained, fulfil their obligations which include having appropriate security measures in place to prevent unauthorised access to, unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing and have executed written agreements recording such obligations.

Furthermore, the contract in place with the contractors documents the fact that staff of the contractor must not access or download recorded images on An Post CCTV systems without the instruction or authorisation of the An Post Crime Prevention Unit or an authorised An Post manager.

12. BRIEFING FOR STAFF REQUIRED TO ENGAGE WITH CCTV IN THE COURSE OF THEIR WORK

Staff using the CCTV system or information should be fully informed to ensure they understand and comply with this policy. In particular, they should know:

- The An Post policies for recording and retaining information;
- How to handle the information securely;
- What to do if they receive a request for access to or a copy of CCTV footage, whether from an authorised agency or an individual;
- How to recognise a data subject access request and what to do if they receive one; and
- That breaches of the policy may be addressed pursuant to section 15 of this policy through An Post's Disciplinary Procedures.

13. IMPLEMENTATION, REVIEW AND AMENDMENTS

This policy has been agreed with the An Post Group of Trade Unions and the Data Privacy Office. The date from which the updated Policy will apply is 1st March 2024.

The implementation of the Policy will be monitored by the Company Secretary of An Post.

The Policy will be reviewed at least every two years, evaluated and amended from time to time. Ongoing review and evaluation will take cognisance of changing information, guidelines, legislation and feedback from staff and others.

14. DATA SUBJECT ACCESS REQUESTS AND OTHER RIGHTS

Individuals have certain rights concerning their personal data relating to them. Employees' rights to their personal data are set out in greater detail in the An Post Employee Privacy Statement and the An Post Access Request Policy. Visitors' rights to their personal data are set out in greater detail in the An Post Web Privacy Statement which is available at https://www.anpost.com/Privacy/Website-Privacy-Policy.

An employee who wishes to make a subject access request under the Company's Access Request Policy should access the Subject Access Request Form from the Intranet, if they wish to use it, and send it to the Data Privacy Office, EXO Building or at privacyoffice@anpost.ie.

Other subject access requests and requests from individuals to view or obtain a copy of any CCTV footage should be redirected to the Data Privacy Office, EXO Building Dublin 1 at privacyoffice@anpost.ie. An employee should fill out the Subject Access Request form and enclose a copy of a recent photograph and/or description.

Any relevant CCTV footage (if it exists) will be made available as soon as possible, and no later than one month from the date that the written request is submitted. An Post, may in certain limited circumstances permitted by applicable law, impose a reasonable charge in respect of a data subject access request.

Because An Post is relying on its legitimate interests to record the CCTV footage, individuals may object to use and disclosure of CCTV footage in which they are captured. However, An Post will only be required to cease its processing of that footage where it cannot show compelling legitimate reasons for it to continue its processing or it needs to use the Personal Data for the purposes of legal claims.

Individuals also have the right, in some circumstances, to have personal data erased. However, An Post will not be required to erase personal data where to do so would prevent it from meeting its contractual obligations, or where it is required to process (including retaining) the personal data in order to comply with a legal obligation, or if the personal data is necessary to establish, exercise or defend An Post's legal rights or for the purpose of legal proceedings.

Any requests for erasure and any objections to use of the CCTV footage should be sent to the Data Privacy Office, EXO Building, Dublin 1or Data Privacy Office at privacyoffice@anpost.ie.

If there are any complaints or queries in relation to this policy or the processing of CCTV footage obtained in accordance with this policy, the Head of Security Services should be contacted who may contact the Data Protection Officer of An Post. Individuals also have the right to lodge a complaint with a supervisory authority (i.e. the Data Protection Commission at info@dataprotection.ie) about An Post's processing of CCTV footage containing their images.

15. BREACHES OF THIS POLICY (INCLUDING BREACHES OF SECURITY)

Any breach of this policy by An Post employees or any other person is a serious issue and may result in disciplinary action. Anyone who considers that this policy has not been followed should raise the matter with the Head of Security Services or their line manager, in the first instance.

All employees are obliged to report actual or potential data protection non-compliance or inadequate compliance with this policy. This allows An Post to:

- investigate the cause and take remedial steps if necessary;
- maintain a register of compliance failures in the Data Privacy Office; and
- notify the Data Privacy Office of any compliance failures that are material either in their own right or as part of a data breach.

For more information on data breach reporting, see the An Post Data Breach Policy.

16. GOVERNING LAW

This policy is governed by the laws of Ireland and is subject to the exclusive jurisdiction of the Irish courts.

Last Updated: February 2024