Oifig na nOibreacha Poiblí
The Office of Public Works

The Office of Public Works

Closed Circuit Television (CCTV) Systems Data Protection Policy

Jonathan Swift Street
Trim, Co Meath
Ireland, C15 NX36

www.opw.ie

Contents

1. Key GDPR Compliance Rules for Those Controlling OPW CCTV Systems

DO	See Section
Only use CCTV systems for the purposes of security and personal safety.	6.2
Contact the DPO if you want to use it for any other purpose before doing so.	6.2
Note the legal basis for using CCTV systems: The legitimate interests of the Commissioners of Public Works in Ireland to protect themselves and their property, the Safety, Health and Welfare at Work Act 2005 and Section 3 of the Occupiers' Liability Act, 1995.	6.1.1.6
Erect at least two clearly visible CCTV warning signs at every entrance.	6.1.2
Make the warning signs readable to people before they enter camera shot.	6.1.2
Ensure that CCTV warning signs state that CCTV is in operation, the purpose(s) for which it used and the DPO's contact details.	6.1.2
CCTV warning signs must be bilingual. If separate English and Irish signs are used, the Irish sign should appear first.	6.1.2
Use coloured warning signs with yellow in the background.	6.1.2
Hold at least 10 copies of the OPW CCTV Privacy Statement at reception to give to Data Subjects on request.	6.1.3
Allow Gardaí investigating a crime to review CCTV footage on-site to see if it is of use.	6.2
Get a formal written request, signed by a superior, if Gardaí wish to take a copy of CCTV footage off the premises.	6.2
Keep a log of these Garda requests and a copy of each formal request.	6.2
Balance the risk to security or personal safety against the risk of intrusion into the privacy of individuals.	6.3

DO	See Section
Locate or mask cameras to avoid monitoring passers-by or private property.	6.3
Fulfil Data Subject Access Requests within 30 days. No fee is payable.	6.4 & 6.7
Retain CCTV images for a maximum of 28 days, 65 days for personal injury claims or for the duration of any legal claims made against the OPW.	6.4
Restrict CCTV access to authorised personnel.	6.5
Log all access to CCTV, including by Gardaí.	6.5
Keep CCTV storage devices and media in a secure location.	6.5
Backup CCTV systems, where possible.	6.5
Pixelate the recognisable CCTV images of other individuals or of identifying features of their clothing or vehicles before fulfilling a DSAR.	6.5
Be able to prove that processing of CCTV images complies with the GDPR.	6.6
Establish and maintain a record of all CCTV related processing activities.	6.6 & 6.12
Report breaches of identifiable CCTV images to DPC and Data Subjects	6.6 & 6.1.12
Communicate with Data Subjects in intelligible, clear and plain language	6.7
Allow Data Subjects to fully exercise all of their rights under the GDPR within 30 days and free of charge.	6.7
Build Data Protection principles into new CCTV installations at the design stage. Involve the DPO from the start.	6.8
Instruct all Processors to fully cooperate with tenants to allow them to fulfil their GDPR obligations	6.9
Have binding legal contracts with all Processors conforming with Article 28	6.10

DO NOT	See Section
Locate CCTV warning signs on cameras, poles, beside cameras or anywhere that a person enters camera shot **before** they can read the sign.	**6.1.2**
Use monochrome signs, or signs with a grey background, as they are unfair.	**6.1.2**
Allow Gardaí wish to remove CCTV footage without a formal written request.	**6.2**
Continuously monitor visitors or staff at their work.	**6.3**
Monitor areas where individuals have a reasonable expectation of privacy such as toilet cubicles and urinals, showers, changing rooms, locker rooms or rest rooms.	**6.3**
Record passers-by on the street or monitor the private property of others.	**6.3**
Use CCTV systems to record audio.	**6.3**
Use OPW CCTV systems for covert surveillance under any circumstances.	**6.3**
Show or give anyone CCTV footage with identifiable images of other Data Subjects or that allows them to be indirectly identified (e.g. from vehicles).	**6.5**
Act as a Controller/Joint Controller for OPW-installed CCTV systems in owned /leased estate premises occupied by tenants	**6.9**
Allow Processors to process CCTV images except on documented instructions.	**6.10**
Allow Processors to engage a sub-processor without the prior authorisation.	**6.10**
Act as a Controller/Joint Controller for CCTV systems in cafés, tea rooms or canteens operated by concessionaires	**6.11**

2. Introduction

This policy relates to the use of Closed Circuit Television (CCTV) systems on properties occupied by the Office of Public Works (OPW), whether owned, leased or rented.

CCTV is a technology that uses video cameras to transmit signals to a specific place. It is, in effect, an internal television network. It differs from broadcast television in that the signal is not transmitted publicly.

CCTV systems are generally used to conduct surveillance for security or for health and safety purposes. Accordingly, they capture images that may identify individuals, either directly, by capturing recognisable images of faces, or indirectly, by recording vehicle registration numbers or distinctive items of apparel. Systems on the market today are capable of facial and number plate recognition and recording audio as well as video. The use of CCTV has expanded greatly in recent years as the costs of systems have fallen in tandem with a rise in their sophistication, particularly in the quality of the images recorded, with high-definition colour cameras now being commonplace.

As a result, individuals, particularly in an urban setting, may have their images recorded multiple times per day: on public transport, in stations, in public areas and in shops and restaurants. As CCTV images are date and time-stamped, this allows the movements of individuals to be tracked, sometimes in real-time. The use of motion-sensing cameras, which only record for a period after they detect motion, and high-capacity digital video recorders, mean that without intervention, images may be retained for long periods. Where these images are retained for lengthy periods, this increases the risk to the privacy of individuals, as their movements throughout that period can be tracked.

There are Data Protection and Privacy implications in relation to the use of CCTV systems. Unless such systems are used with proper care and consideration, they can give rise to concern that the privacy of individuals is being unreasonably invaded.

This policy sets out how OPW will manage its CCTV estate and the standards that will apply in respect of the data they capture.

The policy complies with the EU General Data Protection Regulation (GDPR), which takes effect from 25 May 2018 and the Data Protection Acts 1988 to 2018.

3. Purpose of the Policy

The purpose of this policy is to inform managers and staff of their responsibilities for the management and use of CCTV facilities under their control, with special emphasis on the OPW's legal obligations under the EU General Data Protection Regulation (GDPR), with effect from 25 May 2018 and the Data Protection Acts, 1988 to 2018. The associated *OPW Closed Circuit Television (CCTV) Systems Privacy Statement* informs Data Subjects what we do with their identifiable CCTV images. Files containing example signs are also included, which can be printed and laminated for internal use or given to sign makers to manufacture external signs.

4. Scope of the Policy

This policy covers all OPW occupied properties, whether owned, leased or rented, where CCTV cameras have been installed. This includes maintenance depots, heritage sites and staff offices. It does not include the OPW managed estate, whether owned or leased.

There are CCTV systems installed on a number of sites where the OPW is not the lead tenant in the building, for example, the Government Offices in both Hebron Road, Kilkenny and Pearse Street, Athlone. In such cases, the OPW is **NOT** responsible for these CCTV systems and they are outside the scope of this Policy. The lead tenant is responsible for these CCTV systems.

Some OPW sites have CCTV systems used to monitor entrances to allow gates or barriers to be operated from within the premises. These systems do not record images, but still process them. They are within the scope of this Policy.

The OPW has also installed hundreds of CCTV systems in some of its managed (owned or leased) buildings, which other public sector bodies occupy as tenants. These CCTV systems are installed under a standard protocol to cover all entrances and car parks. The systems protect the staff and property of the tenants. Tenants may have also installed their own CCTV systems. The OPW-installed CCTV systems, together with any CCTV systems installed by the tenants, are outside the scope of this Policy and remain the sole responsibility of these tenants.

5. CCTV and Data Protection Legislation

The Office of Public Works is subject to the GDPR and the Data Protection Acts 1988 to 2018 .

Recognisable images captured by CCTV systems are personal data. They are therefore subject to the provisions of this legislation.

A new Supervisory Agency, the Data Protection Commission (DPC), established by the Data Protection Act 2018, enforces the GDPR and the Data Processing Acts 1988 to 2018. This replaces the Office of the Data Protection Commissioner (ODPC).

The Data Protection Commissioner has raised concerns about expanded use of CCTV systems and their "society-wide implications". The Commissioner has stated that "unless such systems are used with proper care and consideration, they can give rise to concern that the individual's "private space" is being unreasonably eroded".

Article 5 of the GDPR sets out seven principles of data protection, with an eighth, Data Subject rights, set out in Articles 15 – 22. The principles relevant to the personal data processed by CCTV systems are listed below. Personal data shall be:

- **Processed lawfully, fairly and transparently in relation to the Data Subject**

  a) To process identifiable CCTV images **lawfully**, at least one of the following lawful grounds for processing must apply:

  - A contractual necessity where a Data Subject is a party to a contract or if requested by a Data Subject before entering a contract'
  - A non-contractual legal obligation on the Controller (OPW).
    This requires a legal basis.
  - The protection of the vital interests of the Data Subject or another natural person.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller (OPW).
    This requires a legal basis.
  - The legitimate interests pursued by the Controller or by a third party, where these legitimate interests are not overridden by the fundamental rights and freedoms of the Data Subject which require the protection of personal data, in particular where the Data Subject is a child.

  b) To process identifiable CCTV images fairly, Data Subjects must be informed that CCTV systems are in operation and the purposes for which the images are captured. These purposes should be stated in a CCTV Policy (this document) and by having signs warning Data Subjects that a CCTV system is in operation and informing them of the purposes for which it is used. These signs must be visible to a Data Subject before their image is captured by the CCTV system.

  c) To process identifiable CCTV images transparently, Data Subjects must be provided with the information in the *OPW CCTV Privacy Statement*, as required by Article 13 of the GDPR. See the privacy statement or Section 6.7.1 of this Policy for more details.

- **Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes**
  Only use CCTV images for the purposes set out in this document and stated on warning signs: currently **security** and **personal safety**. **Do not** use them for any other purpose.

- **Adequate, relevant and limited to what is necessary**
  Only the minimum personal data necessary should be captured. The risk to the security of a property or to the health and safety of staff, contractors or visitors must be balanced against the risk of intrusion into the privacy of individuals.

- **Accurate and, where necessary, kept up to date**
  This is not relevant to processing personal data captured by CCTV systems.

- **Not kept in an identifiable form for longer than necessary**
  28 days (65 days in the case of a personal injury), unless required for criminal investigation or legal proceedings.

- **Processed to ensure appropriate security, using appropriate technical and organisational measures**, to protect it from:
  - Unauthorised or unlawful processing
  - Accidental Loss
  - Disclosure
  - Destruction

  Access to CCTV systems, including to storage devices and storage media, should be restricted to authorised personnel and logged. DVR CCTV systems should be backed up.

- **As a Controller, the OPW is responsible for and must demonstrate compliance with all of the principles above.**

- **The OPW must allow Data Subject to exercise their rights** in Articles 15 – 22 of the GDPR, as restricted by Article 23 and Sections 51 – 56 of the Data Protection Act 2018. These rights are:
  - Access to their identifiable CCTV images
  - Rectification (correction) of their identifiable CCTV images
  - Erasure of their identifiable CCTV images
  - Restriction of processing of their identifiable CCTV images
  - The OPW must notify recipients of any rectification, erasure or restriction of processing of the identifiable CCTV images of Data Subjects
  - Data Portability
  - Object to processing of their identifiable CCTV images
  - Not to be subjected to automated individual decision-making

Article 34 obliges the OPW to tell Data Subjects about a personal data breach involving their identifiable CCTV images in clear and plain language without delay, where the breach is likely to result in a high risk to their rights and freedoms. Data Subjects must be given the name and contact details of the DPO, the likely consequences of the breach and the measures taken (or proposed) to addresses the breach, including mitigation measures.

Article 77 gives Data Subjects the right to complain to the Data Protection Commission if they consider that the processing of their identifiable CCTV images infringes the GDPR.

Article 79 gives Data Subjects the right to an effective judicial remedy against the OPW or its Processors if they consider that their rights under the GDPR have been infringed by processing of their identifiable CCTV images that does not comply with the GDPR.

Under Article 82, Data Subjects who have suffered material or non-material damage as result of an infringement of the GDPR have the right to be compensated by the OPW or its Processors.

6. Procedures for the Use of OPW CCTV Systems

Compliance with the procedures in this section is essential for OPW CCTV usage as they are legal requirements under the General Data Protection Regulation (GDPR) and the Data Protection Acts, 1988 to 2018.

6.1. Lawful, Fair and Transparent Processing of CCTV Images

Article 5.1.a of the GDPR states that personal data shall be processed lawfully, fairly and transparently in relation to the Data Subject. This is the principle of *lawfulness, fairness and transparency*, one of the eight Data Protection principles

6.1.1. How can CCTV Images be Processed Lawfully?

The lawful grounds for processing personal data are in Article 6 of the GDPR. A public authority can only process it lawfully if at least one of the following is true:

6.1.1.1. Consent of the Data Subject to the Recording of Their CCTV Image for Specific Purpose(s)

Consent **cannot** be used where a clear imbalance exists between the Data Subject and the Controller, especially where the Controller is a public authority or an employer, as is clearly the case for the OPW.

6.1.1.2. Contractual Necessity Where the Data Subject is a Party to the Contract

Contractual necessity **cannot** be used as there is no contract between the Commissioners and their staff, contractors or visitors regarding the capture of their images by OPW CCTV systems.

6.1.1.3. Non-contractual Legal Obligation on Controller

No such legal obligation exists.

6.1.1.4. Protection of the Vital Interests of the Data Subject or Another Natural Person

This **cannot** be used, since the primary purpose for the use of CCTV system is the protection of the Commissioners and their property, i.e. protecting the vital interests of the Controller, which is clearly at odds protecting the vital interests of Data Subjects.

6.1.1.5. Performance of a Task Carried out in the Public Interest or in the Exercise of Official Authority Vested in the Controller

This requires a legal basis, the legitimate interests of the Commissioners of Public Works in Ireland to secure themselves and their property in their own interests and not in the public interest, just like any other property owner. Personal safety, protecting the health and safety of their staff, contractors and visitors is clearly in the exercise of the Commissioners' official authority. It has a legal basis in the Safety, Health and Welfare at Work Act 2005 and Section 3 of the Occupiers' Liability Act, 1995.

6.1.1.6. Legitimate Interests Pursued by the Controller or a Third Party

This does **not** apply to processing carried out by public authorities in the performance of their core and statutory tasks. It **applies** to tasks that are non-core, not set out in legislation and in the interests of the public body and not in the public interest, such as security, protecting the Commissioners of Public Works in Ireland and their property.

6.1.2. How can CCTV Images be Processed Fairly?

Before a person's image can be captured by a CCTV system, they must be informed (a) that CCTV is in operation and (b) of the purposes for which these images (personal data) are captured.

While the *OPW Closed Circuit Television (CCTV) Systems Privacy Statement* document states these purposes, it would be both unfair and entirely unreasonable to expect a Data Subject to read the privacy statement on the OPW's website before visiting an OPW heritage site or entering an OPW building. However, to ensure that Data Subjects have access to it, at least ten copies of the privacy statement should be kept at the reception of all locations where OPW CCTV systems are in operation.

However, the easiest and fairest way to inform Data Subjects of the purposes for which CCTV images are being captured is through clear and unambiguous signs. Clearly visible signs (as shown out on the next page and in Appendix 1) should be erected **at every entrance** to the site, premises or property. Data Subjects should notice and be able to read these sign before they enter camera shot. The signs **must** state that CCTV is in operation, the purpose(s) for which the images are being captured and the contact details for the DPO.

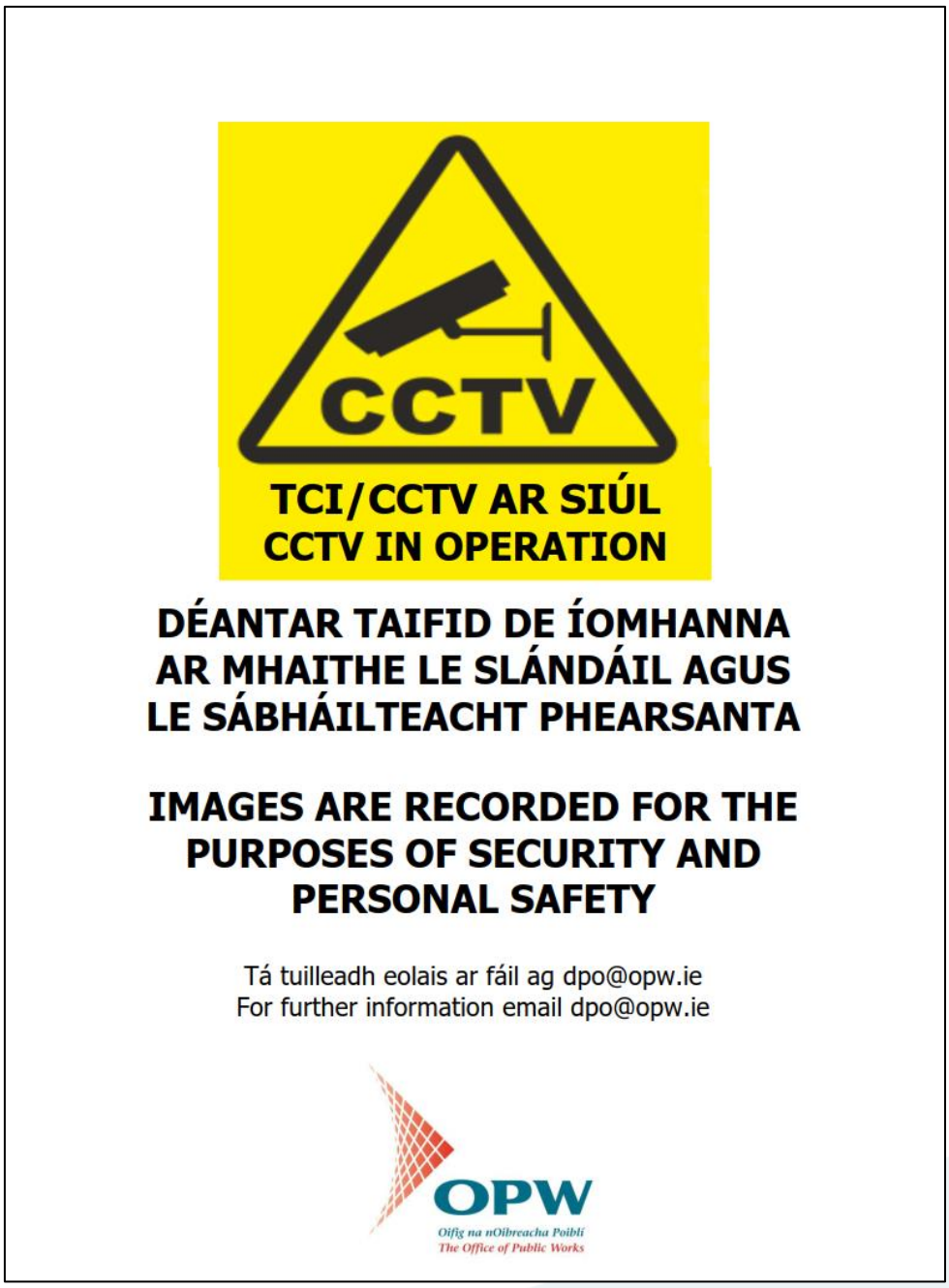
Use the generic email for the DPO, dpo@opw.ie on the signs, as this is both concise and does not need to be changed if a new DPO takes over. Separate Word and PDF files containing copies of these signs accompany this policy and can be printed directly. Signs should never be located on cameras or camera poles, adjacent to cameras or in any other location where a Data Subject's image has been captured before they have had the opportunity to be informed that CCTV is in operation or the purposes for which the captured images are to be used.

CCTV warning signs must comply with the Official Languages Act 2003. To do so, they must either be bilingual, as shown, or where separate English and Irish signs are used (see Appendix 1), the Irish version should appear first.

Wherever possible, a Data Subject should pass at least **two** warning signs before their image is captured. As they are warning signs, they **must** be in colour, with a yellow background. Black and white signs, or signs with a grey (or other muted colour) background are unfair, as they are much harder for a Data Subject to notice.

Signs on cameras or camera poles are also unfair, as the Data Subject enters camera shot before they can even read the sign. These are examples of unfair signs:

To minimise costs, you can print the signs in the PDF and Word files that accompany this policy on a colour printer and laminate them. These are ideal for internal use, but are not robust enough for external use. External signs must be metal or plastic.



6.1.3. How can CCTV Images be Processed Transparently?

Before a person's image can be captured by a CCTV system, they must be informed (a) that a CCTV is in operation and (b) of the purposes for which these images (personal data) are captured. The *OPW Closed Circuit Television (CCTV) Systems Privacy Statement* provides these purposes, currently **security** and **personal safety**, along with all the other information that OPW must give to Data Subjects under GDPR Article 13.

It would be both unfair and entirely unreasonable to expect Data Subjects to read this document on the OPW website before visiting an OPW heritage site or entering an OPW building. However, at least ten copies of the privacy statement should be held at the reception of all sites where OPW CCTV systems are in operation, and given to Data Subjects on request.

6.2. Purpose Limitation for Processing of CCTV Images

Article 5.1(b) of the GDPR states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any way incompatible with those purposes. This is the *purpose limitation* principle.

CCTV images can only be used for the purposes specified in this document and on the CCTV warning signs. These purposes are currently **security** and **personal safety**. If CCTV images are required for additional purposes, these must be approved in advance by the OPW's Data Protection Officer and, if necessary, by the Data Protection Commission. This policy, the privacy statement and all CCTV warning signs must then be amended.

Some CCTV systems may cover part of neighbouring premises or streets. When investigating a crime, which may or may not have occurred on OPW premises, An Garda Síochána may wish to view CCTV footage to see if it is of assistance. Where An Garda Síochána view the footage on OPW premises or that of an OPW Processor, no data protection concerns arise.

If An Garda Síochána wish to take away a copy of CCTV footage, however, they **must** provide a formal written request, which:

- States that An Garda Síochána is investigating a criminal matter
- Is written on Garda Síochána headed stationery
- Is signed by a superior officer of the requesting Garda
- Sets outs the details (dates, times and durations) of the CCTV footage required
- Cites the legal basis for the request

The legal basis is Section 41(b) of the Data Protection Act 2018. This provides that the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful where the processing is necessary for the purposes of preventing, investigating or prosecuting criminal offences.

This request should be given to and retained by manager or staff member on the site responsible for the release of the CCTV images. It may be posted, faxed or emailed. Each site using CCTV should maintain a log of all such Garda Síochána requests.

6.3. Minimisation of Data Captured by CCTV Systems

Article 5.1.c of the GDPR states that personal data collected shall be adequate, relevant and limited to what is necessary. In other words, it should be proportionate and should collect only the minimum personal data necessary. This is the *data minimisation* principle.

When processing personal data by means of a CCTV system, the risk to the security of a property or to the health and safety of staff, contractors or visitors must be balanced against the risk of intrusion into the privacy of individuals. Use of CCTV in car parks, on the external perimeter and/or entry/points of a property for security and/or personal safety is proportionate. However, using CCTV to continuously monitor visitors or staff at their work would be disproportionate, unless, for example, the staff concerned were working in very hazardous or high-risk areas. Examples of hazardous places would be those that might contain toxic gases, such as mines, tanks or sewers. Examples of high-risk areas would be locations that handle very large amounts of cash of high value items, such as a cash office in a bank, a jeweller's or a pharmaceutical storage area.

A key consideration is what CCTV systems monitor. The use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be very disproportionate. Toilets, showers, changing rooms, locker room and rest rooms are obvious examples. To justify use in such an area, an organisation would have to demonstrate and document in writing that a pattern of security breaches had occurred in the area prior to the installation of the CCTV system, which was serious enough to warrant constant electronic surveillance and a high level of intrusion into the privacy of Data Subjects.

The very high burden of proof required for such a justification falls to the organisation, and because of the balancing against the privacy risk, the bar is set very high. The security breaches would need to be very serious and everything would have to be carefully documented. It is not simply a case that in order to have security that there cannot be privacy. Where such use can be justified, the CCTV cameras should never be capable of capturing images from toilet cubicles or urinal areas. Cameras placed to record external areas or entrances from the inside should be positioned in such a way as to prevent or minimise recording of passers-by on the street or of another person's private property. Where this is not possible, these areas should be screened or masked on the camera.

Some modern CCTV systems also have the facility to record audio (sound or voices). The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. The Data Protection Commission considers that audio recording by equipment used for security purposes is a considerable added intrusion into the privacy and data protection rights of individuals. Even where members of the public or staff are aware that their voices are being recorded, the Data Protection Commissioner does not accept that the use of such audio recording equipment is in any way justifiable or warranted for any purpose. CCTV systems should **not** be used to record audio and when equipment has this facility, it should be disabled.

OPW CCTV systems should not be used for covert surveillance under any circumstances.

6.4. Retention of Identifiable Images Captured by CCTV Systems

Article 5.1.e of the GDPR states that personal data collected shall not be kept in an identifiable form for longer than necessary for the purposes for which it is processed. This is the principle of *data minimisation*.

Most CCTV footage is actually useless. Where nothing out of the ordinary happens, it contains hours of dull footage of empty premises. Most of it is never viewed. Where it may contain images of identifiable Data Subjects, however, it can attract Data Subject Access Requests (DSARs) from individuals seeking copies of their personal data. From 25 May 2018, no fee is payable for a first DSAR and it must be fulfilled within 30 days. In fulfilling CCTV DSARs, the OPW cannot release the identifiable images of other Data Subjects, so anything which makes another individual identifiable: faces, distinctive clothing or identifying features of vehicles, such as registration numbers, roof racks or unusual hubcaps must be pixelated.

If the CCTV camera is recording at 30 fps (frames per second), each second of video will require 30 images to be pixelated. An hour of CCTV footage would require the pixilation of 108,000 separate images (60 x 60 x 30). To pixelate images, each section to be pixelated must be done individually. Assuming that each image could be pixelated in 1 minute, an hour of video would take 1,800 person hours, or with an 8-hour day, 45 person weeks. At €20 an hour it would cost **€36,000** or **€600** per minute. Specialist companies can be contracted to pixelate CCTV videos but may cost more than €20 per hour.

As most incidents or accidents happen very quickly, the response to a DSAR should focus on these few seconds or minutes, as otherwise the costs involved become excessive. It would be unreasonable for a Data Subject to request the 4 hours of footage for the entire duration that their car was parked in an OPW car park. Negotiate with Data Subjects to get them to accept shorter relevant video clips instead. If they are unwilling to accept these, refuse their unreasonable or excessive DSARs and let them complain to the Data Protection Commission.

The retention period of OPW CCTV systems is **28 days**. Systems should be configured to automatically overwrite or delete images after 28 days. Where such automation is not possible, those who manage or are in charge of the CCTV system should manually delete images older than 28 days on a daily basis.

If the managers or those in charge of the CCTV system become aware that an incident has occurred, the relevant footage should be copied and kept securely (locked up) for 28 days, unless required before that. The two exception to this are set out in the next two paragraphs.

In the case of personal injury (and associated property damage), where a claim may be made against the OPW, the copy of the relevant footage may be kept for **65 days**. Section 8 of the Civil Liability and Courts Act 2004 provides a legal basis for this, as a plaintiff has two months (60 days) to make a claim for personal injuries. In the case of property damage **alone**, the Statute of Limitations Act 1957 provides a six-year period for making a claim. It would not be reasonable or proportionate to retain CCTV footage for such a long period, just in case a claim might be made, so the **28 day** retention period applies.

Where a claim is made against the OPW, the copy of the relevant footage should be retained for the duration of the case and any follow up appeals. Section 41(c) of the Data Protection Act 2018 provides a legal basis for processing personal data to establish, exercise or defend legal rights, for obtaining legal advice or for actual or prospective legal claims and proceedings.

Where a vehicle has been damaged in a car park by a third party (not by the OPW), any CCTV footage of the incident should not be kept for longer than 28 days.

6.5. Security of Identifiable Images Captured by CCTV Systems

Article 5.1.f of the GDPR states that personal data collected shall be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures, to protect it from:

- Unauthorised or unlawful processing
- Accidental Loss
- Disclosure
- Destruction

This is the principle of *integrity and confidentiality*.

It is vital that security precautions are taken to prevent unauthorised people from having access to view, copy or interfere with CCTV footage. Access should be restricted to authorised personnel only. The CCTV system should be password protected with each authorised user having their own named login. Where this is not possible, only review CCTV images in a secure area, and not in a generally accessible place such as reception.

Access should be automatically logged (user name, login and logout dates and times). Where an automatic log is not possible, keep a written log who access the CCTV system to view images, including Gardaí viewing it to see if it contains material relevant to a criminal investigation. The storage device, e.g. DVR (Digital Video Recorder), DVD recorder or VCR and any storage media (e.g. DVDs, videotapes) should be stored in a secure environment.

Under GDPR Article 5.1.f, the OPW cannot disclose a Data Subject's identifiable CCTV images to others. When members of the public, staff or contractors have their vehicle or property damaged in a car park or have an accident, such as a trip or fall, they may report it to reception and ask to see or for a copy of the CCTV footage there and then**. Do NOT show anyone unredacted CCTV footage as this may show the identifiable images of other Data Subjects or identifying features of their clothing or vehicles.**

They may subsequently make a DSAR for relevant CCTV footage in support of their case. **Do NOT give anyone recognisable CCTV images of other individuals or of identifying features of their clothing or vehicles in response to a DSAR, unless these have been pixelated first.** Frequently, the individual whose property or vehicle has been damaged or who has been injured will, understandably, be upset and enraged. While an individual is entitled to a copy of footage in which they appear, they are not entitled to any footage which identifies any other Data Subjects, including identifiable vehicles or clothing. They should **not** be supplied with this **in any circumstances**.

Anything that identifies any other individual: faces, distinctive clothing or unique characteristics of vehicles, e.g. registration numbers, roof racks or unusual hubcaps must be pixelated. As the pixelated footage is unlikely to conclusively show who was responsible for causing the damage or injury, the results of a DSAR are unlikely to be of much use to the Data Subject, as all it will show will be pictures of their own vehicle or themselves. Such a DSAR could run up large pixelation costs for the OPW.

In any case, this is **not** the stated purpose of the CCTV system. This should be patiently explained to the individual whose property or vehicle has been damaged or who has been injured, even if they do not want to know or are unlikely to listen.

DVR systems should be backed up, where possible. It is generally not possible to backup other types of CCTV systems.

6.6. Accountability for Data Captured by CCTV Systems

Article 5.2 of the GDPR states that as a Controller, the OPW is responsible for and must be able to demonstrate compliance with all of the principles from sections 6.1 to 6.5. This is the principle of *accountability*. Article 24 further states that the OPW must take account of the risks to data subjects involved in processing personal data (capturing CCTV images) and implement must appropriate technical and organisational measures to ensure that we comply with the GDPR and to be able to demonstrate this compliance. **It is not enough to say that our processing of identifiable CCTV images complies with GDPR – we must be able to prove it.**

How can this be achieved?

The OPW must:

- Have a CCTV policy and must implement it (Article 24).
- Establish internal data protection assessment procedures before creating new CCTV systems.
- Map its CCTV systems to identify all personal image capturing processing activities and maintain an inventory of them (Article 30).
- Have a Data Protection Officer and other individuals with responsibility for Data Protection in general and specifically in relation to CCTV (Articles 37-39).
- Provide adequate and specific Data Protection awareness, training and education to staff regarding the correct and legal use of CCTV systems (Article 39).
- Allocate sufficient resources for Privacy Management and Data Protection. This includes training, budget and staffing. (Article 38).
- Set up transparent procedures to manage Data Subject Access Requests (DSARs), correction requests and deletion requests. Correction requests will not apply in the case of CCTV as the system captures an accurate representation of a Data Subject within the limitations of the technology used, even it the image is horrible.
- Establish an internal complaints handling mechanism.
- Set up internal procedures to effectively manage and report security breaches involving images captured by CCTV systems (Articles 33-34).
- Undertake Data Protection Impact Assessments in specific circumstances where capturing CCTV images presents a high risk to the rights and freedoms of Data Subjects (Article 35).
- Undertake regular Data Protection Audits to ensure that all these measures are being implemented and are working in practice (Article 39).

6.7. Data Subject Rights and CCTV Systems

Article 12 of the GDPR sets out how Data Subjects can exercise their rights, initiating the process by contacting the DPO. Article 13 specifies the information which the OPW must provide to Data Subjects about CCTV images which are collected from them.

This information is set out in Section 6.7.1 below and in the *OPW Closed Circuit Television (CCTV) Systems Privacy Statement*. Any information or communications provided by the OPW to Data Subjects must be written in concise, intelligible, clear and plain language, and be sent by post or via PW's secure "drop box" facility.

If the Data Subject requests it and the OPW can confirm their identity, it can be provided orally, providing that it is brief enough and technically feasible. Confirmation that the OPW has CCTV images of a Data Subject could be provided orally; copies of the images themselves obviously could not.

The OPW must allow Data Subjects to exercise their rights in Articles 15 – 22 and 34 of the GDPR, as restricted by Article 23 and Sections 56 – 61 of the Data Protection Act 2018.

The OPW must provide information within **one month** on the actions it has taken in response to a request made under the Data Subject rights in Articles 15 – 22. This is a reduction from the 40 days allowed under the Data Protection Acts 1988 and 2003.

This period may be extended by a further **two months** when necessary, based on the complexity of the request or the number of requests involved, but the Data Subject must be informed of this within the first month, together with the reason for the delay.

If the OPW does not take action in response to a Data Subject's request made under the Data Subject rights from Article 15–22, it must inform the Data Subject without delay and, at the latest, within **one mont**h. The Data Subject must also be told that they have the options of complaining to the DPC and of seeking a judicial remedy

Where a request is made electronically, the information must be provided electronically, unless the Data Subject requests otherwise.

Information provided to a Data Subject under Article 13 and any communication or actions taken under Articles 15 -22 and 34 must be supplied **free of charge.** Where the requests from a Data Subject are **manifestly unfounded** or **excessive**, especially where repetitive, the OPW may either charge a reasonable fee based on the administrative cost of meeting the request or refuse to act on it. *Manifestly unfounded* means very obviously wrong or not based on fact. Some examples:

- A Data Subject requests CCTV images from an OPW car park, because they believe that their car was damaged there. It is later discovered that the car was actually damaged elsewhere, so the Data Subject was mistaken.
- Someone requests CCTV footage from a heritage site that they had not actually visited, having confused one heritage site with another. Kinsale, Killarney, Cahir and Roscrea are all towns with more than one heritage site.

A request for all the CCTV the OPW has of a particular Data Subject would clearly be *excessive*. Requests should indicate the particular site involved and be as precise as possible about dates and times. However, it is up to the OPW to **prove** that the request is manifestly unfounded or excessive in nature. Where a request is vague or ambiguous, however, the OPW should not initially refuse it or charge for it. Instead, the OPW should seek clarification of they want from the Data Subject. If this is not forthcoming, then a request may be refused or charge imposed.

Where the OPW has reasonable doubts as to the identity of the person making a request for Data Subject rights under Articles 15 – 21, it can request that the person provide additional information necessary to confirm their identity. Be very careful of requests coming from external email addresses as there is no guarantee that the person is who they claim to be.

Ask for a postal address and then request proof of identity, including proof of address, by post. The OPW's DSAR records should note that ID was provided and the type of documents provided. The copies of identity documents **must not be retained**. The 30-day countdown does not begin until the identity of the person making the request has been satisfactorily verified.

Data Subjects have the following rights under the GDPR and the Data Protection Acts 1988 to 2018:

6.1.4. Access to Their Recognisable CCTV Images (Article 15)

The OPW must confirm to the Data Subject if their identifiable CCTV image has been recorded and, if so, they must be given a copy of the CCTV images recorded (with the images that identify other Data Subjects pixelated), together with the following specific items of information:

	Information Item	Comment
a)	The purposes of the processing of recognisable CCTV images	*Security* and *personal safety*. Include any additional purposes
b)	The categories of CCTV images	Directly or indirectly recognisable images of the Data Subject
c)	Recipients (or categories of Recipients) of the CCTV images	None
d)	Period for which the CCTV Images data will be stored	**28 days**. **65 days** for personal injury cases. For the duration of any legal claims made against the OPW and any appeals.
e)	Inform Data Subjects of their rights to: • Request correction of inaccurate CCTV images • Erasure of CCTV images • Restrict the processing CCTV images so that they can only be stored • Object to the processing of their CCTV images	Does not apply, as it is impossible to correct CCTV images.
f)	Inform Data Subjects of their rights to complain to the DPC	
g)	If automated decision-making, such as profiling, is used, provide meaningful information about the logic used by the algorithm as well as the significance and consequences of such processing for the Data Subject	Does not apply as the OPW does not use automated decision-making with CCTV images
h)	Where CCTV images be transferred out of the EEA or to an international organisation the safeguards relating to the transfer (Article 46)	Does not apply as OPW's CCTV images are not transferred out of the EEA or to an international organisation

Where the Data Subject request further copies of CCTV images, the OPW may charge a reasonable fee based on the administrative costs involved.

6.1.5. Rectification of Their Recognisable CCTV Images (Article 16)

Data Subjects have the right to rectification (correction) by the OPW of their *inaccurate* recognisable CCTV images, without undue delay. This right does not apply, as correcting CCTV images is impossible.

6.1.6. Erasure of Their Recognisable CCTV Images (Article 17)

6.1.6.1. Erasure of CCTV Images

Also known as the right to be forgotten, Data Subjects have the right to have the OPW erase their recognisable CCTV images as soon as possible, where one of the following grounds applies:

a) The identifiable CCTV images are no longer necessary for the purposes for which they were processed.
This should not occur where this policy is followed, as security and personal safety are open-ended purposes.

b) The Data Subject withdraws the consent on which the processing of the recognisable CCTV images is based and there is no other legal ground for processing.
This does not apply as the OPW does not use the consent of Data Subjects as a basis for the processing of CCTV images.

c) The Data Subject objects to the processing of recognisable CCTV images which is based on:

- The performance of a task carried out in the public interest by or in the exercise of official authority vested in the OPW
  The OPW does not use this as a basis for capturing recognisable CCTV images

- The legitimate interests pursued by the OPW or by a third party, where these legitimate interests are not overridden by the fundamental rights and freedoms of the Data Subject which require the protection of personal data
  The OPW's compelling legal grounds for capturing recognisable CCTV images are its legitimate interests in:
  - *Protecting the property of the Commissioners of Public Works in Ireland from theft, criminal damage or any other criminal activity*
  - *Protecting their staff, contractors and any visitors from physical assault, threatening behaviour or robbery*
  - *Protecting the Commissioners of Public Works from fraudulent personal injury claims*
  - *Protecting the health and safety of their staff, contractors and visitors from accidental harm or injury.*

These override the interests, rights and freedoms of Data Subject or are used to establish, exercise or defend legal claims.

- Direct marketing purposes, including profiling
  This does not apply as the OPW does not process recognisable CCTV images for direct marketing purposes

d) The recognisable CCTV images have been captured unlawfully.
This should not occur where this policy is followed.

e) The captured CCTV images have to be erased to comply with a legal obligation under Irish or EU law
There is no such obligation.

f) The CCTV images have been captured in relation to the offer of an Information Society service
The OPW does not offer Information Society services nor use CCTV images for this purpose.

6.1.6.2. Recognisable CCTV Images Processed by Other Controllers

If the OPW has made CCTV images public and must erase them, it must inform other Controllers that the Data Subject has requested the erasure of their CCTV images. As the OPW does not make footage from its CCTV systems public, this is not relevant.

6.1.6.3. Exceptions

The right of erasure does not apply to processing of CCTV images necessary for:

a) Exercising the right of freedom of expression and information

b) Compliance with a legal obligation under Irish or EU law or for the performance of a task carried out in the public interest by the OPW or in the exercise of official authority vested in the OPW

c) Reasons of public health

d) Archiving in the public interest, scientific or historical research or statistics

Exceptions a) – d) do not apply as the OPW does not use recognisable CCTV images for these purposes.

e) Establishing, exercising or defending legal claims.
OPW uses recognisable CCTV images to defend legal claims made against it.

6.1.7. Restriction of Processing of Their Recognisable CCTV Images (Article 18)

Restricted CCTV images may be stored, but cannot be processed otherwise without the consent of the Data Subject; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person or for reasons of important EU or Irish public interest.

The Data Subject can get OPW to restrict recognisable CCTV images where one of the following applies:

a) For a period necessary to enable the OPW to verify the accuracy of CCTV images being contested by the Data Subject. This could arise if a Data Subject is identified indirectly, e.g. by distinctive clothing, or by vehicle characteristics

b) The recognisable CCTV images have been captured unlawfully but the Data Subject opposes their erasure and requests the restriction of their use instead

c) The OPW no longer needs the CCTV images but they are required by the Data Subject for the establishment, exercise or defence of legal claims

d) While verifying that the legal grounds of the OPW override those of a Data Subject who is objecting to the capture of CCTV images which is based on:

   - The performance of a task carried out in the public interest by the OPW or in the exercise of official authority vested in the OPW, or

   - The legitimate interests pursued by the OPW or by a third party, where these legitimate interests are not overridden by the fundamental rights and freedoms of the Data Subject which require the protection of personal data

OPW must inform the Data Subject before it can lift the restriction of processing.

6.1.8. The OPW's Obligation to Notify Recipients Regarding Rectification, Erasure or Restriction of Processing of Recognisable CCTV Images (Article 19)

The OPW must communicate any rectification, erasure or restriction of processing of recognisable CCTV images to each external recipient of these images. The OPW must inform the Data Subject about these recipients on request.

6.1.9. Data Portability (Article 20)

Where recognisable CCTV images are captured on the basis of the consent of a Data Subject or a contract between the Data Subject and the OPW, the Data Subject is entitled to receive their CCTV images in a structured, commonly used and machine readable format (MP4, AVI or WMV) and to transmit these to another Controller. As the OPW uses neither consent nor a contract as a basis for capturing recognisable CCTV images, this right does not apply.

6.1.10. Object to Processing of Their Recognisable CCTV Images (Article 21)

A Data Subject can object to the capture of recognisable CCTV images where:

- This is based on the performance of a task carried out in the public interest by or in the exercise of official authority vested in the OPW.

The OPW does not use this as a basis for capturing recognisable CCTV images

- This is based on the legitimate interests pursued by the OPW or a third party, where these legitimate interests are not overridden by the fundamental rights and freedoms of the Data Subject which require the protection of personal data.

The OPW's compelling legal grounds for capturing recognisable CCTV images are its legitimate interests in:

  - Protecting the property of the Commissioners of Public Works in Ireland from theft, criminal damage or any other criminal activity
  - Protecting their staff, contractors and any visitors from physical assault, threatening behaviour or robbery
  - Protecting the Commissioners of Public Works from fraudulent personal injury claims
  - Protecting the health and safety of their staff, contractors and visitors from accidental harm or injury.

These override the interests, rights and freedoms of Data Subject or are used to establish, exercise or defend legal claims.

- They are processed for direct marketing purposes, including profiling.

This is not relevant, as the OPW does not process recognisable CCTV images for direct marketing purposes.

- They are processed for scientific or historic research purposes or statistical purposes.

This is not relevant, as the OPW does not process recognisable CCTV images for scientific or historic research purposes or statistical purposes.

6.1.11. Not to be Subject to Automated Individual Decision-Making, Including Profiling (Article 22)

Decision-making based solely on automated processing, without any meaningful human involvement, including profiling, that has legal effects on a Data Subject, or similarly significantly affects them, are prohibited as a Data Subject has the right not to be subject to such decisions. An example would be using facial recognition with CCTV to automatically identify and fine individuals who had trespassed in a restricted area. This right does not apply if the decision is:

- Necessary for a contract between the Data Subject and the OPW
- Authorised by EU or Irish law to which the OPW is subject
- Based on the Data Subject's explicit consent

While still safeguarding the Data Subject's rights, freedoms and legitimate interests.

6.1.12. Communication of a Personal Data Breach to a Data Subject (Article 34)

Where a breach of recognisable CCTV images has occurred, that is, they have been:

- Accessed by unauthorised persons
- Disclosed to unauthorised persons
- Lost
- Destroyed, or
- Unlawfully processed

and this is likely to result in a **high risk** to the rights and freedoms of Data Subjects, the OPW must inform the Data Subjects without undue delay. This communication must describe the nature of the breach in clear and plain language. At a minimum, it must include:

- The name and contact details of the DPO or other contact point where more details can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to address it and mitigate its possible adverse effects.

It is **not** necessary to inform Data Subjects, where:

- The recognisable CCTV images were encrypted
- Subsequent measures have been taken to ensure that there is no longer a high risk to peoples' rights and freedoms
- It would involve disproportionate effort. In this case there must be a public communication that informs Data Subjects in an equally effective manner.

6.1.13. Restrictions (Article 23)

The rights in Article 12 – 22 (Sections 6.7.1 – 6.7.9) and Article 5 (Sections 6.1 – 6.6) are not absolute and are subject to the restrictions in Article 23 of the GDPR and Sections 56 – 61 of the Data Protection Act 2018. The main restrictions are:

- National security
- Defence
- Public security
- Prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties
- Important objectives of general public interest, such as:
  - EU or Irish economic/financial interests
  - Monetary, budgetary and taxation matters
  - Public health
  - Social security
- Protection of judicial independence and judicial proceedings
- Prevention, investigation, detection and prosecution of breaches of ethics for regulated professions
- Monitoring, inspection or regulatory functions
- Protection of Data Subject or the rights and freedoms of others
- Enforcement of civil law claims

6.1.14. Lodge A Complaint With The DPC (Article 77)

Data Subjects may complain to the Data Protection Commission, where they consider that their rights under the GDPR have been infringed.

6.1.15. An Effective Judicial Remedy Against the OPW or its Processors (Article 79)

Data Subjects have the right to an effective judicial remedy against the OPW or its Processors, where they consider that their rights under the GDPR have been infringed.

6.8. New Installations of CCTV Systems

Article 25 of the GDPR requires new CCTV installations to have appropriate technical and organisational measures built-in, right at the design stage, so that the data protection principles are implemented from the start and that they continue to be throughout its operational life. The DPO should be consulted and involved from the beginning of the process, as required under Article 38.1, and not on the day before the system is due to be commissioned.

6.9. OPW Installed CCTV Systems in Owned or Leased Estate Portfolio

The OPW's security contractors have installed hundreds of CCTV systems in many of its owned or leased buildings, which other public sector bodies occupy as tenants. There are multiple tenants in these buildings in some cases. These CCTV systems were installed under a standard protocol to cover all entrances and car parks.

Article 4.7 of the GDPR defines a Controller as the organisation that determines the purposes and means of processing personal data, in this case identifiable CCTV images. Article 26 defines Joint Controllers as two or more Controllers who jointly determine the purposes and means of processing. Who is the Controller of these OPW-installed CCTV systems: the OPW, the tenant or are they both Joint Controllers? The purpose of these CCTV systems is clearly to protect the tenant's staff and property. The tenant, and not the OPW, decides any additional purpose(s) for which these CCTV systems are used. The tenant also decides on the means, i.e. the ways, in which the CCTV systems are used to achieve those purpose(s).

All the Data Protection issues involving CCTV, such as the legal basis, retention periods, dealing with requests to fulfil Data Subject rights and requests from An Garda Síochána for CCTV footage all flow from the purpose and means. The OPW has no day to day involvement with or control of the use of these CCTV systems, as this is done by the tenant, who decides on retention periods, deals with Data Subject requests or requests from the Gardaí and reviews the footage themselves where an incident occurs. For example, if a visitor suffers a personal injury in an accident on the premises, the tenant will ask the security contractor for the footage in order to review it. If the tenant's property is stolen and An Garda Síochána want the CCTV footage to investigate the crime, they will request it from the tenant, who will again request it from the security contractor. If Data Subjects want to exercise their GDPR rights in respect of their recognisable CCTV images, they will approach the tenant, as their name is over the door, and not the OPW. In general, a Data Subject cannot reasonably be expected to identify a property's landlord.

These OPW-installed CCTV systems are outside the scope of this Policy and are the sole responsibility of these tenants. Where a building has multiple tenants, the lead tenant, who occupies the largest area within the building, is responsible for the OPW CCTV systems. In its Processor contracts under Article 28, the OPW will instruct its security contractors to cooperate fully with all their tenants to fulfil their Data Protection obligations. The OPW will maintain the CCTV systems along with the other infrastructure of the building such as lifts and intruder alarms.

In some cases, tenants have installed their own additional CCTV systems. These additional systems are outside the scope of this Policy and remain the sole responsibility of the tenants who installed them.

6.10. Processors

Security contractors that operate CCTV systems on behalf of the OPW **are Processors**. Article 28 of the GDPR deals with Processors. The OPW should only use Processors who comply with the GDPR and protect the rights of Data Subjects. Processors must only process CCTV images on documented instructions from the OPW. Processors must not engage a sub-processor without the prior specific or general written authorisation of the OPW. OPW must have a binding legal contract with each of its Processors that specifies that the Processor:

a) Processes the CCTV images only on documented instructions from the OPW, especially regarding transfers of CCTV images to a third country or to an international organisation. Be particularly wary of Processors using a cloud-based provider (sub-processor) to process their data, especially US companies, as their security procedures may involve the replication (copying) of all the data, including OPW's identifiable CCTV images, from their EEA data centres to data centres outside it. Such replication is very easy to do and happens almost constantly. Large multinational sub-processor provide most cloud-based services. These have much greater market power than local processors in the Irish market and provide their service on a 'take it or leave it' basis

b) Ensure that persons authorised to process the CCTV images are committed to or are under an obligation of confidentiality

c) Takes all the technical and organisational measures required to provide the state of the art security as required by Article 32

d) Must not engage a sub-processor without the prior specific or general written authorisation of the OPW

e) Assists the OPW and its tenants to fulfil their obligations to Data Subjects in exercising their rights by providing appropriate technical and organisation methods to enable this

f) Assists the OPW and its tenants to fulfil its obligations in relation to security of processing, data breach notifications, Data Protection Impact Assessments, prior consultation and cooperation with the DPC as set out in Articles 32-36 of the GDPR

g) At OPW's choice, deletes or returns all CCTV image data to the OPW at the end of the contract

h) Provides all the information necessary to the OPW to allow compliance with Article 28 and to cooperate with audits undertaken by the OPW.

Under Article 82, any person who has suffered material or non-material damage as a result of an infringement of the GDPR will have the right to be compensated by the OPW or its Processor(s) for the damage suffered. Where more than one Processor, or both the OPW and a Processor, are involved in the same processing and where they are responsible for any damage caused by processing, each Controller or Processor shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject.

OPW business areas who engage third party companies to operate CCTV systems on their behalf must satisfy themselves that those companies can meet Data Protection requirements and must negotiate formal contracts in compliance with the GDPR. Essentially such contracts should detail what the security company may do with the CCTV data, what security standards should be in place and what verification procedures may apply.

6.11. Concessions (e.g. Cafés, Tea Rooms)

The OPW provides cafés, tea rooms, etc. by means of a concession arrangement. Where these use CCTV, as Article 4.7 defines a Controller as the organisation that determines the purposes and means of processing personal data, the concessionaire and **not** the OPW, is the Controller. The concessionaire is therefore obliged to meet the requirements of the GDPR and the Data Protection Acts 1988 to 2018 regarding the CCTV images it processes.

6.12. Records of Processing Activities Relating to CCTV Systems (Article 30)

It is acknowledged that the OPW CCTV estate has grown organically over the years and that various parties have installed many different CCTV systems over time. Furthermore, responsibility for managing the systems is distributed across many OPW business areas. Business Units should review their CCTV management procedures on an ongoing basis to ensure that they meet the OPW's Data Protection obligations as set out in this Policy.

Article 30 of the GDPR mandates that the OPW must establish and maintain a record of CCTV related processing activities under its responsibility as set out in Appendix 2. Online questionnaires requesting this information will be circulated to all OPW Business Units in the coming months and must be completed, accurately, as quickly as possible, in advance of 25 May 2018.

7. Queries

If you have queries or want clarifications about this policy, please direct them to the Data Protection Officer, based in the OPW's Trim HQ, whom you may contact at dpo@opw.ie. You can ring the DPO on the following numbers: (0761) 106000, (046) 942 6000, (01) 647 6000 or 1890 213 414 (LoCall). Should you wish to write to the DPO, the address is: Data Protection Officer, The Office of Public Works Head Office, Jonathan Swift Street, Trim, Co. Meath, Ireland, C15 NX36. You may also fax the DPO at (046) 948 1793.

APPENDIX 1: CCTV Warning Signs

Figure1: English Version of CCTV Warning Sign

IMAGES ARE RECORDED FOR THE PURPOSES OF SECURITY AND PERSONAL SAFETY

For further information email dpo@opw.ie

OPW
Oifig na nOibreacha Poiblí
The Office of Public Works

Figure 2: Irish Version of CCTV Warning Sign

DÉANTAR TAIFID DE ÍOMHANNA AR MHAITHE LE SLÁNDÁIL AGUS LE SÁBHÁILTEACHT PHEARSANTA

Tá tuilleadh eolais ar fáil ag dpo@opw.ie

OPW
Oifig na nOibreacha Poiblí
The Office of Public Works

Figure3: Bilingual Version of CCTV Warning Sign

Figure4: Smaller (A5) Bilingual Version of CCTV Warnin

APPENDIX 2: Data Mapping Information to be Collected for OPW CCTV Systems

Data Mapping Information to be Collected for OPW CCTV Systems		Needed for Article	
		13	30
Name and contact details of Controller:	The Commissioners of Public Works in Ireland E-mail: info@opw.ie Phone: (0761) 106000 / (046) 942 6000 / (01) 647 6000 / 1890 213 414 (LoCall) Post: The Office of Public Works Head Office, Jonathan Swift Street, Trim, Co. Meath, Ireland, C15 NX36. Fax: (046) 948 1793	Yes	Yes
Name and contact details of Joint Controller (where applicable):	N/A	No	Yes
Name and contact details of Controller's representative (where applicable):	N/A	Yes	Yes
Name of DPO:	Liam S. Kelly	No	Yes
Contact details of DPO:	E-mail: dpo@opw.ie Phone: (0761) 106000 / (046) 942 6000 / (01) 647 6000 / 1890 213 414 (LoCall) Post: Data Protection Officer, The Office of Public Works Head Office, Jonathan Swift Street, Trim, Co. Meath, Ireland, C15 NX36. Fax: (046) 948 1793	Yes	Yes
Purposes of the processing:	Security and Personal Safety	Yes	Yes
If any, additional desired purposes of processing for consideration by DPO/DPC		No	No
Legal basis for the processing:	For security, the legitimate interests of the Commissioners to protect themselves, their property their staff, contractors and visitors from criminal activity. For personal safety, the Safety, Health and Welfare at Work Act 2005 and Section 3 of the Occupiers' Liability Act, 1995	Yes	No
Legal basis for proposed additional processing		No	No

Data Mapping Information to be Collected for OPW CCTV Systems		Needed for Article	
		13	30
Legitimate interests pursued by Controller / third party where processing is based on this:	The legitimate interests of the Commissioners of Public Works in Ireland to protect themselves, their property, their staff, contractors and visitors from criminal activity.	Yes	No
Description of the categories of Data Subjects:	Staff, contractors, visitors	No	Yes
Description of the categories of personal data:	Identifiable CCTV images of Data Subjects, or other characteristics which indirectly identify them, such as vehicle registration numbers.	No	Yes
Recipients or categories of recipients to whom identifiable CCTV images have been/will be disclosed (including those in third countries or international organisations):	None	Yes	No
Categories of recipients to whom identifiable CCTV images have been/will be disclosed (including those in third countries or international organisations):	None	No	Yes
If identifiable CCTV images are transferred to a third country or international organisation:	No	Yes	Yes
Name of third country or international organisation to which identifiable CCTV images is being transferred (where applicable)	N/A	Yes	Yes
Document appropriate safeguards for transfers with no adequacy decision (Articles 46, 47 & 49.1):	N/A	Yes	No
Document appropriate safeguards for transfers with no adequacy decision (Article 49.1):	N/A	No	Yes
If possible, the period for which CCTV images are stored (retention period), otherwise criteria used to determine this period:	Normally a maximum of 28 days; 65 days in the case of possible personal injury claims; for the duration of any legal claims made against the OPW	Yes	No
Where possible, the envisaged time limits for erasure (retention period) of CCTV images:	Normally a maximum of 28 days; 65 days in the case of possible personal injury claims; for the duration of any legal claims made against the OPW	No	Yes

Data Mapping Information to be Collected for OPW CCTV Systems		Needed for Article	
		13	30
Where possible, general description of the technical and organisational security measures appropriate to level of risk (Article 32.1):		No	Yes
Site Operating CCTV:		No	No
OPW Business Area responsible for the site:		No	No
No. of CCTV Cameras deployed at site:		No	No
Contact details for OPW site manager responsible for CCTV:		No	No
Name and contact details of Processor (company) operating CCTV system on OPW's behalf:		No	No
Name and contact details of Processor's representative (where applicable):		No	Yes
Name of Processor's DPO:		No	Yes
Contact details of Processor's DPO:		No	Yes
Categories of Processing carried out on behalf of OPW:		No	Yes
Transfers of identifiable CCTV images by Processor to a third country or international organisation (where applicable):		No	Yes
Name of third country or international organisation to which identifiable CCTV images is being transferred by Processor (where applicable):		No	Yes
Document appropriate safeguards for transfers by Processor without adequacy decision (Article 49.1):		No	Yes
Where possible, general description of the Processor's technical and organisational security measures appropriate to level of risk (Article 32.1):		No	Yes

Data Mapping Information to be Collected for OPW CCTV Systems		Needed for Article	
		13	30
Year of original installation:		No	No
Procedure for storing CCTV data (equipment used, location and who manages the process):		No	No
Details of personnel who have access to CCTV system:		No	No
Logging procedure for accessing CCTV footage:		No	No
Other relevant information:		No	No