Údarás Sábháilteachta Bia na hÉireann
Food Safety Authority of Ireland

Closed Circuit Television (CCTV) Policy

2025

Version: Public

Publication date	Original	Current
	1 June 2023	2 April 2025
Review details	Last reviewed	Next review
	31 March 2025	31 March 2027
Policy Owner	Data Protection Officer (DPO)	
Authorised by	Senior Leadership Team	
Date of Authorisation	31 May 2023	
Revision No.	1	

Contents

Closed Circuit Television (CCTV) Policy

Introduction

Images captured by Closed Circuit Television (CCTV) systems are personal data. Consequently, they are subject to the provisions of the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and related legislation.

This policy sets out the basic conditions of use for CCTV systems in the Food Safety Authority of Ireland (FSAI) premises located at The Exchange, Georges Dock, IFSC, Dublin 1. It is designed to inform relevant parties about the safeguards in place with regard to the operation of, and access to, the CCTV systems used at the FSAI premises and the resultant images. This CCTV policy is available on the website and a copy can be provided to visitors and other third parties on request.

Purpose of policy

The purpose of this policy is to ensure that the FSAI's use of CCTV complies with relevant legislation, regulations and standards. These include, but are not limited to, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Scope

This policy covers the monitoring, recording, use and storage of such recorded material. It applies to all staff and visitors to the FSAI. Other cameras are in operation in common areas of The Exchange building outside of the FSAI offices. These are the responsibility of IPUT plc which owns the building. Consequently, they are outside the scope of this policy and the responsibility of the FSAI.

Ownership of the CCTV system

All material recorded within the FSAI offices is the property of the FSAI. The FSAI is the data controller.

Purpose of CCTV system

The purpose of CCTV surveillance at the FSAI premises is:

- to increase the safety of staff, contractors and visitors to the FSAI's premises
- to act as a deterrent against criminal activity affecting property belonging to the FSAI, FSAI staff, contractors and visitors.

CCTV is used to monitor access to the FSAI office, Reception area and fire exits. The system will not be used to systematically monitor the movements of staff, contractors or visitors.

However, images obtained of persons committing acts of an illegal nature and/or acts which breach the FSAI's rules and regulations may be used as evidence in any subsequent investigation.

Legal basis

The GDPR requires that all data controllers have a legal basis to process personal data. The legal basis permitting the processing of CCTV images for the above purposes is Article 6(1)(f) of the GDPR. This is where the processing is necessary for the legitimate interests pursued by FSAI and its users.[1]

Operation of CCTV system

The FSAI's CCTV system is password protected and can only be accessed by the Facilities Team and Gallant Security Systems (the CCTV system maintenance company). The Facilities Manager has overall responsibility for the operational management of CCTV equipment.

Siting of cameras and signage

The FSAI undertakes to ensure that all cameras are fixed and sited in such a way that only areas intended to be monitored will be covered by the cameras. CCTV recording will be avoided in areas where staff, contractors and visitors have an increased expectation of privacy (such as break rooms and restrooms). Regular checks and reviews are undertaken to ensure that CCTV cameras are working effectively and appropriately in accordance with this policy.

Signage is displayed at prominent locations throughout the office so that staff, contractors and visitors are aware that CCTV cameras are in use. The text and layout of this signage is provided in Appendix I.

Quality of images

It is important that images produced by the CCTV are fit for the stated purpose. The equipment and recordings will be regularly maintained to ensure consistent quality of images.

Retaining information and processing images

Recordings are securely stored on a password protected 4 terabyte hard drive. Viewing is restricted to authorised personnel. The FSAI will only retain CCTV footage for 38 calendar days. Once the 38-day period has expired, the recordings will be destroyed. In the event of receipt of a request for a specific piece of footage, the Facilities Manager must be contacted immediately. He/she/they will arrange for the relevant footage to be saved onto a suitable storage device and retained as necessary for the purposes of dealing with the access request and any subsequent appeal.

[1] Article 6.1: 'Processing shall be lawful only if and to the extent that at least one of the following applies: (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

Data Subject Access Requests (DSARs)

Disclosure of images from the CCTV system is controlled and consistent with the purposes for which the system exists. Individuals have the right to access his/her/their personal data. This includes the person's image in CCTV recordings. Requests should be made in writing to the DPO at the FSAI. This may be done by either writing to, or emailing, the DPO at the following addresses:

By post: Data Protection Officer
Food Safety Authority of Ireland
The Exchange
Georges Dock, IFSC
D01 P2V6
Dublin 1

By email: DPO@fsai.ie

Requests must include the date, time and location where the CCTV footage was recorded. The requester will be asked to provide valid identification.[2] The FSAI aims to respond promptly and within one month of receiving a valid request. A form has been provided in Appendix II which may be used by requesters.

Preparing footage for release

Downloading of footage is carried out by the Facilities Manager. Recorded material is handled with care and in a confidential manner to ensure complete regard for individual privacy. Footage is downloaded onto a secure suitable storage device. A copy is given to the requester and a copy is retained by FSAI in a secure location. Where CCTV images reveal other individuals, their faces may be pixilated so that they are not recognisable.[3] The footage in question is retained until the purpose for which it was downloaded has ended, at which point the footage is securely and permanently destroyed.

If an individual has concerns about CCTV footage, he/she/they are welcome to raise these with the FSAI's DPO. The DPO may be contacted at the two addresses provided above.

Third-party access

On occasion, the FSAI may be asked to disclose CCTV recordings to third parties for a purpose other than that for which they were originally obtained. This may include, but is not limited to, the following:

- An Garda Síochána or another law enforcement body requesting that footage be provided to assist in the investigation of a criminal offence.
- Building Management.

[2] Before a person is given access to personal information relating to themself, he/she/they will be asked to provide proof of identity. These are as follows: (i) a copy of identification bearing the person's full name and photograph (for example, a passport, driver's licence, etc.); and (ii) proof of address to which the materials will be sent (for example, the top of a utility bill bearing both the person's name and address – this must be less than 6 months old). This information is requested to ensure that information is released to the appropriate person and postal/email address.

[3] The cost of pixelation, and who is to bear this cost, will be determined based on the duration of the CCTV footage. Depending on the individual recording, the cost may be borne by the requester and not the FSAI.

- Members of the FSAI's staff involved with the grievance, disciplinary or dignity at work procedures.
- Legal or insurance representatives of data subjects (with written consent of data subjects).[4]
- FSAI's insurers/assessors.
- In exceptional cases, to others to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident.
- CCTV companies for service/repair.

All third-party access requests must be in writing using the CCTV Requests - Third Party Access Request Form which is provided in Appendix III. These may be posted or emailed to the FSAI's DPO at either of the addresses provided above.

All third-party requests for access to CCTV footage will be dealt with on a case-by-case basis to ensure that the principles of data protection are adhered to, and the rights of individuals are not prejudiced. For practical purposes, and to expedite a request in urgent situations, a verbal request may be sufficient to allow for the release of and/or to hold the footage sought to An Garda Síochána. However, any such verbal request should be followed up with a formal written request. A record of all third-party access requests is maintained by the FSAI detailing any provision of footage and to whom.

Accessing footage and identification

All individuals requesting access to CCTV footage will be asked for up-to-date photographic identification (for example, passport, driver's licence, etc.). Members of An Garda Síochána will be asked for identification and badge number.

Those seeking access on behalf of another will be required to provide written consent from the person they are representing. If the request is for a family member, proof of relationship may be also requested.

Unauthorised access

Anyone who uses the CCTV system or accesses CCTV images in an unauthorised manner may be subject to investigation, disciplinary and/or legal action. Unauthorised use is any processing incompatible with the original purpose for collecting this data including, but not limited to, the following:

- Disclosure of images containing personal data to an unauthorised third party, including other employees.
- Unauthorised processing of personal data in the form of copying the images on to a disc, website or print format.
- Circulation of images containing personal data by email or posting of images containing personal data on the internet.

Compliance with this Policy

All employees who are responsible for implementing, managing, operating or using the CCTV system must do so only as authorised and in accordance with this policy. Any failure to comply with this policy may be a disciplinary offence up to and including dismissal.

[4] Written consent should be provided by the data subject/s in advance of any search being requested and subsequently, carried out.

Responsibility

It is the responsibility of the Data Protection Officer (DPO) to monitor this policy, its use and implementation by all staff and contractors of the FSAI.

Related documents

This policy should be read in conjunction with other FSAI policies, including:

- Data Protection Policy

The above list is not exhaustive and other policies may apply.

Document control

It is the responsibility of the Data Protection Officer (DPO) to ensure that this policy is updated at regular intervals for continued compliance.

Appendices

Appendix I: CCTV Sign

Tá íomhánna á dtaifeadadh chun críche sábháilteacht foirne/cuairteoir agus coireachta a chosc.

Déan teagmháil le do thoil: DPO@fsai.ie le haghaidh tuilleadh eolais.

Tá an scéim á rialú ag: An tÚdarás Sábháilteachta Bia na hÉireann.

Images are being recorded for the purpose of staff/visitor safety and crime prevention.

Please contact: DPO@fsai.ie for further information.

This scheme is controlled by: Food Safety Authority of Ireland

Appendix II: CCTV Requests – Data Subject Access Request Form

Údarás Sábháilteachta Bia na hÉireann
Food Safety Authority of Ireland

CCTV Requests
Data Subject Access Request Form

Details Of Requester	
Name	
Address	
Email Address	
Tel Number	
Details Of Request	
Under Article 15 of the GDPR, I request CCTV access as follows	View CCTV Footage ☐ Copy of CCTV footage ☐
Reason for request	
Date of recording	
Time of recording	
Start Download (time)	
End Download (time)	
Location of recording	

I acknowledge that, before I am given access to personal information about myself, I may be asked for ID. I acknowledge that I will not normally be given access to the personal information of another person unless I have obtained the written consent of that person.

Signed: _____ Date: _____

Send completed forms to: DPO, Food Safety Authority of Ireland, The Exchange, Georges Dock, D01 P2V6 or Email: dpo@fsai.ie

Office Use Only	Date	Time	Who By
System Download Requested			
Evidence/Authenticate			
Result			
Copied to Memory Stick			
Download Failed Report			

No of Copies Made		Ref No	
Copy 1 Given To		Date Given	
Copy 2 Given To		Date Given	
Copy 1 Received Back		Date	
Copy 2 Received Back		Date	
No of Still Photos		Date retained copy deleted	
Copies Given To		Date	

Signature of DPO: _____ Date: _____

Appendix III: CCTV Requests – Third Party Access Request Form

Údarás Sábháilteachta Bia na hÉireann
Food Safety Authority of Ireland

CCTV Requests
Third Party Access Request Form

Details Of Requester	
Name	
Address	
Garda Badge No. (where appropriate)	
Email Address	
Tel Number	
Details Of Request	
I request CCTV access as follows	View CCTV Footage ☐ Copy of CCTV footage ☐
Reason for request	
Date of recording	
Time of recording	
Start Download (time)	
End Download (time)	
Location of recording	

I acknowledge that, before I am given access to personal information about myself, I may be asked for ID. I acknowledge that I will not normally be given access to the personal information of another person unless I have obtained the written consent of that person.

Signed: _____ Date: _____

Send completed form to: DPO, Food Safety Authority of Ireland, The Exchange, Georges Dock, D01 P2V6, or Email: dpo@fsai.ie

Office Use Only	Date	Time	Who By
System Download Requested			
Evidence/Authenticate			
Result			
Copied to Memory Stick			
Download Failed Report			

No of Copies Made		Ref No	
Copy 1 Given To		Date Given	
Copy 2 Given To		Date Given	
Copy 1 Received Back		Date	
Copy 2 Received Back		Date	
No of Still Photos		Date retained copy deleted	
Copies Given To		Date	

Signature of DPO: _____ Date: _____

Appendix IV: Review of updated Guidance on the Use of CCTV – Data Protection Commission

Date of Review: 27 June 2024

Introduction

The Data Protection Commission (DPC) updated its 'Guidance on the Use of CCTV' in November 2023.[5] The DPC received a significant number of queries in 2023 relating to the use of CCTV in areas where there is a higher expectation of privacy. As a result, it updated its CCTV guidance to address these issues and individuals' expectations on the use of CCTV in such areas. The guidance now includes a specific section on 'The use of CCTV in areas of an increased expectation of privacy'.

Guidance

The guidance states that in general, data controllers should avoid using CCTV in circumstances where a reasonably high expectation of privacy exists. For example, individuals have the highest expectation of privacy when using changing rooms or the cubicles in toilet facilities. Using CCTV to monitor individuals in these specific areas will likely contravene the General Data Protection Regulation in nearly all circumstances, as the level of intrusiveness and impact on individuals will not be warranted in light of the purposes for its use. It will be challenging for data controllers to justify using CCTV in such areas and will require a rigorous examination of all data protection implications to individuals prior to deployment.

FSAI CCTV Policy

The Food Safety Authority of Ireland CCTV Policy (authorised 31 May 2023) states that 'CCTV recording will be avoided in areas where staff, contractors and visitors have an increased expectation of privacy (such as break rooms and restrooms)'.

Action Required

No action is required with regard to the FSAI CCTV Policy in light of the updated guidance from the DPC as CCTV is not used in areas where individuals have an increased expectation of privacy.

[5] The updated guidance is available at: https://www.dataprotection.ie/sites/default/files/uploads/2023-12/CCTV%20Guidance%20Data%20Controllers_November%202023%20EN.pdf