Code of Practice for the Operation of CCTV

for the Purposes of Prevention, Detection & Prosecution of Litter Offences

LGMA
Local Government Management Agency

CCMA
Cumann Lucht Bainistíochta Contae agus Cathrach
County and City Management Association

Rialtas Áitiúil Éireann
Local Government Ireland

This Code should be read in conjunction with the Litter Pollution Act 1997 as amended by the Circular Economy and Miscellaneous Provisions Act 2002 (the Act). For the avoidance of doubt, in the event of any conflict between this Code and the Act, the legislative provisions in the Act shall prevail.

Contents

Contents 3
1. Executive Summary 4
2. Purpose & Rationale for the Code of Practice 7
3. Definitions & Abbreviations 8
4. Law Enforcement Functions of Each Local Authority in respect of the Deterrence, Prevention, Detection & Prosecution of Litter Offences 12
5. Principles underpinning the use of CCTV for law enforcement purposes 14
6. Consultation on this Code 22
7. Establishing the need for CCTV before deciding to install a CCTV Scheme 23
8. Conducting a Local Data Protection Impact Assessment (Local DPIA) to establish the necessity and proportionality for a CCTV Proposal 26
9. Necessity for the Use of CCTV 27
10. Local consultation on intended CCTV implementation 25
11. Approval process by Oversight Board prior to CCTV Scheme being installed 29
12. Standard operating procedures for the use of CCTV 30
13. Identification of sites where CCTV may be introduced 31
14. Preparation of a Data Protection Impact Assessment 32
15. Preparation of a business case for submission to an Oversight Board 33
16. Appropriate signage when using CCTV for Law Enforcement Purposes under section 23A of the Act of 1997 34
17. Installation of CCTV on-site i.e. sighting and field of vision for CCTV installed on-site 35
18. Security & Controlling Access to CCTV 36
19. Records to be maintained by Local Authorities 37
20. Chain of custody 38
21. Disclosure of CCTV images and recordings 39
22. Data Subject Rights 41
23. Monitoring compliance with this Code of Practice 50

1. Executive Summary

The Litter Pollution Act, 1997 as amended by the Circular Economy and Miscellaneous Provisions Act, 2022 (**"the Act of 1997"**) requires a Local Authority to take all practicable measures for the prevention of the creation of litter and for the prevention and overcoming of the polluting effects of litter in its functional area. A Local Authority may enter into arrangements with, or assist, other persons (including other Local Authorities) for those purposes, or in the taking of such measures on behalf of the Local Authority.

Under section 23A of the Act of 1997, Local Authorities may operate CCTV schemes for the purposes of deterring environmental pollution, and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997. Pursuant to section 23B of that Act, the Local Government Management Agency (**"LGMA"**) is required to prepare and submit to the Minister for the Environment, Climate and Communications (**"the Minister"**) for his or her approval a draft code or codes of practice for the purposes of setting standards for the operation of Section 23A. Section 23B(2) outlines the provisions to be included in the draft codes for the use of CCTV Schemes under section 23A which are as follows:

(a) Carlow Corporate Booklet - A5 8 pager - amendments the procedure and standards to be followed in the operation of section 23A including in the installation of devices to be used in a CCTV scheme;

(b) confidentiality, security, storage, access to, retention, deletion, and any other processing of, data gathered in accordance with section 23A;

(c) the circumstances in which data gathered under section 23A is to be disposed of or destroyed;

(d) the rights of data subjects in so far as they relate to the operation of section 23A;

(e) such other matters, if any, related to the operation of section 23A that the LGMA considers appropriate,

and the code or codes of practice may contain different provisions in relation to different types of devices or systems, in relation to different categories of persons and in relation to the different circumstances in which such devices or systems are operated.

In preparation of this Code and, as required by Section 23B(3) of the Act of 1997, the LGMA prepared a Data Protection Impact Assessment (**"DPIA"**) on the likely impact on data subjects of the types of processing of personal data contemplated by the operation of CCTV schemes by Local Authorities pursuant to Section 23A. Before submitting the draft Code to the Minister, the LGMA provided the DPIA to, and also consulted with, the Minister; the Minister for Housing, Local Government and Heritage; the Minster for Justice; and the Data Protection Commission amongst other relevant stakeholders.

Pursuant to section 23A of the Act of 1997 where the Chief Executive of a Local Authority approves a proposal for a CCTV scheme, the scheme shall be operated in accordance with the code approved under section 23B.

The Minister has approved this code pursuant to Section 23B of the Act of 1997. Consequently, any proposal for a CCTV scheme approved by a Chief Executive of a Local Authority will be a proposal to operate the scheme in accordance with the present code.

The LGMA shall ensure that this Code is reviewed by it on a regular basis with the first review to be not later than 5 years from the date on which the Code is first approved by the Minister, and, in the case of each subsequent review, not later than 5 years from the date of the previous review.

This Code of Practice sets out the procedures and standards for the use of CCTV for the deterrence, prevention, detection, and prosecution of offences under the Act of 1997 that each Local Authority seeking to use CCTV for the stated statutory purpose must adhere to in order for their use of CCTV to comply with the Law Enforcement Directive (LED) as transposed by Part 5 of the Data Protection Act of 2018. The LED deals with processing of Personal Data by data controllers for law enforcement purposes and, as such, falls outside the scope of GDPR. Therefore, the processing of Personal Data by Local Authorities under this Code is subject to the compliance with the LED as transposed into Irish law and not the GDPR regime. As the LED is a directive as opposed to a regulation it requires transposition into Irish law to take legal effect. CCTV schemes can be used to capture footage that can support enforcement actions or prosecutions taken for law enforcement purposes under the Act of 1997.

CCTV cameras which are installed for the purposes covered by this Code may also be used for the purposes of preventing environmental pollution and for the purposes of the investigation, prevention, detection, and prosecution of offences under the Waste Management Act, 1996, as amended (**"the Act of 1996"**) , subject to the requisite approval from the Chief Executive issuing under the Act of 1996. A separate Code of Practice for the use of CCTV under the Act of 1996 has also been produced. CCTV cameras can be used to capture footage that can support enforcement actions or prosecutions taken under either of the two aforesaid pieces of legislation, where approval has been granted.

This sectoral Code recognises that the deployment of CCTV for Law Enforcement Purposes will vary according to the nature of litter offences as defined in the Act of 1997 that may arise in specific locations. As such, the Code does not seek to prescribe how CCTV should be deployed in all circumstances but rather seeks to define the parameters within which each Local Authority must operate when considering whether it is necessary and proportionate to deploy CCTV to tackle local litter offences.

This Code applies to the use of CCTV, which may include processing of personal data, by a Local Authority as a Competent Authority for Law Enforcement Purposes within the meaning of the LED and as such is outside the scope of GDPR. For information in relation to the processing of personal data by a Local Authority that is within the scope of GDPR please see the Data Protection Policy and/or Privacy Statement of each respective Local Authority.

In particular, the Code sets out the procedures to be followed by the various actors involved in considering a proposal for the use of CCTV and particularly for the role of an Oversight Board in vetting any such proposal and in making a recommendation in relation thereto to the Chief Executive of the relevant Local Authority, so that the Chief Executive, or his or her duly and specifically authorised delegate, can take an informed decision with regard to the proposal as to whether, and to what extent, to authorise the use of CCTV. Provided that any such delegate may not be a member of, or have participated in, the deliberations of the Oversight Board which recommended the Proposal under consideration for the use of the CCTV Scheme. These procedures, and the multi-layered nature of the decision making involved prior to the adoption of any decision to deploy CCTV, are designed to ensure the use of CCTV for law enforcement purposes pursuant to this Code, remains strictly necessary and proportionate in both its scope and its time of operation and that its use is, ultimately, balanced as fairly and as equitably as possible with the data privacy rights of data subjects whose data may be collected and processed during and/or arising from surveillance operations and/or activities involving CCTV.

2. Purpose & Rationale for the Code of Practice

The Circular Economy & Miscellaneous Provisions Act, 2022 (**"the Act of 2022"**) has been enacted to make provision for the use by a Local Authority of CCTV and mobile recording devices in certain circumstances and amends the Waste Management Act 1996 and the Litter Pollution Act 1997 accordingly.

Part 4 (i.e., sections 31-36 inclusive) of the Act of 2022 sets out the amendments to Sections 23A & 23B of the Act of 1997.

The statutory requirement for the Local Government sector to introduce a Code of Practice, which must be adhered to by all local authorities, and authorised persons governing the future use of CCTV for the purposes of the deterrence, prevention, detection, and prosecution of offences under the Act of 1997 is contained in Section 23B of the Act of 1997 as inserted by Section 33 (CCTV) of the Act of 2022.

Pursuant to section 23B of the Act of 2022, the LGMA is required to prepare and submit to the Minister for his or her approval a draft code or codes of practice for the purposes of setting standards for the operation of Section 23A.

This code of practice, which has been approved by the Minister pursuant to Section 33(5) of the Act of 2022, sets out a step-by-step approach for the implementation of a CCTV scheme in accordance with section 23A of the Act of 1997, and the procedures and standards that must be adhered to in order to comply with sections 23A & 23B of the Act of 1997.

3. Definitions & Abbreviations

'Act of 1996', means the Waste Management Act 1996 (as amended);

'Act of 1997', means the Litter Pollution Act 1997 (as amended);

'Act of 2018' means the Data Protection Act 2018 (as amended);

'Act of 2022', means the Circular Economy and Miscellaneous Provisions Act 2022;

'AGS' means an Garda Síochána;

'Approval', in relation to a proposal under section 23A(4) of the Act of 1997, means an approval given under section 23A(5) or renewed under section 23A(11) in respect of the CCTV scheme which is the subject of the proposal as defined in section 2 of the Act of 1997;

'Approved CCTV Scheme' means a CCTV scheme in respect of which an approval is in being as defined in section 2 of the Act of 1997;

'Authorised Person' means a person who is appointed in writing by a local authority to be an authorised person for the purposes of this Act or any provisions thereof as the local authority determines, as defined in section 2 of the Act of 1997;

'Automatic Number Plate Recognition device' or **'ANPR'** means a device which engages an automated method of recognising vehicle registration plates from a camera image as defined in section 2 of the Act of 1997;

'Biometric Data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data as defined in section 69(1) of the Act of 2018;

'Business Unit' means the department within a Local Authority that carries out specific functions of the Local Authority;

'CCTV Proposal' means a proposal for the installation and operation of a CCTV Scheme in accordance with Section 23A of the Act of 1997;

'CCTV Scheme' has the meaning given to it by section 23A(1) of the Act of 1997;

'Closed Circuit Television' or **'CCTV'** means a system of recording devices the signals of which are not made publicly available but are monitored, or are capable of being monitored, by a local authority as defined in section 2 of the Act of 1997;

'Code of Practice' or **'Code'** means this code of practice which has been approved by the Minister in accordance with section 23B of the Act of 1997 for the purposes of operating a CCTV scheme in accordance with section 23A of the Act of 1997;

'Competent Authority' has the meaning given to it by section 69(1) of the Act of 2018, subject, where applicable, to section 69(2) thereof;

'Controller' has the meaning given to it by section 69(1) of the Act of 2018;

'DPIA' means Data Protection Impact Assessment and has the meaning given to it by section 84 of the Act of 2018;

'Data Protection Laws' means all applicable national and EU data protection laws, regulations, and guidelines, including but not limited to the Act of 2018, GDPR and any guidelines and codes of practice issued by the DPC;

'Data Processing Agreement' or **'DPA'** means contract in writing between a Controller and a Processor that complies with the requirements in section 80 of the Act of 2018;

'Data Subject' means an individual to whom personal data relate as defined in section 69(1) of the Act of 2018;

'DPC' means Data Protection Commission being the national independent supervisory authority for GDPR and the LED in the State;

'DPO' means Data Protection Officer;

'DSAR' means Data Subject Access Request within the meaning of section 91 of the Act of 2018;

'EPA' or 'the Agency' refers to the Environmental Protection Agency which is a statutory agency established by the Environmental Protection Agency Act 1992. The EPA is responsible for protecting and improving the environment as a valuable asset for the people of Ireland.

'Facial Recognition Device' means a device or system of devices which, through automated use of biometric data, matches or categorises facial images captured by the device as defined in section 2 of the Act of 1997;

'GDPR' means the General Data Protection Regulation EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

"Law Enforcement Purposes" includes processing of personal data for the purposes of preventing, investigating, detecting or prosecuting criminal offences including the safeguarding against, and the prevention of, threats to public security, or the execution of criminal penalties by means that are wholly or partly automated, or where the personal data form part of, or are intended to form part of, a relevant filing system, are not automated, as defined in section 70(1) of the Act of 2018;

'Law Enforcement Purposes under Section 23A of the Act of 1997' means the processing of Personal Data for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997;

'LED' means the Law Enforcement Directive EU Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, which was transposed into Irish Law by part 5 of the Act of 2018 in May 2018. The LED governs the processing of personal data for Law Enforcement Purposes only by a data controller who is a competent authority within the meaning of the LED;

'LGMA' means the Local Government Management Agency;

'Litter' has the meaning given to it in section 2 of the Act of 1997;

'Litter Warden" means a person authorised by a local authority to perform, on behalf of the local authority, the functions of the local authority and of a litter warden under the Act of 1997;

'Local Authority' has the meaning given to it by section 2(1) of the Local Government Act, 2001 (as amended);

'Local DPIA' means a DPIA to be conducted by each Local Authority before a Proposal for a CCTV Scheme is submitted by the Business Unit within the Local Authority to the Oversight Board for assessment in accordance with this Code;

'NTFSO' means the National TransFrontier Shipment of Waste Office;

'Operation', means in relation to closed circuit television, the maintenance and monitoring of closed-circuit television;

'Oversight Board' means the internal management and governance structure to be established by each Local Authority in accordance with this Code;

'Personal Data' means Information relating to –

(a) an identified living individual, or

(b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to -

(i) an identifier such as a name, an identification number, location data, an online identifier, or

(ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the individual,

as defined in section 69(1) of the Act of 2018.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed as defined in section 69 of the Act of 2018;

'Processing' any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, including:

(a) the collection, recording, organisation, structuring, or storing of the data,

(b) the adaptation or alteration of the data,

(c) the retrieval, consultation, or use of the data,

(d) the disclosure of the data by their transmission, dissemination or otherwise making available,

(e) the alignment or combination of the data, or

(f) the restriction, erasure, or destruction of the data,

as defined in section 69(1) of the Act of 2018;

'Processor' means an individual who, or a legal person, public authority, agency, or other body that, processes Personal Data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment as defined in section 69(1) of the Act of 2018;

'Profiling' means any form of automated processing of Personal Data consisting of the use of the data to evaluate certain personal aspects relating to an individual, including to analyse or predict aspects concerning the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements;

'Recording Device' means a device that is capable of recording or processing, or both, visual images or audio, or both, on any medium, from which a visual image or moving visual images may be produced and includes any accompanying document, and, where only visual images or moving visual images are concerned, includes any sound accompanying those images but does not include automatic number plate recognition devices or facial recognition devices as defined in section 2 of the Act of 1997;

'SOPs' means Standard Operating Procedures which will be developed by Local Authorities for use by Business Units within Local Authorities seeking to introduce and implement CCTV schemes in accordance with Section 23A of the Act of 1997 and this Code; and

'WERLAs' means the Waste Enforcement Regional Lead Authorities.

4. Law Enforcement Functions of Each Local Authority in respect of the Deterrence, Prevention, Detection & Prosecution of Litter Offences

Part V of the Act of 1997 provides that each Local Authority shall be responsible for the enforcement of the relevant provisions of the Act of 1997. Prosecutions taken by a Local Authority against an individual identified as having allegedly breached the provisions of the Act of 1997, place the processing of any Personal Data envisaged thereunder as falling within the scope of the LED as transposed into Irish law by Part 5 of the Act of 2018 and outside the scope of GDPR. The following provisions are laid down in Parts II – Part V of the Act of 1997:

Part II –Litter Pollution Generally:
- Prohibitions related to littering;
- Obligations of certain persons to prevent Litter;
- Certain activities that are not prohibited; and
- Duty of occupiers regarding littering.

Part III – Local Authority Functions & Duties Generally:
- Duty respecting public roads;
- Prevention of the creation of Litter;
- Notices requiring the removal of Litter;
- Litter Management Plan; and
- Requirements of a Litter Management Plan.

Part IV - Littering Related Matters:
- Obligations relating to mobile outlets;
- Powers of Local Authorities to require the taking of special measures regarding litter by certain operations;
- Powers of Local Authorities to require the taking of special measures regarding litter creation by major events;
- Prohibition of articles and advertisements on and defacement of certain structures;
- Power of Local Authorities to make bye-laws in relation to litter; and
- Dog related offences.

Part V - Enforcement:
- o Offences involving litter wardens and powers of litter wardens;
- o Operation of CCTV Schemes for law enforcement purposes;
- o Codes of Practice relating to the operation of CCTV Schemes;
- o Admissibility of evidence captured by CCTV;
- o Punishment for offences;
- o Offence related provisions including recovery of costs incurred by a Local Authority and enforcement of fines;
- o Evidence in relation to certain offences;
- o Vehicle related offences; and
- o Fixed penalty notice of certain offences may be given by litter wardens or dog wardens.

Part V of the Act of 1997 provides that each Local Authority shall be responsible for the enforcement of the relevant provisions of the Act of 1997. Prosecutions taken by a Local Authority against an individual identified as having allegedly breached the provisions of the Act of 1997, place the processing of any Personal Data envisaged thereunder as falling within the scope of the LED as transposed into Irish law by Part 5 of the Act of 2018 and outside the scope of GDPR. The following provisions are laid down in Parts II – Part V of the Act of 1997:

Part II –Litter Pollution Generally:
- Prohibitions related to littering;
- Obligations of certain persons to prevent Litter;
- Certain activities that are not prohibited; and
- Duty of occupiers regarding littering.

Part III – Local Authority Functions & Duties Generally:
- Duty respecting public roads;
- Prevention of the creation of Litter;
- Notices requiring the removal of Litter;
- Litter Management Plan; and
- Requirements of a Litter Management Plan.

Part IV - Littering Related Matters:
- Obligations relating to mobile outlets;
- Powers of Local Authorities to require the taking of special measures regarding litter by certain operations;
- Powers of Local Authorities to require the taking of special measures regarding litter creation by major events;
- Prohibition of articles and advertisements on and defacement of certain structures;
- Power of Local Authorities to make bye-laws in relation to litter; and
- Dog related offences.

Part V - Enforcement:
- Offences involving litter wardens and powers of litter wardens;
- Operation of CCTV Schemes for law enforcement purposes;
- Codes of Practice relating to the operation of CCTV Schemes;
- Admissibility of evidence captured by CCTV;
- Punishment for offences;
- Offence related provisions including recovery of costs incurred by a Local Authority and enforcement of fines;
- Evidence in relation to certain offences;
- Vehicle related offences; and
- Fixed penalty notice of certain offences may be given by litter wardens or dog wardens.

5. Principles underpinning the use of CCTV for law enforcement purposes

Article 8 of the LED states that Member States shall provide for processing of Personal Data to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a Competent Authority for the purposes set out in Article 1(1) of the LED i.e., Law Enforcement Purposes and that it is based on Union or Member State law. It also states that Member State law regulating processing within the scope of the LED shall specify at least the objectives of processing, the Personal Data to be processed and the purposes of the processing. Section 71(2)(a) of the Act of 2018 lays down a lawful basis for processing Personal Data when it is for Law Enforcement Purposes and necessary for the performance of a function of the Controller.

Chapter 2 (Section 71) of the Act of 2018 identifies the general principles of data protection that underpin the processing of Personal Data for law enforcement purposes under the LED (the Principles).

These Principles, which are listed below, place specific obligations on a Local Authority as a Controller.

General Principles
The data protection principles, in section 71 of the Act of 2018, are summarised below:

5.1 Principle 1 – the data shall be processed lawfully and fairly

Lawfulness

5.1.1 Section 71(2)(a) of the Act of 2018 states that processing of Personal Data shall be lawful where, and to the extent that –
(a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70 (1)(a) [Law Enforcement Purposes] and the function has a legal basis in the law of the European Union or the law of the State.

Personal Data.

5.1.2 Section 23A of the Act of 1997 provides a lawful basis for a Local Authority to set up a CCTV Scheme in accordance with that section and with this Code for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997, which is a function of Local Authorities.

5.1.3 A Local Authority as a Controller and Competent Authority within the meaning of the LED as transposed into Irish Law by Part 5 of the Act of 2018 may rely on section 23A of the Act of 1997 and section 71(2)(a) of the Act of 2018 as a lawful basis for processing Personal Data captured by CCTV for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997.

5.1.4 In order for any processing of Personal Data carried out by a Local Authority for Law Enforcement Purposes under section 23A of the Act of 1997 and section 71(2)(a) of the Act of 2018 to be lawful, it must be necessary. This means that the processing must be a targeted and proportionate way of achieving the purpose. As such, if a Local Authority can reasonably achieve the purpose by some other less intrusive means, the processing shall not be considered lawful. Consequently, the necessity, or otherwise, for data processing arising from the use of CCTV must always be an important consideration for Local Authorities in deciding whether to authorise the use of CCTV in any given situation.

Transparency and Fairness

5.1.5 The LED as transposed into Irish law by Part 5 of the Act of 2018, requires organisations to be open and transparent in their processing of Personal Data, so that reasonable expectations are set with the Data Subject regarding the likely use and disclosure of their Personal Data. As Controller of the Personal Data collected through CCTV schemes authorised in accordance with section 23A of the Act of 1997, each Local Authority is obliged to provide Data Subjects with information about what their data is being used for, and the legal basis for that processing. In addition, the Data Subject shall be informed as to whether their Personal Data will be shared, and if so, with whom.

5.1.6 Where Personal Data relating to a Data Subject are collected from the Data Subject, the Local Authority as the Controller shall, at the time when Personal Data are obtained, provide the Data Subject with all of the following information:

(a) the identity and the contact details of the Controller;
(b) the contact details of the DPO of the Controller, where applicable;
(c) the purpose for which the Personal Data are intended to be processed or are being processed;
(d) information detailing the right of the Data Subject to request from the controller access to, and the rectification or erasure of, the Personal Data;

(e) information detailing the right of the Data Subject to lodge a complaint with the Commission and the contact details of the Commission;
(f) in individual cases where further information is necessary to enable the Data Subject to exercise his or her rights under this Part, having regard to the circumstances in which the Personal Data are or are to be processed, including the manner in which the data are or have been collected, any such information including:

(i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data;
(ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;
(iii) where applicable, each category of recipients of the data.

Each Local Authority operating a CCTV Scheme shall provide all passers-by with sufficient and adequate notice by way of placing appropriate signage outside the boundary of the line of sight of cameras operating in relation to an Approved CCTV Scheme prior to entering or coming into contact with any Local Authority CCTV operations. This will provide any individual with the opportunity to be given a fair opportunity to be informed of the intended processing, and to also have the option not to have their Personal Data captured. A Privacy Statement or Policy for CCTV usage shall be made available to the public on each Local Authority website.

5.1.7 The content of the Privacy Statement or Policy or the signage, as the case may be, shall:
- Use clear and plain language;
- Be easily noticed and legible;
- Ensure Data Subjects understand that CCTV will be in operation;
- Ensure a picture/icon of the camera will be placed on the signage (indicating image recording in operation);
- Outline the purpose of the processing i.e., to deter, detect, prevent, and prosecute offences under the Act of 1997;
- Identify the Data Controller;
- Provide contact details for the DPO of the Data Controller, should a member of the public wish to contact them seeking further information; and
- Provide information about how Data Subject can exercise their rights including their right of appeal to the DPC.

5.2 Principle 2 – the data shall be collected for one or more specified, explicit, and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes

5.2.1 The purpose of retaining and processing a Data Subject's Personal Data must be specified when the data is collected. Once attained, the data cannot be used for alternative or secondary purpose unless the processing is compatible with the purpose for which the Personal Data were initially collected or otherwise permitted by law. This Principle is designed to safeguard the Data Subject from having their data further processed for a variety of purposes not envisaged when their data was initially collected, and which is not lawful.

5.3 Principle 3 – the data shall be adequate, relevant, and not excessive in relation to the purposes for which they are processed

5.3.1 The processing of excessive amounts of Personal Data is unnecessary and detrimental to the rights of the Data Subject and must be avoided. The Personal Data which will be processed by each Local Authority shall whilst adequate, be relevant and restricted to what is necessary for the processing purposes in order to achieve the stated objective. This requires, in particular, ensuring that CCTV equipment should be recording for the minimum amount of time that is consistent with the purposes for which the cameras have been deployed.

Local Authorities shall implement appropriate technical and organisational measures and necessary safeguards into the processing of Personal Data arising from the installation of a CCTV Scheme under this Code. See Section 7 for more detail.

5.4 Principle 4 – the data shall be accurate, and, where necessary, kept up to date

5.4.1 In order for the footage captured by an Approved CCTV Scheme to be used for Law Enforcement Purposes under Section 23A of the Act of 1997, it is critical that each Local Authority's Information System team ensures that all devices shall be maintained and serviced regularly, and that any timing, clock, or geo-location facilities are synchronised and verified. Otherwise, there is a risk that unsynchronised footage could introduce doubt and inconsistency into the captured data, rendering it useless for investigative or enforcement purposes. It is strongly recommended that the lens and focus on any CCTV camera is regularly cleaned and calibrated to ensure that the images captured are legible and intelligible for the purpose(s) for which they are processed.

5.5 Principle 5 – the data shall be kept in a form that permits the identification of a Data Subject for no longer than is necessary for the purposes for which the data are processed

5.5.1 Personal Data shall only be held in a form which allows identification of the Data Subject only for as short a time as possible and shall then be anonymised or erased. As early as possible in the life cycle of the data, the Local Authority must have processes in place to remove any identifying reference to the Data Subject.

5.5.2 Data captured by an Approved CCTV Scheme which supports an enforcement action or prosecution for an offence under the Act of 1997 will be kept for the duration for which such proceedings are in progress plus any period required for appeals purposes. Personal Data collected and not required for enforcement or prosecutions must be permanently deleted from a Local Authority's IT system. Video footage captured by an Approved CCTV Scheme and not required for a prosecution must be deleted within 28 days from capture unless a Local Authority is otherwise required by law to retain it for a longer period.

5.6 Principle 6 – the data shall be processed in a manner that ensures appropriate security of the data

5.6.1 In order to preserve Personal Data integrity and privacy, the security and stability of the Personal Data shall be protected by each Local Authority and any associated Processors via appropriate technological and organisational measures which will be specified in SOPs to be developed locally by a Local Authority. The impact of a Personal Data Breach on a Local Authority may be damaging, and care must always be taken when responding to Personal Data Breaches. Aside from the fines and penalties which may be associated with such a breach, the reputation of a Local Authority could be adversely impacted as well as public confidence.

5.6.2 Data collected by an Approved CCTV Scheme will be recorded either at a CCTV control room or on-site at the camera's location. The methodology will depend upon whether the CCTV cameras are capable of providing real time footage directly to the CCTV control room. CCTV footage will be downloaded from the on-site camera to a secure encrypted software platform where access will be restricted to authorised Local Authority staff and/or Authorised Persons. Encrypted Local Authority storage platform must be auditable and be capable of generating data logs, if required, which can demonstrate when and if Personal Data was consulted by any person or whether Personal Data was disclosed or transferred to another person, in the automated processing systems of a Local Authority.

5.6.3 Under the section 86 of the Act of 2018, where a Personal Data Breach occurs, the Controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the DPC of the breach.

Where the notification to the Commission is not made within 72 hours, the notification shall be accompanied by the reasons for the delay. Each Local Authority must have its own Personal Data Breach Policy & Procedure and shall also implement an access control and password policy to protect systems and information from unauthorised use or access.

5.6.4 Under section 87 of the Act of 2018 where a Personal Data Breach occurs that is likely to result in a high risk to the rights and freedoms of a Data Subject, the Controller shall, without undue delay, notify the Data Subject to whom the breach relates, unless the Local Authority has:

(i) implemented appropriate technological and organisational protection measures that were applied to the Personal Data affected by the Personal Data Breach, in particular where the said measures, including encryption, render the Personal Data unintelligible to any person who is not authorised to access it; or

(ii) taken measures in response to the Personal Data Breach that ensure that the high risk to the rights and freedoms of a Data Subject from the breach is no longer likely.

5.7 Principle 7 - Storage Limitation & Retention Periods

5.7.1 A Local Authority shall ensure that an appropriate time limit is established for the erasure of Personal Data captured by an Approved CCTV Scheme or the carrying out of periodic reviews of the need for the retention of Personal Data captured by an Approved CCTV Scheme. A Local Authority shall ensure, by means of procedural measures, that the time limit set down for erasure of the Personal Data is observed.

5.7.2 Data shall be held in a form that allows identification of the Data Subject only for as short a time as possible and shall then be anonymised or erased. As early as possible in the life cycle of the data, the Local Authority shall have processes in place to remove any identifying reference to the Data Subject unless it is required for evidence in court proceedings. Data collected from unauthorised waste premises will be retained until enforcement action is concluded and all appeals exhausted by the Occupier of the Premises. Retention periods may exceed the stated timeline where legal actions are still ongoing or the data in question is to be further processed in accordance with this Code or otherwise as permitted under law.

5.7.3 The retention period applicable to Personal Data captured by an Approved CCTV Scheme will vary due to the intended evidential purpose that data may serve. Initial retention periods shall be reviewed by a Local Authority and reset when informed by experience. A proportionate approach should always be used to inform retention periods, and these should not be based upon infrequent and/or exceptional cases.

5.7.4 Personal Data collected and assessed as not required shall be manually deleted from Local Authority secure encrypted storage platform within 28 days from capture in accordance with Local Authority policy.

5.7.5 The National Records Retention Policy document for Local Authority Records will also inform Local Authority policies on data retention and will be appended where applicable to the Local Authority policy.

5.8 Principle 8 – Third Party Organisations and Data Processor Agreements

5.8.1 A Local Authority may instruct third party service providers to assist it with performing its functions under the Act of 1997. Such service providers are recognised as Data Processors under the LED, as transposed by Section 80 of the Act of 2018 and a written contract or Data Processing Agreement (DPA) must be in place between a Local Authority and each Processor which complies with the requirements of section 80 prior to the commencement of processing.

5.8.2 Section 80(2) of the Act of 2018 sets out considerable, detailed obligations for Processors. A Local Authority shall adopt a proactive stance with regard to negotiating and concluding DPAs that are compliant with the legislation. Section 80 stipulates that a DPA must set out:

- The subject-matter and duration of the processing;
- The nature and purpose of the processing;
- The type of Personal Data and categories of Data Subjects; and
- The obligations and rights of the Local Authority as the data controller.

5.8.3 A DPA shall, at a minimum, stipulate that the Processor will:

i. Process the Personal Data only on the basis of documented instructions of a Local Authority, except in so far as the law of the European Union or the law of the State requires the processor to act otherwise;
ii. procure the services of another processor (in this section referred to as a "secondary processor") in relation to the processing only where authorised to do so in advance and in writing by the controller, which authorisation may be specific or general in nature;
iii. Not transfer Personal Data to a country outside of the European Economic Area (EEA);
iv. Ensure that any persons authorised to process the Personal Data have committed themselves clearly and in writing to protect the confidentiality of the Personal Data;
v. Provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that the processing shall comply with the provisions of section 80 and the rights and freedoms of the Data Subjects are protected;
vi. Undertake to assist a Local Authority by implementing appropriate technical and organisational measures, to fulfil the Local Authorities obligations towards the Data Subject's rights;
vii. At the end of the provision of data processing services, delete or return all the Personal Data to the Local Authority, and delete existing copies unless EU or relevant Member State law requires storage of the data; and
viii. Make available to a Local Authority all information necessary to demonstrate compliance with the obligations laid down in the LED as transposed into Irish law by Part 5 of the Act of 2018 allowing for and contributing to audits, including inspections, conducted by the Local Authority or another auditor mandated by the Local Authority.

Moreover, where a Processor is authorised to and wises to enlist another processor (secondary processor) for carrying out specific processing activities on behalf of a Local Authority, it shall be the responsibility of the Processor to ensure that the same level of protection exists for the Personal Data during this element of the processing by the secondary processor, as exists between the Local Authority and the Processor itself. The Processor shall ensure that a contract providing equivalent protection is entered with it by the secondary processor.

5.9 Principle 9 – Accountability

5.9.1 Each Local Authority must be able to actively demonstrate compliance with the Principles set out above which are laid down in the LED as transposed into Irish Law by Part 5 of the Act of 2018. A Local Authority must be capable of demonstrating its compliance in terms of the organisational, procedural and systems solutions which are in place to protect the Personal Data and comply with the Principles.

6. Consultation on this Code

Consultation and engagement are important as it provides an opportunity to identify any potential concerns and modify the Code of Practice to achieve a balance between the functions of a Local Authority vis-à-vis environmental protection and individual privacy rights. Section 23B(4) of the Act of 1997 requires that there shall be consultation with various bodies. Section 23B(4) specifically states as follows:

> "Before submitting a draft code or codes of practice to the Minister under this section, the Local Government Management Agency—
> (a) shall consult with—
> (i) the Minister,
> (ii) the Minister for Housing, Local Government and Heritage,
> (iii) the Minister Justice, and
> (iv) the Data Protection Commission
>
> (b) shall provide the assessment referred to in subsection (3) to the persons referred to in paragraph (a) before consulting with those persons, and
>
> (c) may consult with any other person or body appearing to the Local Government Management Agency to have an interest in the operation of section 23A and such other person that the Minister may direct."

As part of this consultation process a high level DPIA on the proposed use of CCTV was prepared and submitted to the DPC. This DPIA applied to the projected use of CCTV in all 31 Local Authorities for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997. Individual Local Authorities are required to engage in appropriate consultation with the public, as part of the Local DPIA process (see below for more details).

7. Establishing the need for CCTV before deciding to install a CCTV Scheme

A CCTV Scheme in this Code of Practice refers to CCTV that may be used solely for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997.

Where a Local Authority considers that the installation and operation of a CCTV Scheme may be an appropriate use of technology for the achievement of the Law Enforcement Purposes under Section 23A of the Act of 1997. Business Units who intend to submit a CCTV Proposal under the provisions of this Code of Practice to the Oversight Board must demonstrate the necessity and proportionality for the intended CCTV Scheme by means of a Local DPIA before the Oversight Board will be in a position to recommend its installation to the Chief Executive for final approval. CCTV shall only be introduced to address/resolve an identifiable and specific problem constituting offences under the Act of 1997.

To that end CCTV shall only be deployed for specific operational tasks in specific designated locations and not used for general patrol/surveillance. i.e., CCTV Schemes are not to be used to routinely monitor the movements of members of the public. CCTV will assist Local Authority Litter Wardens to deliver a more effective enforcement by:

- Enabling the best use of resources, resolving incidents more quickly thereby providing efficiencies;
- Targeting of enforcement action insofar as an accused that may have committed an offence can be identified and prosecuted;
- Allowing the deployment of the right resources to the right location enabling Local Authority resources to be used more effectively;
- Providing evidence with high probative value to assist in the prosecution of an accused;
- CCTV footage will allow the scale and type of the waste to be clearly demonstrated in prosecutions;
- Promoting the usage of emerging technologies in overt monitoring where their use will be more effective in achieving the stated aims without increasing risks to Data Subjects; and
- CCTV will be used as a deterrent to potential offenders in a specific location.

Data Protection by Design and Default

In accordance with the provisions of Section 76 of the Act of 2018 this Code of Practice seeks to ensure that the processing to be undertaken by Local Authorities under this Code must ensure the necessity for the use of CCTV and the identification of risks to the privacy of Data Subjects are considered at the design stage. The application of the Code, the DPIA process, the role of the oversight board and the implementation of the various standardised policies and procedures shall ensure that each Local Authority seeking to use CCTV for deterring environmental pollution and the deterrence, prevention, detection and prosecution of offences under

the Act of 1997 will have undertaken a 'privacy by design and default' process prior to the deployment of CCTV and have implemented the required appropriate technical and organisational measures in order to be compliant with section 76(2) of the Act of 2018.

Data protection by design shall be implemented by adopting technical or organisational measures and safeguards such as storing Personal Data available in a structured, common machine readable format, providing information about the storage of data, having malware detection systems, training Local Authority staff (and/or, where apposite, other Authorised Persons) about basic "cyber hygiene", establishing privacy and information security management systems, and implementing data minimisation practices.

Local Authorities shall take a "state of the art" approach and when determining the appropriate technical and organisational measures to be deployed, shall take account of the current progress in technology that is available in the market. The requirement is for Local Authorities to have knowledge of, and stay up to date on, matters such as: technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of Data Subjects taking into account the evolving technological landscape. Organisational measures are required to ensure the effectiveness of technological measures. Examples of organisational measures include the adoption of internal policies; up to date training on technology, security, and data protection; and IT security governance and management policies.

Only Personal Data which are necessary for the specific purpose of the processing shall be processed by Local Authorities. This means that by default, Local Authorities shall not collect more data than is necessary, they shall not process the data collected more than is necessary for their purposes, nor shall they store the data for longer than necessary. The basic requirement is that data protection will be built into the processing by default. Technological and organisational measures such as those outlined earlier will also be required to ensure appropriate design by default is in place for Approved CCTV Schemes prior to their installation under this Code.

Examples of privacy be design & default

1. Local Authorities shall ensure that the CCTV equipment that is procured and installed is such that its functionality is appropriate and proportionate to the stated objective for which it is being deployed. CCTV cameras with enhanced or additional functionality not required for a site-specific deployment shall have that additional functionality disabled.

2. Business Units seeking to recommend the deployment of CCTV shall demonstrate through their DPIA that the sight and field of vision for their proposed CCTV Scheme will be such that the cameras will be installed in such a way as to ensure that only the specific area required is captured and limited insofar as possible in relation to the impact on Data Subjects' privacy. Masking will be deployed so as to ensure, insofar as is possible, that the front curtilage of private dwellings especially upstairs windows and back gardens are not captured. Other measures such as disabling auto-scan and roaming capabilities of cameras must also be implemented, where applicable.

3. Each Local Authority, subject to cost considerations, shall procure or engage a commercial provider, to ensure that CCTV footage being retained for prosecution purposes will be pixellated so as to ensure, insofar as is possible, that Data Subjects in the background who are not the subject matter of a prosecution or potential prosecution are not identifiable.

4. Each Local Authority shall develop a set of Standard Operating Procedures (SOPs) that will define the operating procedures to be followed by Business Units seeking to recommend the installation of a CCTV Scheme. Section 12 of this Code prescribes the suite of SOPs that must be in place prior to the deployment of a CCTV Scheme for the purposes covered by this Code of Practice.

A CCTV Proposal shall only be considered justifiable and reasonable if an Authorised Person can demonstrate to the Oversight Board that less intrusive reasonable steps have already been taken to deter environmental pollution and facilitate the deterrence, prevention, detection, and prosecution of offences under the Act of 1997, without any positive impact in countering and reducing instances of offending prior to recommending a CCTV Proposal. This may include deploying alternative less intrusive deterrent strategies such as:

a) increasing lighting in an area prone to offences,
b) improved signage,
c) carrying out more frequent inspections, and
d) increased public awareness campaigns.

Restrictions on use of CCTV and certain technical functionality

A CCTV Scheme shall only be installed and operated for the permitted purposes under the Act, namely, to deter environmental pollution and facilitate the deterrence, prevention, detection, and prosecution of offences under the Act of 1997.

Under section 2 of the Act of 1997, CCTV is defined to mean a system of recording devices the signals of which are not made publicly available but are monitored, or capable of being monitored by a Local Authority. The term 'recording device' is also defined in section 2 as a device that is capable of recording or processing, or both, visual images or audio, or both, on any medium, from which a visual image or moving visual images may be produced and includes any accompanying document, and, where only visual images or moving visual images are concerned, includes any sound accompanying those images but does not include automatic number plate recognition devices or facial recognition devices.

Therefore, a CCTV Scheme permitted under Section 23A of the Act of 1997 specifically excludes automated number plate recognition (ANPR) and facial recognition devices.

8. Conducting a Local Data Protection Impact Assessment (Local DPIA) to establish the necessity and proportionality for a CCTV Proposal

Prior to placing a CCTV Proposal before an Oversight Board and recommending the Board seek approval from the Chief Executive for the CCTV Proposal for Law Enforcement Purposes under the section 23A of the Act of 1997, the Business unit seeking to proceed with the CCTV Proposal must undertake a Local DPIA. A standard template DPIA document will be issued to all Local Authorities to be used locally by Business Units when submitting a CCTV Proposal to an Oversight Board. Local DPIAs must be undertaken in advance of a CCTV Proposal being submitted to the Oversight Board and well before any procurement, installation or where existing CCTV installations are involved, adaptations to, of a CCTV Scheme. Local DPIAs can be submitted as either a stand-alone document or as an integral part of a business case. The purpose of a Local DPIA will be to facilitate the identification and implementation of appropriate measures to eliminate or minimise any risks , including cumulative risk, arising out of the processing of Personal Data by other CCTV Schemes and MRD deployments, and comply with the requirements of data protection by design and by default under section 76 of the Act of 2018. According to the DPC, data protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage and data protection by default means that the user settings must be automatically data protection friendly and that only data which is necessary for the specific purpose of the processing is gathered at all. A draft Local DPIA must be submitted to the DPO for review and the final Local DPIA signed off by the relevant Director of Services/Head of Section before being submitted, along with the business case, to the Oversight Board.

9. Necessity for the Use of CCTV

Proving necessity based on the number of complaints received regarding breaches of the Act of 1997 and enforcement actions taken and prosecutions

Business units, or Authorised Persons, seeking to demonstrate the necessity for a CCTV Proposal to counter litter issues in a specific site shall, in their Local DPIA and/or business case, detail the number of complaints received locally in relation to alleged breaches or offences of the Act of 1997 at the specific site. In addition, Business Units can use details of the number of enforcement actions and (if further required) successful prosecutions associated with alleged offences committed at the specific site where the Business Unit seeks authorisation to deploy a CCTV Scheme.

It should be noted that all complaints and allegations must be actively investigated by Local Authorities for breaches under the Act of 1997. Failure to effectively investigate these complaints may result in significant environmental pollution and threaten public health.

Proving necessity based on the number of recorded observations of Authorised Persons

Business Units, or Authorised Persons, seeking to demonstrate the necessity for the use of a CCTV Proposal in:

(a) deterring environmental pollution, and

(b) facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997

in a specific site shall, in their DPIA and/or business case, detail the number of recorded observations made by Authorised Persons in respect of incidents or activities at the proposed site where it is planned to install the CCTV, where the incidents are not the subject of a of formal complaint.

A CCTV Scheme shall only be introduced to address/resolve an identifiable and specific problem with alleged breaches of the Act of 1997. A CCTV Scheme shall only be deployed in order to:

- prevent further alleged breaches of the Act of 1997 in locations where the necessity for the use of a CCTV Scheme has been demonstrated by means of a Local DPIA;
- detect who is responsible for alleged breaches of the provisions of the Act of 1997,
- support the prosecution of those responsible for the alleged breaches of the Act, and;
- where there is evidence of less intrusive measures to deter, prevent, detect, and prosecute offences under the Act of 1997 having already been deployed without success.

A CCTV Scheme shall only be authorised by the Chief Executive of a Local Authority for introduction where it is clearly established that it is necessary to address/resolve an identifiable, specific, and significant problem with serious and/or repeated alleged breaches of the Act of 1997.

10. Local consultation on intended CCTV implementation

As an integral part of the Local DPIA and business case process individual Local Authorities shall engage in the most appropriate level of consultation with the public, that will be impacted by the introduction of a CCTV Scheme in the specific locations detailed in the Local DPIA.

The appropriate level of consultation will be determined by the extent to which the introduction of a CCTV Scheme increases the risks to Data Subjects by its introduction. Each site specific Local DPIA shall define what levels, extent, and methodologies for consulting with the public each Local Authority will have undertaken prior to a CCTV Scheme, which is to be approved and implemented locally, being put in place. It should be noted that consultation with the public can take many forms and will be a matter for each Local Authority to determine, as appropriate.

It is a matter for each Local Authority to determine the appropriate level of public consultation that should occur. There must, however, be effective local consultation and such consultation should take the form of one or other types of consultation as specified in the examples provided below, or similar levels of consultation.

Examples of appropriate levels of consultation with the public are as follows:

- Feedback obtained from elected representatives, on behalf of their constituents, where CCTV is to be deployed;
- On-line public consultation;
- In person public information events; and
- Direct engagement with local community groups and bodies potentially impacted by the deployment of CCTV.

11. Approval process by Oversight Board prior to CCTV Scheme being installed

In order to comply with this Code, each Local Authority is required to establish an Oversight Board. This Oversight Board will assess the necessity and proportionality for a CCTV Proposal submitted to it by Business Units or by Authorised Persons, prior to the Oversight Board recommending the CCTV Proposal to the Chief Executive of the Local Authority for full and final approval.

Membership of a Local Authority Oversight Board must be such that it contains sufficiently senior managers in charge of Business Units in the Local Authority that use CCTV and include the Head of Information System (HIS). In addition, the DPO must be a member of the Oversight Board and must be able to perform his/her independent function regarding whether to recommend or reject any CCTV Proposal before proceeding with a recommendation to the Chief Executive.

Senior managers who are members of the Oversight Board and who make a proposal for CCTV use on behalf of their Business Unit to the Oversight Board shall recuse themselves from the decision on whether to make a recommendation for the proposed use of CCTV to the Chief Executive. The senior manager(s) may attend at such board meetings to present and explain their proposal and its rationale on behalf of their Business Unit and leave the meeting thereafter to enable senior personnel from other Business Units within the Local Authority, who are independent of the proposing Business Unit, to make a decision to recommend the proposed use of CCTV to the Chief Executive or not.

Where the Oversight Board has endorsed the CCTV Proposal, it must then be submitted to the Chief Executive for consideration and final decision by means of formal written approval (if approved) as provided for in Section 23A(7) of the Act of 1997.

12. Standard operating procedures for the use of CCTV

Each Local Authority shall develop a set of Standard Operating Procedures (SOPs) that will define the operating procedures to be followed by Business Units seeking to install and operate a CCTV Scheme under the provisions of Section 23A of the Act of 1997 and this Code of Practice, in the following areas:

- Identification of sites where CCTV is to be introduced to tackle an identified problem.
- Preparation of a Local Data Protection Impact Assessment;
- Preparation of a business case for submission to the Oversight Board;
- Appropriate signage to be installed in the location where CCTV is deployed for Law Enforcement Purposes under Section 23A of the Act of 1997;
- Installation of CCTV on-site i.e., sighting and field of vision for CCTV installed on-site.
- Operation and monitoring of CCTV by Authorised Persons and/or authorised Local Authority staff;
- Security and maintenance of CCTV equipment including cameras and monitors;
- Retention, storage, and destruction of Personal Data captured by CCTV recordings;
- Identifying and providing (where required) the appropriate level of child safeguarding vetting for authorised Local Authority staff viewing CCTV footage:
- Maintaining a record of data processing activities (ROPA) that complies with section 81 of the Act of 2018;
- Chain of custody;
- Appropriate levels of training to be provided to Local Authority staff submitting business cases and/or operating CCTV Schemes for Law Enforcement Purposes under section 23A of the Act of 1997;
- Sharing & transfer of CCTV images and recordings to Authorised Persons and/or Competent Authorities for prosecution purposes;
- Periodic review of adherence to terms under which Approval was given for a CCTV Scheme covered by section23A of the Act of 1997 and the terms of this Code of Practice; and
- Procedure for handling concerns and complaints from individuals and organisations about the use of CCTV for Law Enforcement Purposes under section 23A of the Act of 1997.

The purpose of the SOPs will be to detail the items to be covered for the installation and operation of a CCTV Scheme for the deterrence of environmental pollution and facilitating the deterrence, prevention, detection and/or prosecution of offences under the 1997 Act.

Local Authorities shall have regard to this Code of Practice when drafting local policies; procedures and SOPs governing the installation and operation of a CCTV Scheme.

In addition to the above SOPs a number of standardised guidance documents will be developed to assist individual Local Authorities implement the above SOPs and ensure insofar as is possible a uniform approach to compliance with Data Protection Laws and may include:

- Flowchart detailing process steps to be followed by Business Units seeking to get approval for the use of CCTV from the Oversight Board of a Local Authority;
- Terms of reference and suggested membership for a local Oversight Board;
- Template Local DPIA;
- Template business case document for CCTV Proposals;
- Template data processing agreement;
- Template data sharing agreement;
- Template RoPA;
- Sectoral records retention schedule for CCTV footage.
- Procedures for handling requests from data subjects seeking to exercise their rights under Chapter 4 of Part 5 of the Act of 2018."

13. Identification of sites where CCTV may be introduced

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals have a reasonable expectation of privacy is prohibited. CCTV shall only be utilised in a fair and ethical manner and, where installed for the purposes of this Code of Practice, only for the stated purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997.

CCTV shall only be introduced to address/resolve an identifiable and specific problem with alleged breaches of the Act of 1997. Each Local Authority will therefore only select locations for the installation of CCTV cameras where a Local DPIA has demonstrated that there is necessity for the use of such CCTV. The CCTV installation being considered shall be proportionate to the specific site and the installation of any such CCTV Scheme shall be the least intrusive means possible to protect the privacy of individuals. Cameras shall be positioned in such a way as to prevent or minimise the recording of such places to the greatest extent possible. Privacy masking is to be applied, insofar as is possible, on CCTV cameras, where necessary, in order to block-out areas where individuals may have a reasonable expectation of privacy. In any area where CCTV is in operation, there will be a prominent sign displayed notifying people of same.

14. Preparation of a Data Protection Impact Assessment

Business Units and/or Authorised Persons who are considering proposing the deployment of CCTV in accordance with section 23A of the Act of 1997 and this Code shall prepare a Local DPIA. The Local DPIA shall adhere to the approach detailed at section 9 of this Code and will be in the form detailed in the template Local DPIA which will be provided to the litter enforcement sections of Local Authorities or Authorised Persons.

Review of DPIAs

Local DPIAs shall be reviewed as the Oversight Board considers appropriate, subject to a maximum of 3 years between each review, or when a change in circumstances occurs, which would trigger a review of the DPIA. Changes that might trigger an automatic review of a DPIA would include where an Approved CCTV Scheme is expanded or adjusted in any way by the Local Authority e.g., a different model of CCTV is procured to replace a faulty, damaged, or obsolete device. A review will also automatically be required where there is no change to the Approved CCTV Scheme itself but there is a significant change to the local built environment, which is captured by the Approved CCTV Scheme, e.g., or if a crèche, nursing home or treatment centre is built in an area already monitored by an Approved CCTV Scheme.

Outcomes from reviews

Where the outcome from such a review and accompanying updated DPIA is:

(a) the necessity for the use of the Approved CCTV Scheme no longer exists, or

(b) is such that the Approved CCTV Scheme is no longer operated in accordance with the terms of the original Approval, or this Code,

then the Oversight Board shall recommend to the Chief Executive of the relevant Local Authority that the Approval be revoked by the Chief Executive pursuant to Section 14A(12) of the Act of 1996 or that the Approval be renewed subject to terms and conditions, if any, as he or she considers appropriate.

15. Preparation of a business case for submission to an Oversight Board

A Business Unit within a Local Authority and/or Authorised Persons following completion of their Local DPIA, shall submit a CCTV Proposal within a given Local Authority's geographical area of responsibility to the Oversight Board of that Local Authority for consideration. A business case must be approved by the Director of Service in a Local Authority submitting the CCTV Proposal as project sponsor and include a proposed allocation of funding for installation and annual funding for maintenance, communications, and monitoring costs for the duration of the proposed installation, not being a period of greater than 3 years.

A business case to an Oversight Board shall be accompanied by or include evidence of a formal Local DPIA having been carried out using the approved template Local DPIA.

16. Appropriate signage when using CCTV for Law Enforcement Purposes under section 23A of the Act of 1997

Section 90 of the Act of 2018 sets out the statutory requirements that each Local Authority, as Controller under the LED as transposed into Irish law by Part 5 of the Act of 2018 must meet so as to ensure that Data Subjects are provided with the necessary information in advance of entering an area where an Approved CCTV Scheme's recording will take place.

Each Local Authority shall ensure that adequate CCTV signage is placed at locations where CCTV camera(s) are sited for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997. Signage must be clearly visible and legible to members of the public and includes the name and contact details of the Local Authority as Controllers as well as the specific purpose(s) for which the CCTV camera is in place in each location. The DPO shall be consulted, in advance, on any signage and other transparency materials.

Appropriate locations for signage include:

- at or in close proximity to each camera;
- entrances to premises in which cameras are located e.g., car parks where bottle banks are located;
- any other areas/locations where CCTV has been located for the purposes covered by section 23A of the Act of 1997 and this Code of Practice.

Each Local Authority shall publish its own privacy statement or data protection policy on its website for the information and adherence of staff and for public awareness and information.

17. Installation of CCTV on-site i.e., sighting and field of vision for CCTV installed on-site

The Business Units within the Local Authority shall periodically review, but at least once every 3 years the sight and field of vision for each CCTV Scheme installed to ensure that the specific area required is captured and limited insofar as possible in relation to the impact on Data Subjects' privacy. Care is to be taken to review images to reduce the risk of capturing sensitive Personal Data e.g., Crèches, schools, and parks. Masking is to be considered, insofar as is possible, on the front curtilage of private dwellings, especially on upstairs windows, and back gardens. Other measures such as disabling auto-scan and roaming capabilities of cameras must also be implemented where appropriate, and detailed instructions are to be included in local SOPs. The Local Authority DPO is to be consulted in advance. Any significant changes to an already approved CCTV Scheme shall be brought back to the Oversight Board for its consideration before being submitted to the Chief Executive for renewal of the Approval.

18. Security & Controlling Access to CCTV

Local DPIAs and Business case documentation prepared by each Business Unit seeking CCTV Approval to install and operate a CCTV Scheme must identify the limited number of authorised staff and/or Authorised Persons that will be approved to have access to the CCTV cameras, monitors and recordings and process Personal Data.

Access rights can only be authorised so that identification of which authorised Local Authority staff and/or Authorised Persons has/have accessed to the CCTV Scheme or viewed CCTV images at any given point in time can be produced easily in the form of an access log as part of audit or reporting requirements. Local SOPs will stipulate that the authorised Local Authority staff and/or Authorised Persons allowed access to the monitoring room are prohibited from using personal smartphones or other recording devices in a CCTV monitoring room.

Unique log in/access credentials shall be issued to each authorised staff member and/or Authorised Persons. The sharing of log in credentials is prohibited and will normally lead to disciplinary action under the respective employment policies of Local Authorities.

All authorised Local Authority staff and/or Authorised Persons that are involved in monitoring or viewing or otherwise processing CCTV footage must receive appropriate training in the use of CCTV and compliance with Data Protection Laws generally. Local SOPs will set out clear guidelines regarding such training including, where appropriate, if any of the personnel involved will be subject to child safeguarding vetting.

Supervising access to and maintenance of the Approved CCTV Scheme will be the responsibility of Authorised Persons and/or authorised staff appointed by each Local Authority that is operating the Approved CCTV Scheme. Personal Data captured by CCTV in accordance with this Code shall be stored by Local Authorities in a way that maintains its integrity and security and shall , where possible, include encrypting the Personal Data where it is possible to do so.

Each Local Authority shall ensure where remote access to live recording is permitted, that the data arising is stored on a secure and encrypted software system/platform with access restricted to Authorised Persons and/or authorised Local Authority staff only. The conditions governing encryption, software systems/platforms and authorised Local Authority staff and/or Authorised Persons permitted to have access to such systems shall be dealt with in the Local DPIA.

19. Records to be maintained by Local Authorities

19.1 Appropriate written records shall be created and maintained by Local Authorities to demonstrate their compliance with their obligations under Part 5 of the Act of 2018, to include:

19.1.1 A record of its data processing activities (RoPA) for each category of processing activity for which it is responsible in compliance with the requirements laid down in section 81(1) of the Act of 2018 and make it available to the DPC for inspection and examination upon request;

19.1.2 A data log in compliance with the requirements laid down in section 82 of the Act of 2018, if applicable, in relation to the automated processing systems of a Local Authority such that amongst other things, it can be ascertained when and if Personal Data was consulted by any person or whether Personal Data was disclosed or transferred to another person;

19.1.3 A register of any Personal Data Breaches in compliance with the requirements laid down in section 86(6) of the Act of 2018 and furnish it to the DPC upon request;

19.1.4 Records of any factual or legal basis for the decision made to rely on any restriction of Data Subject Rights that are applied under section 94 of the Act of 2018 and make that record available to the DPC if requested.

20. Chain of custody

20.1 Where CCTV footage is viewed and footage of incidents which may lead to prosecutions is identified by Authorised Persons and/or authorised Local Authority staff then this footage shall be separated, saved and downloaded from the Approved CCTV Scheme camera feed or from the cameras storage device (SD), as soon as practically possible after it is viewed and ear marked for retention, to a secure and restricted access folder on the Local Authorities online storage platform, in line with the chain of custody SOPs to be developed by each Local Authority.

20.2 Each Local Authority shall ensure that the chain of custody SOPs relating to the CCTV footage is adhered to, so as to ensure, insofar as is possible, the admissibility of the CCTV footage in any Court proceedings. The Local Authorities SOPs shall detail the steps to be followed when the following arise,

- Requests to view or access CCTV made on foot of a valid Data Access Request;
- Transfer/sharing of CCTV footage to Authorised Persons and/or Competent Authorities where it is required to do so lawfully as part of the Law Enforcement Purposes under section 23A of the Act of 1997;
- Steps to be followed to redact or obscure background images and/or images of other Data Subjects who are not the subject of the prosecution or potential prosecution, without diminishing the quality of the footage so as to affect its admissibility in any ensuing Court proceedings.

21. Disclosure of CCTV images and recordings

21.1 The principal purposes for the operation of a CCTV Scheme under section 23A of the Act of 1997 and this Code are deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act, however, there may be instances where it is appropriate to share, transfer or disclose information including Personal Data with other enforcement bodies who are Competent Authorities in pursuit of Law Enforcement Purposes. Responsibility for ensuring effective governance arrangements shall be undertaken by the Oversight Board within Local Authorities to facilitate effective joint working with those Competent Authorities. The disclosure of Personal Data obtained from an Approved CCTV Scheme must be lawful and in compliance with the Principles at section 5 above. Disclosure of images or information constituting Personal Data may be appropriate where Data Protection Laws provide exemptions which permit its disclosure, provided that the applicable requirements of the Data Protection Laws are satisfied, or where otherwise permitted by law. A proportionality assessment shall be carried out to ensure the benefits of the proposed sharing of the Personal Data are balanced with the individual Data Subject's privacy rights.

It is a matter for each Local Authority to identify who is the person(s) authorised within the Business Unit to make the decision regarding whether Personal Data may be shared and whether it is that person who will carry out the proportionality assessment therein referenced, or whether that latter assessment will, or may, be carried out by somebody else and the result of that assessment presented to the relevant decision-maker for decision in consultation with the Data Protection Officer.

21.2 Personal Data will only be shared or provided to Authorised Persons and/or Competent Authorities for Law Enforcement Purposes or where it is otherwise required to be shared or transferred in accordance with law including a decision of a supervisory authority such as the DPC or a court judgment and/or order. The terms of the data sharing arrangement shall be governed by an agreement in writing to ensure that all parties involved in the processing do so in accordance with the Data Protection Laws.

21.3 Personal Data may also be provided to AGS in appropriate circumstances. A request in writing must be submitted by AGS to the Local Authority for consideration. AGS will need to include information citing the relevant legislation upon which it is seeking to rely (which must be for Law Enforcement Purposes) and set out the reasons why it submits that the disclosure of the data in question is necessary and proportionate to that purpose in order for the request to be lawful within the meaning of section 71(5) of the Act of 2018.

21.4 As a Competent Authority under the LED, a Local Authority may on occasion share Personal Data captured by an Approved CCTV Scheme with other Competent Authorities for Law Enforcement Purposes, e.g., other Local Authorities (which may include WERLAs and the NTFSO) or the EPA, for the prosecution of offences under the Act of 1997. It may also share with Competent Authorities outside of the State e.g., Local Authorities in Northern Ireland.

21.5 The Litter Enforcement sections of individual Local Authorities may supply copies of CCTV data to their own legal department(s) (which may include third parties such as external legal firms and Counsel) for the purposes of obtaining legal advice or progressing prosecutions. Where a case involving CCTV data is before the courts the law agent representing the Local Authority may be required to supply both the accused, opposing legal representatives of the accused and/or the Courts Service with copies of the CCTV data being relied on in Court.

- 21.6 Personal Data requiring external transfer is to be shared via a secure encrypted ShareFile system. In limited circumstances where broadband may be an issue, encrypted portable media will be used to transfer the CCTV footage. In such instances, the media in question shall be hand delivered to the third party (this may include Authorised Persons, authorised personnel within other Local Authorities, the EPA and AGS) and shall be accompanied by chain of custody documentation to ensure the integrity of the data for evidential purposes. The DPO in each Local Authority shall endorse the transfer of the data and require approval by an authorised representative of the third party prior to the transfer or sharing of any data.
- 21.7 There may be other limited occasions when disclosure of Personal Data to another third party, such as to a person whose property has been damaged, may be appropriate. Such requests should be approached with care and in accordance with Data Protection Laws , and in a manner that is cognisant of the local policy and procedures of the applicable Local Authority.

22. Data Subject Rights

22.1 The processing of Personal Data by operating an Approved CCTV Scheme in accordance with Section 23A of the Act of 1997 and this Code is for the purposes of deterring environmental pollution and facilitating the deterrence, prevention, detection, and prosecution of offences under the Act of 1997. Therefore, a Local Authority acting as a Competent Authority governed by the LED as transposed into Irish law by Part 5 of the Act of 2018 is processing Personal Data under the LED regime and not the GDPR regime. For information on rights and obligations that arise under GDPR, Data Subjects will be referred to the privacy statement and data protection policies of Local Authorities insofar as the processing of any Personal Data occurs that is captured by GDPR, and accordingly, is outside the scope of this Code.

22.2 Data Subjects have the following rights in the LED regime which are laid down in Chapter 4 of Part 5 of the Act of 2018:

(a) Rights in relation to automated decision making (section 89)
(b) Right to information (section 90)
(c) Right of access to Personal Data (section 91)
(d) Right to rectification of inaccurate Personal Data (section 92)
(e) Communication with a Data Subject (section 93)
(f) Indirect exercise of rights and verification by the DPC (section 95).

22.3 In addition, pursuant to section 87 of the Act of 2018, where a Personal Data Breach occurs that is likely to result in a high risk to the rights and freedoms of a Data Subject, a Local Authority shall, without undue delay, notify the Data Subject to whom the breach relates, unless the Local Authority has:

(i) implemented appropriate technological and organisational protection measures that were applied to the Personal Data affected by the Personal Data Breach, in particular where the said measures, including encryption, render the Personal Data unintelligible to any person who is not authorised to access it; or
(ii) taken measures in response to the Personal Data Breach that ensure that the high risk to the rights and freedoms of a Data Subject from the breach is no longer likely to materialise.

22.4 Pursuant to section 94 of the Act of 2018, a Local Authority may restrict, wholly or partly, the exercise of a right of a Data Subject set out above, where it is satisfied that it constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the Data Subject for the purposes of:

a) avoiding obstructing official or legal inquiries, investigations, or procedures;
b) avoiding prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c) protecting public security;
d) protecting national security; or
e) protection the rights and freedoms of other persons.

22.5 A Local Authority acting in its capacity as a Controller shall have clear polices and guidelines in place to deal with Data Subject rights in relation to Personal Data captured by CCTV that comply with Part 5 of the Act of 2018. The policies on Data Subjects rights must be communicated to Data Subjects in a concise, intelligible, and easily accessible form using clear and plain language in a notice or policy published on a Local Authority's website. The Data Subject rights referenced in paragraph 23.2 above are set out in more detail below and are subject to any restrictions in section 94 as outlined above that may arise on a case-by-case basis.

22.6 Rights in relation to automated decision making

A Local Authority shall inform Data Subjects that Local Authorities do not use Personal Data for the purpose of automated decision making or profiling and that Profiling that results in discrimination against an individual on the basis of a special category of Personal Data is prohibited.

22.7 Right to Information

Data Subjects shall be provided with the following information at the time their Personal Data is obtained to comply with section 90 of the Act of 2018 unless the information is already in the possession of the Data Subject:

22.7.1 The identity and contact details of the Local Authority as Controller;
22.7.2 The contact details of the DPO of the Local Authority;
22.7.3 That the Personal Data will be processed for Law Enforcement Purposes under section 23A the Act of 1997;
22.7.4 information detailing the right of the Data Subject to request from the Local Authority access to, and the rectification or erasure of, the Personal Data;
22.7.5 information detailing the right of the Data Subject to lodge a complaint with the DPC and the contact details of the DPC;
22.7.6 in individual cases where further information is necessary to enable the Data Subject to exercise his or her rights under Part 5 of the Act of 2018, having regard to the circumstances in which the Personal Data are or are to be processed, including the manner in which the data are or have been collected, any such information including:
22.7.6.1 the legal basis for the processing of the data concerned, including the legal basis for any transfers of data (if applicable);
22.7.6.2 the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;
22.7.6.3 where applicable, each category of recipients of the data.

22.8 Right to Access Personal Data

Where a Data Subject who believes that Personal Data relating to him or her have been or are being processed by or on behalf of a Local Authority, if he or she so requests the Local Authority by notice in writing, he or she is to be provided with the following information to comply with section 91 of the Act of 2018:

22.8.1 Be informed by the Local Authority whether Personal Data relating to him or her have been or are being processed by or on behalf of the Local Authority;
22.8.2 where such data have been or are being so processed, be provided by the Local Authority with the following information:
22.8.3 A description of –
22.8.3.1 the purpose of, and legal basis for the processing,
22.8.3.2 the categories of Personal Data concerned,
22.8.3.3 the recipients or categories of recipients to whom the Personal Data concerned have been disclosed, and
22.8.3.4 the period for which the Personal Data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period.
22.8.4 A communication of the personal data concerned. This obligation shall be complied with by supplying the Data Subject with a copy of the information concerned in permanent form unless the supply of such a copy is not possible or would involve disproportionate effort or the Data Subject agrees otherwise;
22.8.5 Any available information as to the origin of the Personal Data concerned unless the communication of that information is contrary to the public interest. This obligation shall be complied with by supplying the Data Subject with a copy of the information concerned in permanent form unless the supply of such a copy is not possible or would involve disproportionate effort or

the Data Subject agrees otherwise;

22.8.6 A Local Authority shall respond to a request made by a Data Subject under section 91 of the Act of 2018 and provide the information specified above to the Data Subject not later than one month after the date on which the request is made. This period can be extended by a further two months in certain circumstances more particularly outlined in section 91(5) and 91(6).

22.8.7 Where on foot of a DSAR under section 91 information that would otherwise need to be provided to a Data Subject by a Local Authority includes Personal Data relating to another individual that would reveal, or would be capable of revealing, the identity of the individual, a Local Authority shall not provide the Data Subject with the information that constitutes such Personal Data relating to the other individual.

22.8.8 A Local Authority shall use reasonable endeavours to obscure or pixelate CCTV footage of an individual who is not the Data Subject making a DSAR unless the supply of the footage in question is not possible or would involve a disproportionate effort or the consent of the third party to the release of its Personal Data is obtained. Where appropriate, a summary of the Personal Data concerned may instead be furnished to a Data Subject rather that the information that constitutes such Personal Data relating to another individual so that in so far as is possible the Data Subject may exercise his or her rights under Part 5 of the Act of 2018 without revealing or otherwise making it capable of revealing, the identity of the other individual, unless the individual concerned consents to the provision of the information to the Data Subject making the DSAR.

22.8.9 The obligation to provide access to Personal Data under section 91(1) of the Act of 2018 does not apply to Personal Data relating to the Data Subject that consists of an expression of opinion about the Data Subject by another person given in confidence or on the understanding that it would be treated as confidential. It also does not apply to information about the description of the recipients or categories of recipients to whom the Personal Data concerned have been disclosed insofar as a recipient is a public authority which may receive data in the context of a particular inquiry in accordance with the law of the state.

22.8.10 Where a Local Authority has previously complied with a request pursuant to section 90(1) of the Act of 2018 the Local Authority is not obliged to comply with a subsequent identical or similar request by the same individual unless, in the opinion of the Local Authority, a reasonable interval has elapsed between compliance with the previous request and the making of the current request. In determining a reasonable interval for this purpose, regard shall be had to the nature of the Personal Data, the purpose for which it is processed and the frequency with which it is altered. Where a Local Authority refuses to act upon a request for these reasons it shall as soon as practicable notify the Data Subject in writing.

22.9 Right to Rectification

Data Subjects are to be provided with the following information to comply with section 92 of the Act of 2018:

22.9.1 A Data Subject may request a Local Authority in writing to rectify Personal Data if he/she is of the opinion that a Local Authority is processing Personal Data relating to him or her that are inaccurate. For the purposes of this paragraph Personal Data are inaccurate if they are incorrect or misleading as to any matter of fact or they are incomplete in a material manner. Where a Local Authority is satisfied that the Personal Data to which the request relates are inaccurate, they shall rectify the data as soon as may be and not later than one month after the date on which the request is made.

22.9.2 A Data Subject may request a Local Authority to erase Personal Data if he/she is of the opinion that the Local Authority is processing Personal Data relating to him/her:

(i) in contravention of Data Protection Principles in Part 5 of the Act of 2018 (sections 71(1)-71(6)) or in contravention to the processing of special categories of Personal Data under Part 5 (73(1)), or

(ii) that are required to be erased by the Local Authority in accordance with a legal obligation to which the Local Authority is subject.

Where a Local Authority is satisfied that paragraph (i) or (ii) above applies to the Personal Data it shall erase the data as soon as may be and not later than one month after the date on which the request is made.

22.9.3 A Local Authority shall respond to a request made by a Data Subject under section 92 of the Act of 2018 and provide the information specified above to the Data Subject not later than one month after the date on which the request is made. This period can be extended by a further two months in certain circumstances more particularly outlined in

section 92(7) and 92(8).

22.9.4 Where a Data Subject makes a request to rectify or erase Personal Data and the accuracy of the data is contested by the Data Subject and it is not possible to ascertain whether the data are so inaccurate or the Personal Data are required for the purposes of evidence in proceedings before a court or tribunal or in another form of official inquiry, the Local Authority shall restrict the processing of the data and shall not rectify or erase the data, as the case may be.

22.9.5 Where a Local Authority complies with a request to rectify or erase Personal Data or restricts the processing of the Personal Data for the reasons outlined in paragraph 23.9.4 the Local Authority shall notify in writing the Data Subject concerned, each controller from which the Personal Data concerned were received and each person to whom the Personal Data concerned where disclosed of the rectification, erasure or restrictions concerned, as the case may be. The person to whom the Personal Data was disclosed may in turn have an obligation to rectify, erase or restrict the processing of the data in question in the same manner as the Local Authority, if applicable.

22.9.6 If a Local Authority is not satisfied to rectify or erase Personal Data on foot of a request to do so and paragraph 23.9.4 does not apply, the Local Authority shall as soon as practicable notify the Data Subject in writing pursuant to section 91(11) of the Act of 2018 and such notification must include:

22.9.6.1 the reasons for the Local Authority's decision under that subsection, and

22.9.6.2 information relating to the Data Subject's right to request the DPC to verify the lawfulness of the processing concerned.

22.9.7 Where a Local Authority has restricted the processing of Personal Data pursuant to section 92(11) as set out in paragraph 23.9.6 above and proposes to lift that restriction, the Local Authority shall inform the Data Subject and any controller from which the Personal Data concerned were received and each person to whom the Personal Data concerned were disclosed, if applicable, and the person so notified shall lift any restriction implemented in the same manner and to the same extent.

22.9.8 A Data Subject's right to rectify or erase personal data in accordance with section 92 of the Act of 2018 shall not apply to Personal Data contained in witness statements.

22.10 Communication with Data Subject

Where a Local Authority provides or makes available information to a Data Subject on foot of the aforementioned Data Subject rights, the following provisions apply:

22.10.1 The information shall be provided by appropriate means including electronic means and be provided in so far as is possible in the same format which the request is made.

22.10.2 A Local Authority shall not impose a charge on a Data Subject for information provided to him/her under section 90.

22.10.3 A Local Authority shall not impose a charge on a Data Subject for information provided to him/her under section 91 or 92 unless it is manifestly unfounded or excessive in nature having regard to the number of requests made by the data subject to the controller under those sections. In those circumstances a Local Authority may charge a reasonable fee to the Data Subject in request of the request, having regard to the administrative cost to the Local Authority of complying with the request or fuse to act upon the request.

22.10.4 If a Local Authority refuses to act upon the request, it shall notify the Data Subject in writing. Such a notification shall include the reasons for which the Local Authority is refusing to act upon the request and information relation to the right of the Data Subject under Chapter 3 of Part 6 of the Act of 2018 to lodge a complaint with the DPC and the contact details of the DPC.

22.10.5 Where a Local Authority refuses to act upon a request, it shall be for the Local Authority to demonstrate that the request was manifestly unfounded or excessive in nature.

2.10.6 For the purposes of exercising a right to communication under section 93 of the Act of 2018 as set out above, Data Subject includes an individual who makes a request for access to information under section 91(1), irrespective of whether the Local Authority is processing Personal Data relating to the individual.

22.11 Right to Indirect Exercise of rights and verification by DPC

22.11.1 Where an individual is aware having been notified that the exercise of his/her rights have been restricted by a Local Authority pursuant to section 94 of the Act of 2018 or believes that the exercise of his/her rights have been so restricted and that he or she has not been notified of the said restriction, the individual may make a request in writing to the DPC to verify whether the Local Authority is processing Personal Data relating to him/her and if so, whether the processing is in compliance with Part 5 of the Act of 2018.

22.11.2 Where the DPC receives such a request, it may take such steps as appear to it to be appropriate including the exercise of its powers pursuant to section 132 of the Act of 2018 (information notice to controller/processor). The DPC having taken those steps shall inform the individual making the request that all necessary verifications or reviews have been carried out by the DPC and of his/her right to seek a judicial remedy for infringement of a relevant provision of the Act of 2018. Nothing in section 95 of the Act of 2018 shall require the DPC to disclose to a Data Subject whether or not a Local Authority has processed or is processing Personal Data relating to him/her.

22.12 Miscellaneous Provisions relating to Data Subject Rights

22.12.1 Where applicable, Local Authority local policies shall identify locations covered by CCTV in an effort to ensure insofar as possible transparency in its processing of Personal Data under this Code.

22.12.2 Local Authorities shall not impose a charge on a Data Subject for information provided to him/her under section 90 and nor shall a charge be imposed for information provided under sections 91 or 92 unless the request is considered to be manifestly unfounded or excessive in nature. In those circumstances, a Local Authority may charge a reasonable fee or refuse to act upon the request.

22.12.3 Data Subjects who believe their Personal Data are inaccurate or require deletion will need to provide such information as a Local Authority may reasonably require to ensure it can identify the Data Subject making the request under Chapter 4 of Part 5 of the Act of 2018, and to allow the Local Authority to locate any relevant Personal Data or information, such as relevant dates and timeframes, if a request is for a copy of video footage captured by CCTV, or to otherwise enable the Local Authority to process the request as permitted in Data Protection Laws. To enable the Local Authority to satisfy itself as to the identity of the Data Subject or to satisfy itself as to whether the Personal Data concerned are inaccurate or should be erased, the Local Authority may request such additional information from the Data Subject as may be necessary to confirm his or her identity or to so locate or satisfy itself, as the case may be, that the Personal Data concerned are inaccurate or should be erased, and the period of time from the making of such a request for additional information, until the request is complied with, shall not be reckonable as part of the timeframe set out in Section 91(2) and 91(4) of the Act of 2018, as the case may be.

22.12.4 Local Authority staff responsible for handling DSARs shall have clear guidance on the circumstances in which disclosure is appropriate and the timelines within which they are obliged to handle DSARs and respond to requests under section 92 of the Act of 2018. Arrangements shall be in place to restrict disclosure of Personal Data where such disclosure would not be consistent with the purpose for deploying CCTV under the Act of 1997 or otherwise where restrictions on the above-mentioned Data Subject rights are supported by the grounds outlined in section 94.

22.12.5 The method of disclosing Personal Data in response to a DSAR shall be secure to ensure it is only seen by the intended recipient.

22.12.6 Local Authorities must inform Data Subjects that the transfer of Personal Data is not permitted to a third country i.e., non-EU country or international organisation, unless it complies with Chapter V of the LED as transposed into Irish law by sections 96-100 of the Act of 2018 (Transfers of Personal Data to third countries or international organisations) and Data Protection Laws, where applicable.

23. Monitoring compliance with this Code of Practice

The Oversight Board in each Local Authority shall be responsible for monitoring compliance by each Local Authority with the requirements of section 23A of the Act of 1997 and this Code to ensure that Approved CCTV Schemes are compliant on an ongoing and regular basis and ensure that the deployment of a CCTV Scheme should not be a permanent arrangement once put in place, but rather must be subject to ongoing review to continue to verify if its retention is justified and a necessary and proportionate measure. Reviews of Local DPIAs underpinning Approved CCTV Schemes must take place at a minimum of every 3 years, but more often if circumstances require. An Approval given by the Chief Executive of a Local Authority for a CCTV Scheme under section 23A of the Act of 1997 shall expire not later than 5 years from the date on which the Approval was given and the Chief Executive shall cause a review of the operation of an Approved CCTV Scheme to be carried out by an Authorised Person not later than 5 years from the date on which it was given by the Chief Executive.

LGMA
Local Government Management Agency

Cumann Lucht Bainistíochta Contae agus Cathrach
County and City Management Association

Rialtas Áitiúil Éireann
Local Government Ireland