Code of Practice for the use of Mobile Recording Devices

for the Purposes of Prevention, Detection and Prosecution of Waste 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 Waste Management Act 1996 as amended by the Circular Economy and Miscellaneous Provisions Act 2002 (the Act of 1996). 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

1.0 Executive Summary

The Waste Management Act, 1996 as amended by the Circular Economy and Miscellaneous Provisions Act, 2022 (**"the Act of 1996"**) identifies the role and functions of Local Authorities in protecting the environment and human health by preventing or reducing the adverse impacts of the generation and management of waste.

Section 14B of the Act of 1996 authorises Local Authorities to operate a mobile recording device for the purposes of preventing, investigating, detecting, or prosecuting offences under the Act of 1996. Pursuant to Section 14C 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 14B. Section 14C(2) outlines the provisions to be included in the draft code for the use of mobile recording devices under section 14B which are as follows:

(a) the procedures and standards to be followed in the operation of mobile recording devices as provided for in section 14B;
(b) confidentiality, security, storage, access to, retention, deletion, and any other processing of, data gathered in accordance with the operation of mobile recording devices as provided for in section 14B;
(c) the circumstances in which data gathered by the operation of mobile recording devices as provided for in section 14B is to be disposed of or destroyed;
(d) the rights of data subjects in so far as they relate to the operation of mobile recording devices as provided for in section 14B;
(e) such other matters, if any, related to the operation of mobile recording devices as provided for in section 14B that the Local Government Management Agency considers appropriate.

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, the LGMA prepared a high-level 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 mobile recording devices by Local Authorities pursuant to Section 14B of the Act of 1996. 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 14B(3) of the Act of 1996 a mobile recording device shall be operated by an authorised person in accordance with the code approved under section 14C.

The Minister has approved this Code pursuant to Section 14C of the Act of 1996. Consequently, any proposal for use of a mobile recording device approved by a Chief Executive of a Local Authority will be lawful provided it complies with this 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.

In particular, the Code sets out the procedures to be followed by various personnel involved in considering a proposal for the use of mobile recording devices (**"MRDs"**) 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 MRDs. 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 MRDs. These procedures, and the multi-layered nature of the decision making involved prior to the adoption of any decision to deploy MRDs and most particularly exceptional decisions to deploy the covert use of MRDs, are designed to ensure the use of MRDs 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 arising from surveillance operations and/or activities involving MRDs under this Code.

2.0 Definitions & Abbreviations

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

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

'AGS' means An Garda Síochána;

'Authorised Person' means a person who is appointed in writing to be an Authorised Person for the purposes of the Act of 1996, or any part or section thereof as more particularly defined in section 5 of the Act of 1996 by

(a) the Minister;

(b) a Local Authority

(c) the Agency;

(d) the Commissioner of the Garda Síochána (or a member of the Garda Síochána nominated by that Commissioner for the purposes of appointing Authorised Persons under this Act, or

(e) such other person as may be prescribed.

'Automatic Number Plate Recognition Device' means a device which engages an automated method of recognising vehicle registration places from a camera image as defined in section 5 of the Act of 1996;

'Body-worn recording device' means a recording device affixed to or contained in the clothing, uniform, or headgear of an Authorised Person as defined in section 5 of the Act of 1996;

'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' means closed circuit television comprising 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 5 of the Act of 1996;

'Code of Practice' or **'Code'** means this code of practice which has been approved by the Minister in accordance with section 14C of the Act of 1996 for the purposes of operating a MRD in accordance with section 14B of the Act of 1996;

'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;

'Covert MRD' means the operation of a MRD covertly by an Authorised Person by using a hidden or concealed MRD, without notifying a Data Subject that the MRD is in operation;

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

'Data Protection Laws' mean 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 Subject' means an individual to whom Personal Data relate as defined in section 69 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;

'DPC' means the 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;

'ECHR' means the European Convention on Human Rights;

'Environmental Pollution' has the meaning given by section 5 of the Act of 1996;

'EPA' or **'the Agency'** means the Environmental Protection Agency;

'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 5 of the Act of 1996;

'GDPR' means the General Data Protection Regulation (EU) Regulation 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;

'IAA' means Irish Aviation Authority;

'Law Enforcement Purposes' means the 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)(a) of the Act of 2018;

'Law Enforcement Purposes under Action 14B of the Act of 1996' means the processing of personal data for the purposes of preventing, investigating, detecting, or prosecuting offences under the Act of 1996 or ensuring the personal safety or security of an Authorised Person in so doing;

'Law Enforcement Directive' or **"LED"** means the Law Enforcement 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 a Competent Authority 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. The LED governs the processing of personal data by a data

controller who is a Competent Authority within the meaning of the LED for Law Enforcement Purposes only;

'LGMA' means the Local Government Management Agency;

'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 the proposed use of MRDs is submitted by the business unit within the Local Authority to the Oversight Board for assessment in accordance with this Code;

'Local 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 MRDs in accordance with this Section 14B of the Act of 1996 and this Code;

'Mobile Recording Device" or **"MRD'** means a recording device, other than CCTV, and includes a body-worn recording device as defined in section 5 of the Act of 1996. Examples of a MRD may include a dashcam, smartphone, drone amongst other similar devices, for the purpose of this Code of Practice and may change from time to time depending on advancements in technology.

- **"NTFSO"** means the National Transfrontier Shipment Office;

'Occupier' includes, in relation to any premises, the owner, a lessee, any person entitled to occupy the premises and any other person having, for the time being, control of the premises as defined in section 5 of the Act of 1996;

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

'Overt MRD' means the use of MRD to obtain data and images with the knowledge of the individual that they are being recorded;

'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;

'Premises' has the meaning given to it by section 5 of the Act of 1996;

'Processing' of or in relation to personal data, means 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;

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

'PSA' means Private Security Authority and is the statutory body with responsibility for licensing and regulating the private security industry in Ireland.

'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 5 of the Act of 1996;

'ROPA' means Record of Data Processing Activity and has the meaning given to it by section 81 of the Act of 2018;

'WERLAs' means the Waste Enforcement Regional Lead Authorities.

3.0 Overview

3.1 The task of enforcing the Act of 1996 and preventing or reducing the adverse impacts of the generation and management of waste can be challenging for Local Authorities. The emergence of MRD technologies in recent years provides an opportunity to greatly enhance the compliance assessment capabilities of Local Authorities in discharging their functions under the Act of 1996. The use of MRDs can improve the quality of evidence and reduce response times to complaints in relation to alleged offences being committed under the Act of 1996. Furthermore, the operation of MRDs has the potential to mitigate risks to the personal safety and security of Local Authority staff and /or Authorised Persons working in this remit.

3.2 The starting point for a Local Authority in achieving the most appropriate balance between the protection of human health and the environment and individual human rights is to adopt a set of guiding principles that are applicable to the proposed use of MRDs in compliance with Section 14B of the Act of 1996. It is envisaged that by adhering to the guiding principles Local Authorities will be able to establish that the proposed use of MRDs is necessary and proportionate to the purpose for which it will be operated and in accordance with recommended procedures and standards, to ensure compliance with the Act of 1996 and this Code.

3.3 To achieve this, the Code sets out guiding data protection principles at sections 9 - 20 that shall apply to the use of all MRDs under Section 14B of the Act 1996 and this Code. These guiding principles draw together good practice and existing legal obligations to create a regulatory framework which can be understood by Authorised Persons and the public alike.

3.4 The guiding principles can be applied to numerous variations in circumstances, including changes in technology and will enable a Local Authority to reach informed and appropriate decisions when considering either the development or use of MRDs or the processing of information or Personal Data obtained as a result of operating MRDs.

4.0 Purpose of the code

4.1 This Code governs the operation of MRDs for the purposes of preventing, detecting, investigating, or prosecuting offences under the Act of 1996 or ensuring the personal safety or security of an Authorised Person in so doing. The LED and GDPR operate in parallel with each other. The LED was introduced to harmonise laws across the EU in relation to data processing in law enforcement. Whilst GDPR generally applies to data controllers who process personal data for several purposes. The LED specifically applies to processing of personal data by a data controller who is a **'Competent Authority'** within the meaning of the LED for **'Law Enforcement Purposes'** only. The LED is an EU Directive as opposed to a Regulation, so it does not have direct effect in Ireland and, instead, requires Irish legislation to transpose it into Irish law. Part 5 of the Act of 2018 transposes the LED into Irish law, in particular sections 69-104 of Act of 2018.

4.2 This Code is confined to the processing of data to include Personal Data by Local Authorities as Competent Authorities for Law Enforcement Purposes within the meaning of the LED and as such the processing of Personal Data in accordance with this Code falls outside the scope of GDPR. For further information in relation to the processing of Personal Data by a Local Authority in its capacity as a Controllers that falls within the scope of GDPR (and thus outside of this Code), please see each Local Authority's Data Protection Policy and/or Privacy Statement.

4.3 Modern and ever-advancing MRDs provide increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images, information, and data. The overarching purpose of this Code will enable Authorised Persons to make legitimate and justifiable use of available MRD technology in a way that the public will reasonably and foreseeably expect and to a standard that maintains public trust and confidence.

4.4 When used appropriately, MRDs are valuable tools in preventing environmental pollution, protecting human health and the environment.

4.5 The local government sector is fully supportive of the use of MRDs to prevent, detect, investigate, or prosecute offences under the Act of 1996 whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need; proportionate; effective, and compliant with any relevant legal obligations. It is the way in which technology is used that is potentially intrusive rather than the technology itself and, therefore,

a decision to use MRDs must be articulated clearly, documented as to the stated purpose for any deployment and be transparent, with the community being informed as to the nature of the recording activity being conducted and the justification for it taking place (with the exception of the deployment of Covert MRD in very limited circumstances as detailed in section 19 of this Code). The technical design solution for such a deployment shall be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation.

4.6 Decisions as to the most appropriate technology shall always consider the potential to meet the stated purpose without unnecessary interference with human rights; and any deployment should not continue for longer than necessary.

4.7 This Code, which has been approved by the Minister pursuant to Section 14C of the Act of 1996, identifies clear procedures, standards, and guidelines in best practice for Authorised Persons without being overly prescriptive on operational and technical measures required. This ensures that it does not stifle innovation or fail to retain relevance in an arena where technology and professional practice is expected to continue evolving.

4.8 A set of Standard Operating Procedures (SOPs) will be developed that will define the operating procedures which must be followed by the Business Units within Local Authorities seeking to propose the introduction and implementation of a MRD under the provisions of Section 14B of the Act of 1996 and this Code.

5.0 Scope of activity to which this code applies

5.1 The Code applies to the use of MRDs by Authorised Persons for the purposes of preventing, detecting, investigating, or prosecuting offences under the Act of 1996 or the purposes of ensuring the personal safety or security of those Authorised Persons in so doing.

5.2 The use of Covert MRDs by Authorised Persons shall only be considered in exceptional circumstances and those circumstances are set out in more detail at Section 19 below of this Code, but all considerations, factors and procedures that apply in relation to authorising the overt use of MRDs will also apply, insofar as is practicable, to any proposed decision in relation to authorising the covert use of MRDs.

6.0 Effect of the code

By virtue of Section 14B(3) of the Act of 1996, a MRD must be operated by an Authorised Person in accordance with this Code as provided for in section 14C of the Act. For the sake of transparency, Local Authorities must be able to demonstrate how they have had regard to this Code in their local policies and SOPs. This Code is legally binding on Local Authorities and any limited situations in which adherence with this Code may not be possible when considering whether to approve the use of MRDs must be clearly detailed in Local DPIAs adopted in advance of a decision to authorise the deployment of MRDs by a Chief Executive of the relevant Local Authority and prior consultation with the DPC in such circumstances will be mandatory in advance of the authorisation to deploy such MRDs.

6.1 The duty to have regard to this Code also applies when a Local Authority uses a third party to discharge relevant functions covered by this Code and where it enters partnership arrangements. Contractual provisions i.e., data processing agreements that comply with the requirements of section 80 of the Act of 2018 agreed after this Code comes into effect with such third-party service providers or partners must ensure that contractors are obliged by the terms of the contract to have regard to the Code when exercising functions to which the Code relates.

6.2 Section 15 of the Act of 1996 provides for Local Authorities (which in this instance includes authorised staff in specialist divisions set up within certain Local Authorities e.g., WERLAs and NTFSO), to undertake monitoring and inspections for the performance of its functions under the Act of 1996. Section 15(1)(a) states: "Each Local Authority and the Agency shall carry out, or cause to be carried out, such monitoring of the nature, extent and effects of emissions to the environment arising from the holding, recovery or disposal of waste as it considers to be necessary for the performance of its functions under this Act."

6.3 Section 59(1) of the Act of 1996 defines Local Authority functions regarding waste and the enforcement of the provisions within the Act. It states: "Each Local Authority shall, save in a particular case where a provision of this Act provides to the contrary, be responsible for the supervision of, and the enforcement of the relevant provisions of this Act in relation to, the holding, recovery, and disposal of waste within its functional area." Where there is any conflict between this Code and the legislation relevant to other enforcement functions of Local Authorities (including any secondary legislation made or statutory guidance issued) that legislation and/or statutory guidance shall apply.

6.4 Section 71 of the Act of 2018 identifies the general principles of data protection that underpin the processing of Personal Data by a Competent Authority in Ireland for Law Enforcement Purposes within the meaning of the LED, which has been transposed into Irish law by Part 5 of the Act of 2018.

6.5 Section 14 of the Act of 1996 defines the powers of an Authorised Person, and the relevant sub-sections include:

6.5.1 Section 14(1)(a) allows an Authorised Person "…for any purpose connected with this Act - at all reasonable times, or at any time if he or she has reasonable grounds for believing that there may be a risk of environmental pollution arising from the carrying on of an activity at the premises or that such pollution is occurring, enter any premises and bring thereon such other persons (including members of the Garda Síochána) or equipment as he or she may consider necessary for the purpose,"

6.5.2 Section 14(4) states that "Whenever an authorised person enters any premises or boards any vehicle, pursuant to this section, the authorised person may therein, as appropriate –

(a) make such plans, take such photographs, record such information on data loggers, make such tape, electrical, video, or other recordings and carry out such inspections,
(b) make such tests, make such copies of documents and records (including records in electronic form) found therein and take such samples),
(c) carry out such surveys, take such levels, make such excavations, and carry out such examinations of depth and nature of subsoil,…"

6.6 A failure to observe any provision of section 14, 14B and 14C of the Act of 1996 or a failure on the part of any Local Authority or Authorised Person to observe any provision of this Code does not (without prejudice to the power of the court to exclude evidence) of itself affect the admissibility of evidence thereby obtained.

7.0 Consultation on the Code

7.1 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 14C(4) of the Act of 1996 requires that there shall be consultation with various bodies. Section 14C(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 for Justice, and
  (iv) the Data Protection Commission

(b) shall provide the assessment [a DPIA] 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 14A or 14B and such other person that the Minister may direct."

7.2 As part of this consultation process a high level DPIA on the proposed use of MRDs by Authorised Persons was prepared and submitted to the DPC by the LGMA. This DPIA was based on the anticipated use of MRDs in all 31 Local Authorities for the purposes of preventing, investigating, detecting, and prosecuting offences under the Act of 1996. Individual Local Authorities are required to undertake their own Local DPIA before proposing the use of MRDs for Law Enforcement Purposes to the Oversight Board within each Local Authority for recommendation to the Chief Executive and should engage in appropriate public consultation as part of the Local DPIA process.

7.3 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 MRD is proposed 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 proposed deployment of MRD.

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 a Local DPIA. Changes that might trigger an automatic review of a DPIA would include where an approved use of a MRD is expanded or adjusted in any way by the Local Authority e.g., a different model of MRD is procured to replace a faulty, damaged, or obsolete device.

Outcomes from reviews

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

(a) that the necessity for the use of MRDs no longer exists; or
(b) Is such that the approved deployment of MRDs is no longer operated in accordance with the terms of the original approval, or this Code,

then the Oversight Board should recommend to the Chief Executive of the relevant Local Authority that the existing approved use of MRDs be revoked by the Chief Executive pursuant to this Code or that that it be renewed subject to terms and conditions, if any, as he or she considers appropriate .

8.0 Oversight Board

8.1 In order to comply with this Code, each Local Authority is required to establish an Oversight Board. This Oversight Board which will assess the necessity and proportionality for the proposed use of MRDs by Business Units within a Local Authority or by Authorised Persons prior to the Oversight Board recommending the proposed use of MRD(s) to the Chief Executive of the Local Authority for full and final approval.

8.2 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 MRD 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 MRD proposal before proceeding with a recommendation to the Chief Executive.

8.3 Senior managers who are members of the Oversight Board and who make a proposal for use of a MRD 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 a MRD 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 decide whether or not to make a decision to recommend the proposed use of a MRD to the Chief Executive.

8.4 Where the Oversight Board has endorsed the proposed use of a MRD, it shall then be submitted to the Chief Executive for consideration, and final decision by means of formal written approval

8.5 Responsible and legitimate use of MRDs is dependent upon transparency and accountability on the part of an Authorised Person. The provision of information to the public is the first step in transparency and is also a key mechanism of accountability. In the development or review of the operation of MRDs under Section 14B of the Act of 1996 appropriate consultation and engagement with the public by Business Units within a Local Authority will be an important part of assessing whether there is a legitimate aim and a pressing need for the operation of MRDs, and whether the system itself is a proportionate response by Local Authorities to alleged offences under the Act of 1996. Such consultation and engagement will also provide an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.

8.6 Local DPIAs shall be the subject of regular review as more particularly outlined at section 7.3 above, as part of that review process the Oversight Board shall assess whether such devices remain justified in meeting the stated purpose(s) and consider the success of the historical use to determine the justification for the continued use of MRDs. This will enable Local Authorities to adopt new and emerging technologies which could be more appropriate or represent a more proportionate measure to be deployed by Local Authorities.

The data protection principles that apply under the LED as transposed into Irish law by Part 5 of the Act of 2018 are broadly similar to the data

9.0 Guiding Data Protection Principles

protection principles that apply under GDPR. However, the transparency requirements under the LED are not as strict as GDPR due to the potential to prejudice an ongoing investigation in certain circumstances. Local Authorities shall adopt the following guiding data protection principles as detailed in section 71 of the Act of 2018 when processing personal data in the operation of MRDs for the purposes of preventing, investigating, detecting, or prosecuting offences under the Act of 1996:

9.1 The Personal Data shall be processed lawfully and fairly;

9.2 The Personal 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 unless otherwise permissible under law (see 11.3 and 11.7 below);

9.3 The Personal Data shall be adequate, relevant, and not excessive in relation to the purposes for which they are processed;

9.4 The Personal Data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;

9.5 The Personal 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;

9.6 The Personal Data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against
1. unauthorised or unlawful processing, and
2. accidental loss, destruction, or damage.

9.7 A Local Authority shall ensure that an appropriate time limit is established for the erasure of the data or the carrying out of periodic reviews of the need for the retention of the data. A Local Authority shall ensure, by means of procedural measures, that the time limit set down for erasure of the data is observed.

9.8 The Oversight Board established within each Local Authority shall ensure that the Local Authority is able to demonstrate that the processing of Personal Data for which it is responsible is in compliance with the principles outlined in paragraphs 9.1 – 9.7 above. This shall include regular audit-type reviews of a previous decision of a Chief Executive to approve the proposed deployment of MRDs to ensure it remains justifiable i.e., necessary, and proportionate, and in compliance with the above-mentioned principles and this Code.

10.0 Principle 1 – Personal data shall be processed lawfully and fairly

10.1 Article 8 of the LED states that Member States shall provide for processing 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) [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.

10.2 Section 71(2)(a) of the Act of 2018 states that processing of Personal Data shall be lawful where, and to the extent that –
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 Local Authorities in their capacity as Competent Authorities will rely solely on the grounds provided for in section 71(2)(a) i.e., Law Enforcement Purposes to process Personal Data under this Code.

10.3 Section 14B of the Act of 1996 provides that an Authorised Person acting in the course of his or her duties under the Act of 1996 may, in accordance with that section and with this Code, operate a MRD for the purposes of:

(a) preventing, investigating, detecting, or prosecuting offences under the Act of 1996, or
(b) ensuring the personal safety or security of an Authorised Person in preventing, investigating, detecting, or prosecuting offences under the Act of 1996.

10.4 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 14B of the Act of 1996 and section 71(2)(a) of the Act of 2018 as a lawful basis for processing Personal Data captured by the operation of MRDs for Law Enforcement Purposes on the basis that the processing is necessary to carry out their functions under the Act of 1996.

10.5 In order for any processing of Personal Data carried out by a Local Authority for Law Enforcement Purposes to be lawful, it must be necessary. This means that the processing must be a targeted and proportionate way of achieving the purpose. This targeted and proportionate approach must be fully justified in the Local DPIA.

10.6 Local Authorities shall be transparent in relation to how Personal Data is processed where practicable, unless it involves the use of Covert MRD in exceptional circumstances, which is dealt with later in this Code at section 19, or where it would otherwise interfere with the prevention, investigation, detection or prosecuting of offences under the Act of 1996.

10.7 In order to ensure that the processing of Personal Data is fair, each Local Authority must adhere to the standards and procedures laid down in this Code and the data protection principles laid down in the LED as transposed into Irish Law by section 71 of the Act of 2018 and set out above.

10.8 Insofar as is possible, prior to activating the recording on an MRD, an Authorised Person shall endeavour to seek to identify the Occupier of the Premises. If applicable, an Authorised Person will notify the Occupier that they believe there is a potential risk of environmental pollution arising at the Premises and any data collected may be used in enforcement proceedings. An Authorised Person will also caution the Occupier and advise them of their rights in appropriate circumstances. Where an Authorised Person experiences a threat to his/her personal safety and security either verbally and/or physically, the Authorised Person may, where appropriate to do so, inform the Occupier of the perceived threat and activate the MRD to capture data which may be used in future enforcement proceedings. This section does not apply to the operation of Covert MRD.

10.9 This Code governs the processing of Personal Data by Local Authorities as Competent Authorities under the LED as transposed into Irish Law by Part 5 of the Act of 2018. Therefore, it is limited to processing Personal Data for Law Enforcement Purposes. Whenever a Local Authority processes Personal Data which is not for Law Enforcement Purposes, then that processing of Personal Data will be outside of the scope of this Code and within the scope of GDPR. Each Local Authority's Privacy Notice or Data Protection Policy will govern their processing of Personal Data where it falls outside of the purposes envisaged in this Code, which is Law Enforcement Purposes only.

10.10 The objectives envisaged by the use of MRDs include:

- Enhanced waste premises inspections;
- Enhanced levels of compliance;
- Prevention, detection, and investigation of environmental offences;
- Enforcement of environmental law;
- Protection of human health and the environment;
- Protection of property;
- Public safety; and
- Personnel safety and security.

10.11 The application of MRD technology will:

- Assist with the routine inspections of waste premises;
- Assist with non-routine inspections of unauthorised waste premises;
- Provide situational understanding to Local Authorities regarding waste premises;
- Assist with the assessment of emerging environmental pollution/threats;
- Assist with investigations into environmental complaints; and
- Assist with employee and employer health and safety obligations.

10.12 MRDs assist Local Authority staff and/or Authorised Persons to deliver a more effective waste enforcement service by: -

- Providing better situational analysis/understanding prior to entry onto waste premises;
- Providing a visual record of onsite inspection and/or engagement with members of the public;
- Allowing for better enforcement of waste premises permits, to prevent stockpiling or exceedance of threshold limits on waste sites. This will help protect the environment and natural habitats;
- Enabling the scale and type of the waste activity to be readily assessed ensuring a co-ordinated response;
- Enabling the best use of resources, resolving incidents more quickly thereby providing efficiencies;
- Targeting of enforcement action;
- Allowing the deployment of the right resources to the right location enabling Local Authority resources to be used more effectively;
- Enhancing the health & safety of Local Authority staff and/or Authorised Persons by deploying MRD into situations which would otherwise involve risk to individuals;
- Ensuring compliance with the Safety, Health, and Welfare at Work Act 2005 (as amended);
- Providing good quality evidence to assist apprehension and prosecution of alleged offenders; and
- MRD data allows the scale and type of waste to be clearly demonstrated in prosecutions.

11.0 Principle 2 – The purpose of the collection of personal data

11.1 Local Authorities shall process Personal Data only for the purposes for which it is collected in accordance with this Code, which is for the prevention, investigation, detection, and prosecution of offences under the Act of 1996 or for ensuring the personal safety or security of Authorised Persons in so doing or otherwise permitted under law (see section 11.3 and 11.7).

11.2 A decision to operate MRDs and collect Personal Data must always have a clearly defined explicit and legitimate purpose that is compatible with section 14B of the Act of 1996. It should be in pursuit of a legitimate objective of the Local Authority and be necessary and proportionate in attempting to achieve that objective. Preventing, detecting, investigating, or prosecuting offences under the Act of 1996 is a legitimate aim pursued by Local Authorities. Ensuring the personal safety of an Authorised Person acting in pursuit of that aim is, similarly, a legitimate aim

11.3 Pursuant to section 71(5) of the Act of 2018, where a Local Authority collected Personal data for Law Enforcement Purposes, the Local Authority or another Controller may process the data for a purpose so specified other than the purpose for which the data were collected insofar as:

(a) the controller is authorised to process such Personal Data for such a purpose in accordance with the law of the European Union or the law of the State, and
(b) the processing is necessary and proportionate to the purpose for which the data are being processed.

11.4 It is envisaged that Personal Data captured by MRDs for Law Enforcement Purposes within the meaning of Section 14B of the Act of 1996 may be shared with Local Authorities for Law Enforcement Purposes as laid down in the Act of 1996 and other legislation e.g. if MRDs capture Personal Data which relates to offences committed under the Litter Pollution Act 1997 (as amended) it may be further processed for Law Enforcement Purposes pursuant to that legislation despite the fact that it was initially collected for Law Enforcement Purposes in accordance with this Code pursuant to Section 14B of the Act of 1996..

11.5 It is also envisaged that Personal Data captured by MRDs for Law Enforcement Purposes within the meaning of Section 14B of the Act of 1996 may be further processed by Local Authorities by sharing that Personal Data with other Competent Authorities for Law Enforcement Purposes. For instance, Local Authorities may share Personal Data with AGS provided AGS intend to process the Personal Data for Law Enforcement Purposes and the processing is necessary and proportionate to that purpose.

11.6 If the request to share Personal Data is submitted by another Competent Authority to a Local Authority for purposes other than Law Enforcement Purposes, then a lawful basis needs to be established by that Competent Authority which complies with GDPR and Data Protection Laws generally and all rights and obligations arising thereunder will apply to that request as it will, therefore, be outside the remit of this Code and instead fall within the scope of GDPR.

11.7 Section 71(6) of the Act of 2018 permits a Local Authority as Controller to process Personal Data whether the data were collected by the Local Authority or another Controller for:

(a) Archiving purposes in the public interest;
(b) Scientific or Historical research purposes, or
(c) Statistical purposes,

Provided that the said processing –
(i) is for a purpose specified in section 70(1)(a) [Law Enforcement Purposes], and
(ii) is subject to appropriate safeguards for the rights and freedoms of data subjects.

11.8 It is envisaged that whenever a Local Authority may process Personal Data for statistical purposes it will detail these purposes in its local policies and apply data minimisation principles to that processing, such that Data Subjects will not be identifiable insofar as possible and appropriate safeguards on publication of information for statistical purposes will be applied.

12.0 Principle 3 – Personal data shall be adequate, relevant, and not excessive

12.1 Personal Data captured by MRDs shall be adequate, relevant, and restricted to what is necessary for the purposes for which it is processed in order to achieve the stated objective. This requires, in particular, ensuring that the period for which the Personal Data is stored is limited to a strict minimum – see Section 16 below for more information on retention periods.

12.2 The operation of MRDs shall be limited to processing data in relation to waste premises and Occupiers of waste premises within the meaning of the Act of 1996. It shall not involve the regular monitoring of a publicly accessible area on a large scale. However, the data captured by MRDs has the potential to also include Personal Data of Data Subjects on waste premises as well as passers-by (Data Subjects). Appropriate measures to mitigate against those risks to Data Subjects rights and freedoms must be outlined in the Local DPIA.

12.3 MRDs shall only be deployed for specific operational tasks and not used for general patrol or surveillance. The minimum amount of data required for the purposes outlined in Section 14B of the Act will be captured. Proportionality is an important consideration in the use of MRDs for Law Enforcement Purposes. Authorised Persons must only activate the recording on the MRD when needed and deactivate it when it is not needed, to avoid collecting excessive amounts of Personal Data. This shall be clearly detailed in the Local DPIA.

12.4 A Local DPIA shall be undertaken whenever the development or review of a MRD is being considered by a Local Authority to ensure that the purpose of the system is and remains justifiable and that privacy is assessed, and appropriate safeguards are put in place to mitigate against risks and protect Data Subject rights, insofar as possible.

12.5 Local DPIAs will 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 authorised MRDs deployed in the area and CCTV schemes operating in the area, and comply with the requirements of data protection by design and by default under section 76 of the Act of 2018. The Local DPIA must include both a high level or overall DPIA on MRD use generally and a dynamic DPIA for each specific intervention must be conducted because the processing is likely subject to ongoing changes and a continuous process rather than a once off exercise. Where such an assessment follows a formal and documented process in the form of a Local DPIA, such processes help to ensure that sound decisions are reached on implementation both in terms of appropriate communication and necessary measures to safeguard against disproportionate interference with privacy and ensuring the use of MRDs is relevant and not considered excessive.

12.6 A DPIA helps to identify and mitigate against any data protection related risks arising from the proposed use of MRDs and helps ensure compliance with obligations on a Local Authority as a Controller of Personal Data under the LED which is transposed into Irish law by Part 5 of the Act of 2018. The Local Authority, through the Local DPIA, can demonstrate that both the necessity and extent of any interference with a Data Subject rights has been properly considered.

12.7 Technologies associated with MRDs are varied and include unmanned aircraft systems (UAS) or drones, mobile telephone handsets, dashcam systems and Body Worn Devices. The MRD technology is evolving and may include such technology provided a Local DPIA is conducted and the concepts of data protection by design and by default in section 76 of the Act of 2018 are factored into the proposed use of such technologies in advance of their deployment.

12.8 Data Protection by Design and Data Protection by Default
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. There is the potential with different types of technology for new information to be gathered. Appropriate safeguards must be incorporated by Local Authorities which are technology specific and subject to approval by the Oversight Board and the Chief Executive.

12.9 In accordance with the provisions of Section 76 of the Act of 2018 the process detailed in this Code of Practice seeks to ensure that the necessity for the use of an MRD and the identification of risks to the privacy of Data Subjects are considered at the design stage. The application of the Code, the Local DPIA process, the role of the Oversight Board and Chief Executive as well as the implementation of the various standardised policies and procedures ensures that each Local Authority seeking to use MRDs for the prevention, detection and prosecution of offences under the Act of 1996 will both have undertaken a privacy by design and default process prior to the deployment of MRD and have implemented the required appropriate technical and organisational measures in order to be compliant with section 76(2) of the Act of 2018.

12.10 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.

12.11 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: on 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.

12.12 By default, only personal data which are necessary for the specific purpose of the processing are processed. 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 is built into the processing by default. Technological and organisation measures such as those outlined earlier are also required to ensure appropriate design by default is in place for MRDs systems used under this Code.

Examples of privacy be design & default

1. Local Authorities shall ensure that MRD equipment that is procured and deployed is such that its functionality is appropriate and proportionate to the stated objective for which it is being deployed. MRD cameras with enhanced or additional functionality not required for a site-specific deployment must have that additional functionality disabled.
2. Each Local Authority must develop a set of Standard Operating Procedures (SOPs) that will define the operating procedures to be followed by Business Units seeking to deploy and operate MRDs. Section 20 of this Code prescribes the suite of SOPs that must be in place prior to the deployment of an MRD for the purposes covered by this Code.

12.13 Local DPIA's shall be reviewed as the Oversight Board considers appropriate, subject to a general minimum of 3 years between each review, unless, circumstances require, when reviews will be more frequent. Continued use of MRDs in accordance with section 14B of the Act of 1996 shall require a justification of necessity and proportionality.

12.14 A Recording Device within the meaning of section 5 of the Act of 1996 specifically excludes Automatic Number Plate Recognition Devices or Facial Recognition Devices and is, therefore, specifically excluded from this Code. Furthermore, Authorised Persons will be prohibited from using their own personal devices, such as a smartphone or tablet, and will be authorised to only use devices issued by or on behalf of the relevant Local Authority, save, wholly exceptionally, in emergency situations, most particularly where an unexpected but real and concrete perceived threat to personal safety arises.

13.0 Principle 4 – Personal data shall be accurate and kept up to date

13.1 Local Authorities will ensure, insofar as is possible, that Personal Data which it stores is accurate and, where appliable, that it is kept up to date. All reasonable steps shall be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay. For more information on the restrictions that may apply to the rectification of Personal Data held by Local Authorities please see "Data Subject Rights" at section 18 below.

13.2 For the data captured to be used for evidential purposes, it is critical that the Information Systems team within Local Authorities ensure that all MRDs are maintained, and that any timing, clock, or geo-location facilities are synchronised, calibrated and verified. Failure to maintain MRDs may increase a risk that unsynchronised, uncalibrated footage could introduce doubt and inconsistency into the captured data, rendering it of weak evidential value for enforcement purposes.

14.0 Principle 5 – Personal data shall identify data subjects for no longer than is necessary

14.1 Personal Data captured by the operation of MRDs under Section 14B of the Act of 1996 shall not be retained for longer than is necessary to fulfil the purpose for which they were initially obtained.

14.2 Data collected by MRDs will be downloaded and stored in a secure encrypted software platform as soon as practically possible after being captured with access restricted only to authorised Local Authority staff and/or Authorised Persons. Data shall be examined by authorised personnel and/or Authorised Persons and only data that is relevant for evidential purposes will be separated and ear marked for retention for a period that is commensurate with the applicable evidential purposes e.g. where the Local Authority is investigating an alleged offence under the Act of 1996, if the data has evidential value to another law enforcement agency being a Competent Authority, if the data is otherwise to be shared in accordance with this Code or if the data is to be retained otherwise in accordance with law.

14.3 Where Personal Data is captured by the operation of MRDs, and that data is not required by the Local Authority for evidential purposes under the Act of 1996 or otherwise for Law Enforcement Purposes it must be erased in accordance with the Retention Policies of the Local Authority. If that Personal Data cannot be erased in order to preserve evidence, reasonable efforts shall be made to obscure or pixelate such Personal Data so as to render the Data Subject anonymous or unidentifiable where possible. In addition, every effort shall be made to deploy data minimisation techniques as specified in Local DPIAs to reduce the possibility of capturing excessive Personal Data. For example, body worn cameras will only be covertly activated when Authorised Persons, have a safety and security concern arising in respect of, or during, action(s) undertaken for the prevention, investigation, detection, or prosecution of offences under the Act of 1996. Footage will be deleted automatically after 28 days unless it is required for further investigation, in which case it will be deleted after all stages in the process are completed. Unnecessary footage will be deleted when identified.

15.0 Principle 6 – Security

15.1 Putting effective security safeguards in place helps ensure the integrity of Personal Data particularly if it is to be used as evidence in legal proceedings. It builds public confidence in Local Authorities and how they approach the handling of Personal Data.

15.2 Security extends to technical and organisational security, including cyber and physical security. Local Authorities as Controllers of Personal Data must put in place measures to ensure appropriate security of the data and to protect against Personal Data Breaches.

15.3 Data collected by the MRD is to be downloaded from the device to a secure encrypted software platform as soon as is practicable after collection, where access shall be restricted to authorised Local Authority staff and/or Authorised Persons.

15.4 Local Authorities must stipulate in their respective policies governing the operation of MRDs that MRDs active in field operations are to be kept in the custody of the Authorised Person operating them and following operations are to be securely locked in their vehicle for as short a duration as possible until the data thereon can be securely downloaded from the MRD to Local Authority encrypted software platforms and the said data is to be completely removed from the MRD original used to collect the data in question. Authorised Persons are prohibited from storing MRDs containing Personal Data in their vehicle overnight.

15.5 It is important that there are effective safeguards in place to ensure the integrity of recorded Personal Data and information and its usefulness for the purpose for which it is intended to be used. Recorded data comprising Personal Data shall be stored in a way that maintains the integrity of the image and information with particular importance attached to ensuring that meta data e.g., time, date, and location, is recorded reliably, and compression of data does not reduce its quality to an extent that it is no longer suitable for its intended purpose. This is to ensure that the rights of individuals recorded by MRDs are protected and that the material can be used as evidence in court. This will ensure the efficacy of the data when used in criminal proceedings. If there is no clearly justifiable reason to retain the recorded Personal Data, the data must be securely deleted after 28 days from the date of collection.

15.6 Evidence obtained by the operation of MRDs may be admitted as evidence in criminal proceedings and shall not require the device from which it was obtained to be exhibited in court proceedings. A failure to observe any provision of section 14B or this Code on the part of a Local Authority shall not (without prejudice to the power of the court to exclude evidence) of itself affect the admissibility of any evidence thereby obtained. It shall be presumed, unless the contrary is shown, that the information produced by the MRD, and any copies thereof is accurate and the MRD was operated in accordance with this Code pursuant to Section14D of the Act of 1996.

15.7 A person who falsifies, conceals, destroys, or otherwise disposes of information gathered by a recording device while it was or is being operated under the Act of 1996, permits the falsification, concealment, destruction, or disposal, of such information, or knowingly causes damage to or destroys a recording device shall be guilty of an offence. A person shall not be guilty of an offence as aforementioned where he or she destroys or disposes or permits the destruction or disposal of information gathered by a recording device in accordance with this Code or otherwise in accordance with law.

15.8 It is important that data captured by MRDs can be shared with other enforcement agencies who are Competent Authorities, when appropriate. Data requiring external transfer shall be shared via a secure encrypted software system and where same cannot be facilitated, encrypted portable media shall be used, and hand delivered to the Competent Authority in conjunction with chain of custody documentation to ensure integrity of the data. for evidential purposes. Any transfer of Personal Data to a Competent Authority i.e., other Local Authorities, the EPA, AGS, contracted operator or service provider shall be governed by a data sharing agreement or data processing agreement, where appropriate.

15.9 The effectiveness of the operation of MRDs will be dependent upon its capability to capture, process, analyse and store images and information of a quality to assist Local Authorities in preventing, investigating, detecting, or prosecuting offences under the Act of 1996.

15.10 Approved standards may apply to the system functionality, the installation and the operation and maintenance of MRDs. Approved standards are available to inform good practice for the operation of MRDs including those developed by the IAA, PSA or at a European level. Where appropriate, a Local Authority shall consider approved standards relevant to the effective application of technology in operation. It must take steps to secure certification against those standards where such certification is reasonably and readily available. Such certification may involve assessment by an independent certification body. This has benefit of promoting best practice in the operation of the technology in question and promotes public confidence and safety.

15.11 Local Authority staff and/or Authorised Persons who may assist them, shall be trained in the operation of MRD technology in accordance with reasonable industry recommendations (where applicable) to ensure compliant, safe, and efficient use of technology. Where no industry standards apply, staff shall possess the necessary skills and knowledge to effectively operate MRD including training in Data Protection Laws as they apply to the processing of Personal Data under this Code.

16.0 Principle 7 – Storage limitation – Retention periods

16.1 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 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 may be required for evidence in court proceedings.

Authorised waste premises are licensed to operate for a period of 5 years. Data captured by MRDs will be kept for the lifetime of the license to ensure that the maximum permitted intake of waste at the premises is not exceeded and 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. Data collected from unauthorised waste premises will be retained until enforcement action is concluded and all appeals exhausted by the Occupier of the Premises.

16.2 The retention period applicable to Personal Data captured by MRDs 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 exceptional cases.

16.3 Personal Data collected and assessed and deemed not required will be deleted from the Local Authority secure encrypted storage platform within 28 days from capture in accordance with Local Authority policy.

16.4 The National 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.

17.0 Principle 8 – Disclosure of Personal Data

17.1 The principal purpose for the operation of MRDs under this Code is to prevent, detect, investigate, or prosecute offences under the Act of 1996 or for the purposes of ensuring the personal safety or security of Authorised Persons in so doing, however, there may be instances where it is appropriate to share information including Personal Data captured by MRDs 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 sharing of Personal Data obtained from MRDs must be lawful and in compliance with Guiding Principle 2 as per section 11 above. Disclosure of images or information constituting Personal Data may be appropriate where Data Protection Laws provide exemptions which permit it, provided that the applicable requirements of the Data Protection Laws are satisfied or were permitted otherwise by law. An 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 which ensures a proportionate approach by the Local Authority as Data Controller.

17.2 Personal Data shall only be shared or provided to 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. The terms of the data sharing will be governed by agreements in writing to ensure that all parties involved in the processing do so in accordance with the Data Protection Laws and best practice guidance.

17.3 Any transfer of data to a Competent Authority in a third country i.e., outside of the European Union, including to Local Authorities in Northern Ireland or elsewhere in the United Kingdom , will be lawful only if it complies with Chapter V of the LED as transposed into Irish law by sections 96-100 of the Act of 2018 such as a on the basis of an adequacy decision for law enforcement purposes.

17.4 Personal Data shall also be provided to AGS in appropriate circumstances. A request in writing will need to 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 in accordance with this Code) and set out the reasons why it submits that the disclosure of the data in question is necessary and proportionate to that purpose for the request to be lawful within the meaning of section 71(5) of the Act of 2018.

17.5 As a Competent Authority a Local Authority may on occasion share Personal Data captured by MRDs with other Competent Authorities for Law Enforcement purposes, e.g., Authorised Persons, Competent Authorities such as other Local Authorities (which include WERLAs and the NTFSO) or the EPA, for the prosecution of alleged offences under the Act of 1996.

17.6 It is a matter for each Local Authority to identify which person(s) within the Business Unit are authorised 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 DPO.

17.7 The Waste Enforcement sections of individual Local Authorities may supply copies of MRD 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 MRD 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 MRD data being relied on in Court.

17.8 Personal Data requiring external transfer shall be shared via a secure encrypted system and when same cannot be facilitated e.g., if broadband may be an issue, encrypted portable media shall be used to transfer the MRD footage. In such instances, the media will be hand delivered to the Authorised Person or Competent Authority and accompanied by chain of custody documentation to ensure the integrity of the data. The DPO in each Local Authority will endorse the transfer of the data and require approval by an authorised representative of the Authorised Person or Competent Authority prior to the transfer or sharing of any data.

18.0 Principle 9 – Data Subjects Rights

18.1 The processing of Personal Data by the operation of MRDs pursuant to section 14B of the Act of 1996 and in accordance with this Code is for Law Enforcement Purposes only by 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.Therefore, the processing of Personal Data under this Code falls within 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 respective Local Authorities, insofar as the processing of any Personal Data that occurs is captured by GDPR and, accordingly, is outside the scope of this Code.

18.1 Data Subjects have the following rights 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).

18.3 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.

18.4 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) protecting the rights and freedoms of other persons

18.5 A Local Authority acting in its capacity as a Controller shall have clear local polices and guidelines in place to deal with Data Subject rights in relation to Personal Data captured by MRDs that comply with Part 5 of the Act of 2018. With the exception of the operation of Covert MRD, 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 privacy notice or data protection policy published on a Local Authority's website. The Data Subject rights referenced in paragraph 18.2 above are set out in more detail below and are subject to any restrictions in section 94 of the Act of 2018 as outlined above that may arise on a case-by-case basis.

18.6 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 those results in discrimination against an individual based on a special category of Personal Data is prohibited.

18.7 Right to Information

Data Subjects shall be provided with the information in 18.6.1. to 18.6.6. at the time their Personal Data is obtained. This can be done by directing the Data Subjects to a privacy notice or data protection policy on each Local Authorities website, to comply with section 90 of the Act of 2018 unless the information is already in the possession of the Data Subject. Prominent signage can signpost a Data Subject to the location of this information:

18.7.1 The identity and contact details of the Local Authority as Controller;
18.7.2 The contact details of the DPO of the Local Authority;
18.7.3 That the Personal Data will be processed for Law Enforcement Purposes as set out in Section14B the Act of 1996;
18.7.4 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;
18.7.5 Information detailing the right of the Data Subject to lodge a complaint with the DPC and the contact details of the DPC;
18.7.6 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:

18.7.6.1 the legal basis for the processing of the data concerned, including the legal basis for any transfers of data (if applicable);

18.7.6.2 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;

18.7.6.3 where applicable, each category of recipients of the data.

18.8 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, are to be provided with the following information to comply with section 91 of the Act of 2018:

18.8.1 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;

18.8.2 Where such data have been or are being so processed, be provided by the Local Authority with the following information:

18.8.3 A description of –

18.8.3.1 the purpose of, and legal basis for the processing,

18.8.3.2 the categories of Personal Data concerned,

18.8.3.3 the recipients or categories of recipients to whom the Personal Data concerned have been disclosed, and

18.8.3.4 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.

18.8.4 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 (i.e., written text) unless the supply of such a copy is not possible or would involve disproportionate effort or the Data Subject agrees otherwise;

18.8.5 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;

18.8.6 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) of the Act of 2018.

18.8.7 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 that individual, a Local Authority shall not provide the Data Subject with the information that constitutes such Personal Data relating to that other individual.

18.8.8 A Local Authority will use reasonable endeavours to obscure or pixelate MRD 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.

18.8.9 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.

18.8.10 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.

18.9 Right to Rectification

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

18.9.1 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 are incomplete in a material manner. Where a Local Authority is satisfied that the Personal Data to which the request relates are inaccurate, it shall rectify the data as soon as may be possible and not later than one month after the date on which the request is made.

18.9.2 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 (as outlined in sections 10-16 above) or in contravention to the processing of special categories of personal data under Part 5 (section 73(1) of the Act of 2018), 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 possible and not later than one month after the date on which the request is made.

18.9.3 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) of the Act of 2018.

18.9.4 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.

18.9.5 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 18.10.4 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.

18.9.6 If a Local Authority is not satisfied to rectify or erase Personal Data on foot of a request to do so and paragraph 18.10.4 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:

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

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

18.9.7 Where a Local Authority has restricted the processing of Personal Data pursuant to section 92(11) as set out 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.

18.9.8 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.

18.10 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:

18.10.1 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.

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

18.10.3 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 Local Authority under those sections. In those circumstances a Local Authority may charge a reasonable fee to the Data Subject in respect of the request, having regard to the administrative cost to the Local Authority of complying with the request or refuse to act upon the request.

18.10.4 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 to lodge a complaint with the DPC and the contact details of the DPC.

18.10.5 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.

18.10.6 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.

18.11 Right to Indirect Exercise of rights and verification by DPC

18.11.1 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.

18.11.2 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, if applicable. 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.

18.12 Records to be maintained

18.12.1 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:

18.12.1.1 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;

18.12.1.2 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.

18.12.1.3 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;

18.12.1.4 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 and make that record available to the DPC if requested.

18.13 Miscellaneous Provisions relating to Data Subject Rights

18.13.1 Data Subjects shall be informed verbally (where possible) in advance of the activation of a MRD by Authorised Persons that their Personal Data may be processed, and the Data Subject shall be informed of their rights generally and directed to a privacy notice

or data protection policy of the relevant Local Authority.

18.13.2 Where applicable, Authorised Persons operating a MRD shall have signage on high visibility clothing specifying MRD footage is in use.

18.13.3 Where applicable, individual policies of Local Authorities shall insofar as is possible identify locations covered by MRDs in an effort to ensure insofar as possible transparency in its processing of Personal Data when MRDs are deployed for Law Enforcement Purposes under this Code.

18.13.4 Each Local Authority must ensure that, with the exception where an approval for Covert MRD has been issued, adequate signage is placed at locations where MRDs are used for the purposes of preventing, investigating, detecting, or prosecuting offences under the Act of 1996. Signage is clearly visible and legible to members of the public and includes the name and contact details of the Local Authority as Controllers, signposts Data Subjects to the Local Authority website for more information, as well as noting the specific purpose(s) for which the MRD is deployed. The DPO of the Local Authority shall be consulted, in advance, on any signage and other transparency materials

18.13.5 Appropriate locations for signage include:

18.13.5.1 at or in close proximity to each MRD.

18.13.5.2 entrances to premises in which MRDs are in use.

18.13.5.3 any other areas/ locations where MRDs are in use for the purposes of section 14B of the Act of 1996 and this Code.

18.13.6 Each Local Authority will 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.

For example, if drones are used in public areas where the recording perimeter cannot be easily defined (for example entrance to farmland or other private property), privacy notices may not be enough, and a layered approach may be required:
a) Signage outside the location or at certain perimeter points;
b) Signal notifying the public that the drone is in operation and notifying when recording is taking place by use of sounds/flashing lights;
c) Authorised Persons to identify themselves as the drone operator by wearing highly visible clothing and be ready to provide the information required.

18.13.7 Transparency requires that any information addressed to the public or to the Data Subject be concise, easily accessible, and easy to understand. Clear and plain language and, , where appropriate, visualisation should be used. The appropriate measures to convey this information to the Data Subject depend on the specific context and environment in which the data is collected and processed.

For example, in the case of body worn cameras this may include visible notices on clothing worn by Authorised Persons, badges next to equipment containing information or links, or otherwise declaring to or bringing to the attention of Data Subject the relevant information. The wearer or user of the body worn camera will likely be the first point of contact for affected Data Subject, and therefore should be given appropriate training on how to respond to queries or Data Subject requests.

18.13.8 Data Subjects will need to provide such information as a Local Authority may reasonably require. This shall be set out in the policies of Local Authorities in order to satisfy itself of the identity of the Data Subject making a request under Chapter 4 of Part 5 of the Act of 2018; and to locate any relevant Personal Data or information e.g., relevant dates and timeframes, or otherwise enable the requested Local Authority to process the request as permitted in law.

18.13.9 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, or to otherwise enable the Local Authority to process the request as permitted in Data Protection Laws.

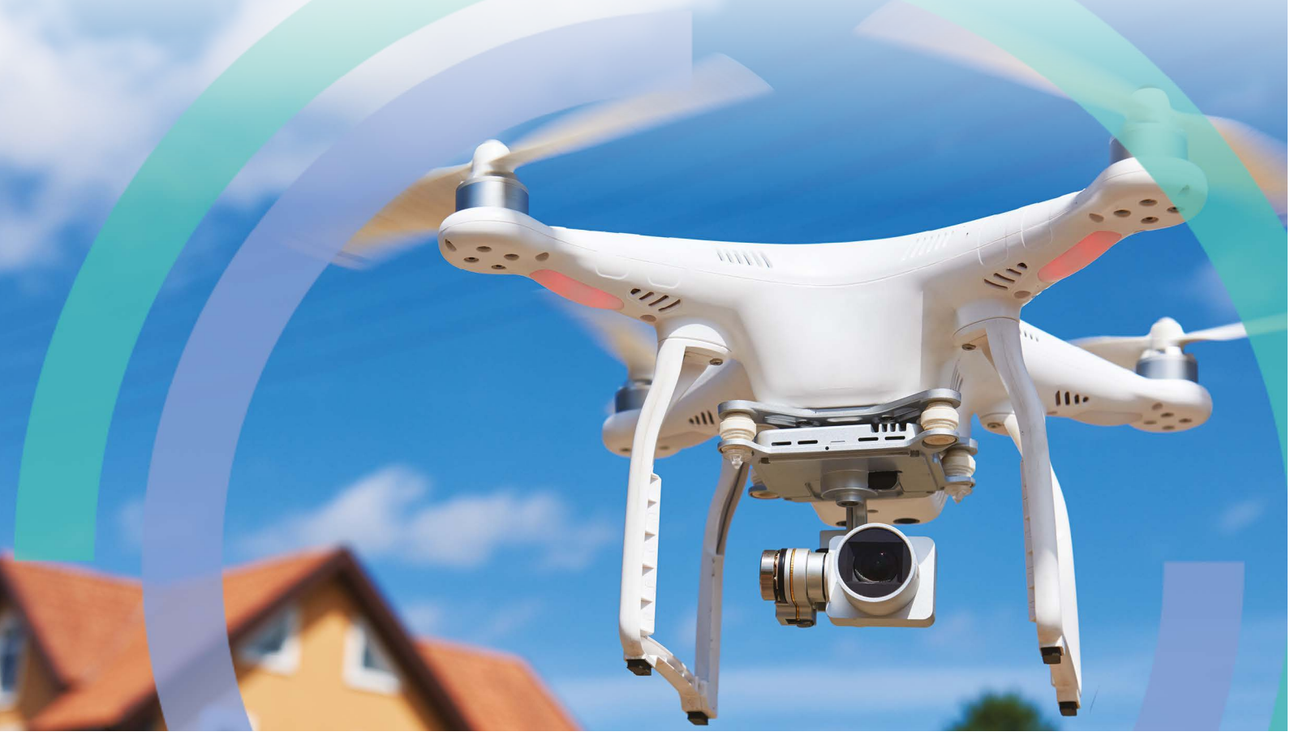
18.13.10 To enable the Local Authority to satisfy itself as to the identity of the Data Subject or to satisfy itself as to whether the Personal Data concerned are inaccurate or should be erased, the Local Authority may request such additional information from the Data Subject as may be necessary to confirm 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 Section2 91(2) and 91(4) of the Act of 2018, as the case may be.

18.13.11 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 MRDs under the Act of 1996 or otherwise where restrictions on the above-mentioned Data Subject rights are supported by the grounds outlined in section 94 of the Act of 2018.

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

18.13.13 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.



19.0 Principle 10 – Covert use of Mobile Recording Devices

19.1 In addition, to the principles, safeguards and related procedures set out above, in the exceptional circumstances where a decision to authorise the use of Covert MRDs is under consideration by the Oversight Board and, the Board places a recommendation for its use before the Chief Executive for a decision to authorise same, the following additional principles, safeguards and procedures shall apply.

19.2 The covert use of MRDs should only be taken in very exceptional circumstances and then only when it is subject to the suitable and specific measures to protect the privacy rights of individuals as specified in this Code of Practice. Such use will only be actioned on a case-by-case basis where the Local Authority has exhausted all other deterrent measures to prevent, investigate, detect and prosecute offences under the Act of 1996, without any positive impact in countering and reducing instances of offending and where the Chief Executive, on foot of a recommendation of the Oversight Board, has considered it necessary to authorise the instances where an Authorised Person may consider use of the Covert MRD in advance of the deployment or operation of Covert MRD. The operation of Covert MRD for this specific and limited situation will be permitted under this Code provided it complies with local SOPs and policies on the use of Covert MRDs.

19.3 The Business Units within Local Authorities exceptionally proposing the use of Covert MRD must demonstrate that it is justifiable and reasonable to the Oversight Board in advance of its deployment and this may be achieved by detailing the less intrusive measures which have already been taken by the Local Authority to prevent, detect, investigate and prosecute offences under the Act of 1996, without any positive impact in countering and reducing instances of alleged offending prior to recommending the use of Covert MRDs. These may include where practicable deploying alternative less intrusive deterrent strategies such as:

- increasing lighting in an area prone to offences;
- improving security;
- carrying out regular inspections;
- investing in regeneration projects with a view to improving the area;
- appropriate and regular training of staff; and
- exhausting all available powers under the Act of 1996 e.g., section 14(1)(a) allows an Authorised Person to bring persons onto a Premises including a member of AGS.

19.4 An Oversight Board in making a recommendation to proceed with the planned deployment of the use of Covert MRD to a Chief Executive of a Local Authority must be satisfied that its recommendation thereto is supported by:

(i) documentary evidence of the incidents which have led to the decision to proceed with same;
(ii) details of the less intrusive measures deployed by the Local Authority before Covert MRDs have been considered an appropriate and necessary response;
(iii) reasonable grounds for believing an alleged offence is going to be committed under section 14 of the Act of 1996 based on intelligence received and/or the observations of an Authorised Person; and
(iv) No covert recording can take place in an area prior to the Oversight Board being satisfied of the necessity for the operation of MRDs and after a Local DPIA has been conducted and recommended by the Oversight Board for approval by the Chief Executive of the Local Authority.

19.5 A Business Unit in a Local Authority that is seeking exceptionally permission to deploy Covert MRD shall complete a specific DPIA for the use of covert MRD. The said specific DPIAs which will be based on SOP, shall address the following factors when considering the necessity and proportionality for the exceptional use of Covert MRD:

- Specify that the use of Covert MRD is solely for the purpose of preventing, investigating, detecting, or prosecuting offences under the Act of 1996 or ensuring the personal safety and security of Authorised Persons in so doing;
- Provide evidence of a threat to the health and safety of Authorised Persons;
- Specify the seriousness of the alleged offences being committed;
- Identify the scale of the alleged offences being committed;
- Provide details of the harm that will arise if the alleged offences remain ongoing;
- Provide details of the cost to the Local Authority to remedy the damage done by the alleged offender;
- Identify the reasons as to why only Covert MRD will be effective in obtaining sufficient evidence to secure a conviction;
- Demonstrate conclusively that the risk to privacy rights of persons unrelated to the alleged offences have been identified and sufficient steps taken to mitigate or eliminate these risks prior to deployment; and
- Specify a detailed timeline for the deployment of Covert MRD with a clear date by which the authorisation for the deployment of Covert MRD will expire.

19.6 It is recognised that in exceptional cases an Authorised Person may determine that it is necessary and proportionate to ensure his/her personal safety and security in preventing, investigating, detecting, or prosecuting offences under the Act of 1996 to use Covert MRD. The deployment of Covert MRDs in this situation shall be a measure of last resort. The use of Overt MRDs, as opposed to Covert MRDs, may greatly enhance personal safety and security and so it will be a very exceptional circumstance that will justify the use of Covert MRD by an Authorised Person for the purpose of ensuring his or her personal safety or security in preventing, investigating, detecting, or prosecuting offences under the Act of 1996.

For example, if an MRD e.g., a drone is used covertly, this may be in response to a problematic site where there is a serious risk of environmental pollution, and the operators of the pose a threat to the personal safety and security of Local Authority Personnel including Authorised Persons.

Examples of instances where deployment of Covert MRD may be considered necessary and proportionate are as follows;

1. Waste Enforcement Officer (WEO), following an anonymous complaint from the public becomes aware of a potential unauthorised End of Life Vehicle (ELV) site. The WEO carries out an inspection of the site and the following is noted:
   - There is a serious risk of environmental pollution;
   - The operator of the site verbally abuses and physically threatens the WEO;
   - On subsequent inspections the site is inaccessible due to high fencing and locked entrance gate;
   - The WEO is unable to contact the operator of the site;
   - The WEO undertakes an inspection of the site using a MRD e.g., drone;
   - Prior to the drone flight a dynamic DPIA and flight risk assessment is carried out; and
   - The images will be used as part of legal proceedings against the operator.

2. WEOs are dealing with a permitted waste facility that has breached the conditions of its permit and is causing serious environmental pollution. The following is noted: -
   - WEOs enter and inspect the site using their powers under Section 14 of the Act;
   - On entering the site, the operator verbally abuses the WEOs and physically threatens them;
   - The WEOs leave the site and discover that their vehicles are vandalised;
   - On subsequent inspections and due to the safety and security concerns, the WEOs decide to undertake a survey of the site to capture and assess the extent of the unauthorised activity using an MRD e.g., a drone
   - Prior to the drone flight the WEOs undertake a dynamic DPIA and flight risk assessment and
   - The images will be used as part of legal proceedings against the operator.

3. A WEO whilst driving in their vehicle observes a truck attempting to unload a potentially suspicious container along the side of a roadway close to the Northern Ireland boarder. The following is noted: -
   - The individuals attempting to unload the container are wearing dark clothing, with their facial

features partially covered with a neck scarf;
- The WEO forms an opinion that there is a potential risk of environmental pollution;
- The WEO assesses the situation and decides not to intervene due to the perceived risk posted to his/her personal safety and security;
- The WEO activates the video recording function on his/her MRD e.g., phone and/or dashcam and records the activity from a distance (within his/her vehicle);
- The individuals dump the container from the vehicle onto the roadway;
- The WEO approaches the container and determines that the liquid is potential waste e.g., diesel wash/laundering sludge; and
- The images are used as part of legal proceedings against the individuals allegedly committing the offence.

19.7 The use of unplanned or emergency Covert MRD by an Authorised Person to ensure his or her personal safety shall be governed by Local SOPs and policies which provide clear guidance to Authorised Persons to enable them to make well-informed decisions about whether to deploy MRDs in unplanned circumstances and examples of when it would be considered justified, e.g. when an Authorised Person may have reasonable grounds for believing that a person has committed an offence or that an offence is going to be committed in accordance with section 14 of the Act of 1996. Local Authorities shall also have policies in place for handling retrospective authorisation by the Chief Executive on the recommendation of the Oversight Board for retention and further use of Personal Data captured by the unplanned use of Covert MRDs. For example, if an MRD e.g., phone and/or dashcam is to be used covertly, this may be in response to a situation where a WEO observes an offence being allegedly committed by an individual(s) but decides not to intervene due to the perceived risk posed to his/her personal safety and security.

19.8 The safety and security of Authorised Persons is paramount and appropriate training of staff must be undertaken to include avoiding situations which require use of Covert MRD, where possible, and deploying other less intrusive measures for detecting, preventing, investigating, or prosecuting offences under the Act of 1996 or ensuring the safety and security of Authorised Persons in so doing.

19.9 In addition to complying with this Code, the decision to use Covert MRD must comply with a Local Authority's own SOPs, MRD usage policy and be approved either prospectively or retrospectively, as the case may be, by the Chief Executive of the Local Authority based on a recommendation of the Oversight Board.

19.10 The decision to operate Covert MRD must only be taken in exceptional circumstances, be focused and of short duration with appropriate oversight by the Oversight Board within Local Authorities.

19.11 Only specific and relevant locations or individuals shall be recorded where there are justifiable reasons for doing so. Covert MRD shall not be used for general patrol/monitoring or for routine monitoring of areas prone to offences under the Act of 1996 or to monitor the movements of members of the public.

19.12 It should be noted that the examples provided above are just that, examples. Business Units seeking to exceptionally deploy Covert MRD must always complete a new Local DPIA specified in this Code for the use of Covert MRD and seek approval from the Oversight Board. Prior approval of the use of Covert MRD in any previous similar historical deployment must not be taken as approval for any other deployments of Covert MRD in a similar scenario in another location or at another time.

20.0 Principle 11 – Local Standard Operating Procedures

20.1 A set of Standard Operating Procedures (Local SOPs) shall be developed by Local Authorities and followed by their Business Units when seeking to introduce and implement MRDs in accordance with Section 14B of the Act of 1996 and this Code. The purpose of the Local SOPs will be to detail the considerations and measures to be taken in relation to the operation of MRD for the prevention, detection, investigation and/or prosecution of offences under the Act of 1996.

20.2 The SOPs will be developed in the following areas (which is not an exhaustive list):

- Preparation of a Local DPIA;
- Preparation of a business case for submission to the Oversight Board;
- How to identify situations where the operation of Covert MRD may be considered a necessary and proportionate measure for the purposes of investigating, detecting, preventing, or prosecuting offences under the Act of 1996 or a risk to the personal safety or security of an Authorised Person. This will include less intrusive measures to be deployed before use of Covert MRD may be considered appropriate;
- Appropriate signage to be used when operating an MRD for Law Enforcement Purposes;
- Security and maintenance of MRD equipment including cameras, retention, storage, and destruction of MRD data;
- Providing clear guidelines regarding training including, where appropriate, if any of the personnel involved will be subject to child safeguarding vetting;
- Emergency MRD use where an Authorised Person has reasonable grounds for believing that there may be a risk of an alleged offence being committed or the commission of an alleged offence is occurring within the meaning of section 14 of the Act of 1996;
- Maintaining records in compliance with Data Protection Laws applicable to the use of MRD for Law Enforcement Purposes;
- Chain of custody for data captured on MRDs;
- Restrictions on the use of Covert MRDs;
- Training to be provided to Local Authority staff submitting business cases and/or operating MRDs for Law Enforcement Purposes under section 14B of the Act of 1996;
- Disclosure of MRD data and information to Authorised Persons and/or Competent Authorities for Law Enforcement Purposes;
- Periodic review of approved MRDs to ensure they remain necessary and proportionate and continue to comply with this Code;
- Procedure for handling concerns and complaints from individuals and organisations about the use of MRD for Law Enforcement Purposes under section 14B of the Act of 1996; and Procedures for handling requests from data subjects seeking to exercise their rights under Chapter 4 of Part 5 of the Act of 2018.

20.3 In addition to the Local SOPs outlined in paragraph 20.2 above several standardised guidance documents will be developed to assist individual Local Authorities to implement the 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 approval for the use of MRDs from the Oversight Board who will in turn seek approval from the Chief Executive;
- Terms of reference and suggested appointments to a Local Authority Oversight Board;
- Template Local DPIA;
- Template business case document for MRD proposals;
- Template ROPA;
- Template data processing agreement;
- Template data sharing agreement;
- Records retention schedules.

20.4 Local Authorities when preparing and implementing local policies; procedures and Local SOPs governing the use of MRD shall have regard to this Code.

21.0 Monitoring Compliance with this Code of Practice

21.1 The Oversight Board in each Local Authority shall be responsible for monitoring compliance by each Local Authority with the requirements of section 14B of the Act of 1996 and this Code and for ensuring that the use of MRDs by each Local Authority is compliant on an ongoing and regular basis and that their deployment of MRDs shall not be a permanent arrangement once put in place, but rather must be subject to ongoing review to continue to verify that its retention is justified and remains a necessary and proportionate measure. Reviews of Local DPIAs underpinning an approved use of an MRD must take place at a minimum of every 3 years, but more often if circumstances require.

LGMA
Local Government Management Agency

Cumann Lucht Bainistíochta Contae agus Cathrach
County and City Management Association

Rialtas Áitiúil Éireann
Local Government Ireland