An Coimisiún um Chosaint Sonraí
Data Protection Commission

Decision of the Data Protection Commission under Sections 111 and 124 of the Data Protection Act 2018 in the Case of 02/SIU/2018

Own-Volition Inquiry under Sections 110 and 123 Data Protection Act, 2018

on foot of Data Protection Audit Conducted under

Section 136 of the Data Protection Act regarding

The Surveillance of citizens by the State for

Law Enforcement Purposes

Commission Decision-Maker:

Helen Dixon (Commissioner for Data Protection), sole member of the Commission

Date of Decision: 25th March 2020

Contents

1. Purpose of this Document

1.1 This document is the final decision of the Data Protection Commission in accordance with Sections 111 and 124 of the Data Protection Act 2018 ('the Decision'). I make this Decision having considered the information obtained in the separate own volition inquiry conducted by Authorised Officers of the Data Protection Commission. The Authorised Officers who conducted the inquiry provided Kerry County Council (the **'Council'**) with the draft Inquiry Report and the final Inquiry Report.

1.2 This Decision contains a list of corrective powers under Section 127 of the Data Protection Act 2018 arising from the infringements which have been identified herein by the Decision Maker. It should be noted, in this regard, that the Council is required to comply with these corrective powers, and it is open to this office to serve an enforcement notice on the Council in accordance with Section 133 of the Data Protection Act 2018.

2. Background

2.1 Two officers (the **'Authorised Officers'**) of the Data Protection Commission (**'DPC'**) were authorised on 14 June 2018 to conduct a connected series of own-volition inquiries under Sections 110 and 123 of the Data Protection Act 2018 (**'the 2018 Act'**) into a broad range of issues pertaining to surveillance technologies deployed by State authorities, in particular the various local authorities and An Garda Síochána. In initiating the inquiries, the DPC wished:

i. To establish whether any data processing that takes place in this context is in compliance with relevant data protection laws, and

ii. To ensure that full accountability measures for the collection and processing of personal data are in place in advance of further investment and deployment of newer surveillance technologies.

2.2 Surveillance in public places has the potential to affect most, if not all, persons in the State. A permanent tension exists between surveillance measures to deliver security and other civil liberties, such as the ability to go about one's daily business free from unnecessary supervision. In this State, the Oireachtas has regulated the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places through Section 38 of An Garda Síochána Act 2005 (**'the 2005 Act'**).

2.3 The inquiry leading to this Decision was conducted initially by means of an audit under Section 136 of the 2018 Act. This facilitated the Authorised Officers in

compiling facts in relation to the deployment of surveillance technologies by the Council. The Authorised Officers sent a questionnaire to the Council for the purpose of the opening phase of the audit, sent preliminary queries in relation to the Council's replies to the questionnaire, and sent a request for further information to the Council on 13 May 2019. The Council responded to all of these requests for information.

2.4 The Authorised Officers conducted inspections for the purpose of the next phase of the inquiry. The Authorised Officers met with officials from the Council, including the Council's Data Protection Officer, before attending the following locations in May and June of 2019:

- the Regeneration Office at Áras an Phobail, Tralee;
- [redacted];
- CCTV cameras and signage in Killorglin Town;
- the bottle bank site at Garvey's Car Park, Tralee; and
- the Tralee Amenity Walk.

2.5 Ultimately, the Authorised Officers completed a final Inquiry Report which they submitted to me as Decision-Maker on 4 October 2019. I am obliged to consider that Inquiry Report and reach final conclusions as to whether I identify infringements of data protection legislation.

2.6 On 10 February 2020, I furnished the Council with my Draft Decision in this matter. The Draft Decision contained my provisional views as to whether or not infringements had occurred or were occurring, and a proposal in respect of corrective powers. The Draft Decision was provided to the Council to provide it with a final opportunity to make submissions on the provisional views expressed therein. On 9 March 2020, the Council made submissions on the Draft Decision. I have extensively considered those submissions prior to making this final Decision.

2.7 The findings made in this Decision include findings concerning CCTV systems authorised by the Garda Commissioner under Section 38 of the 2005 Act. This Decision does not consider the criteria used to assess and approve the schemes, nor does it consider whether the approval process was correctly undertaken.

3. Legal regime pertaining to the inquiry and the Decision

3.1 The Council operates CCTV systems for the purpose of detecting those engaged in littering and taking enforcement action in respect of same. Those CCTV systems have not been authorised pursuant to Section 38(1) of the 2005 Act. The Council operates CCTV systems at Amenity Walk to secure public order and

safety at the walkway. Those systems have also not been authorised under Section 38(1). The Council operates further CCTV systems that have been authorised pursuant to Section 38(1). The sole or primary purpose of those CCTV systems is securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences[1].

3.2 The General Data Protection Regulation (**'GDPR'**) is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR was transposed into Irish law by the 2018 Act. However, Article 2(2)(d) of the GDPR provides that:

> *'This Regulation does not apply to the processing of personal data … by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'*

3.3 The Law Enforcement Directive (**'LED'**) is a *lex specialis* that provides specific rules with regard to the processing of personal data for such purposes. The LED is transposed into Irish Law by Part 5 of the 2018 Act, which (as set out in Section 70 therein), applies

> *'…to the processing of personal data by or on behalf of a controller where the processing is carried out—*
>
> *(a) for the purposes of—*
>
> *(i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or*
>
> *(ii) the execution of criminal penalties,*
>
> *and*
>
> *(b) by means that—*
>
> *(i) are wholly or partly automated, or*
>
> *(ii) where the personal data form part of, or are intended to form part of, a relevant filing system, are not automated.'*

[1] This purpose is expressly provided for in Section 38(1) of the 2005 Act.

3.4 'Controller', for the purposes of Part 5, is defined in Section 69(1) as:

> *'(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or*
>
> *(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated—*
>
> *(i) by that law, or*
>
> *(ii) in accordance with criteria specified in that law;'*

3.5 'Competent authority', for the purposes of Part 5, is defined in Section 69(1) as including:

> *'(a) a public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in the State, including the safeguarding against, and the prevention of, threats to public security, or…'*

3.6 The Council is a 'competent authority' pursuant to this definition. It enjoys competence for the prevention, investigation, detection, and prosecution of certain offences under the Litter Pollution Act 1997. Furthermore, it enjoys a general competence regarding the prevention of crime, when performing its functions, under Section 37(1) of The 2005 Act[2].

3.7 Two criteria must be fulfilled for the LED, as incorporated by Part 5 of the 2018 Act, to apply to processing of personal data. Firstly, the processing must be conducted by or on behalf of a 'controller' as defined in Section 69 of the 2018 Act. Secondly, pursuant to Section 70 of the 2018 Act, the processing must be carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or the execution of criminal penalties.

[2] Section 37(1) provides that 'A local authority shall, in performing its functions, have regard to the importance of taking steps to prevent crime, disorder and anti-social behaviour within its area of responsibility.'

CCTV to detect and take enforcement action against those engaged in littering

3.8 The Council is a 'Controller' within the meaning of Section 69(1) of the 2018 Act in respect of the CCTV data that it processes to detect and take enforcement action against those engaged in littering. The Council is a competent authority that is determining the purposes and means of that processing. The Council decided to install those CCTV systems to assist in its litter detection and enforcement responsibilities. Thus, the Council determined the purposes for operating the CCTV systems at those locations. It also determines the means of the processing by determining how the data are processed. It controls who has access to the footage, when the footage is deleted and which images to capture.

3.9 The Council processes the CCTV footage to detect and take enforcement action against those engaged in littering. Section 3 of the Litter Pollution Act 1997 makes it a criminal offence to create litter in a public place. Thus, the purposes of this automated processing include the prevention, investigation, detection or prosecution of criminal offences. The result is that the LED, incorporated through Part 5 of the 2018 Act, is applicable to the CCTV systems used to detect and take enforcement action against those engaged in littering.

CCTV systems operated by the Council pursuant to Section 38 of An Garda Síochána Act 2005

3.10 The final Inquiry Report took the view that the GDPR is applicable to the CCTV systems that the Council operates pursuant to Section 38 of the 2005 Act. This Decision finds that the GDPR is not applicable to the processing of personal data through those systems and that instead, the Law Enforcement Directive, incorporated through Part 5 of the 2018 Act, is applicable. The analysis in respect of this finding is as follows.

3.11 The Council is a 'Controller' within the meaning of Section 69(1) of the 2018 Act in respect of the CCTV data that it processes pursuant to Section 38 of An Garda Síochána Act 2005. Section 38, and the delegated legislation made pursuant to it, determine the purposes and means of that processing of the personal data conducted by the Council in relation to these CCTV. Section 38(1) clearly sets out the sole or primary purpose of the CCTV as *'securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences'*. The means of the processing of the personal data are

set out in Section 38 and the delegated legislation made pursuant to it, including who has access to the CCTV[3] and the systems that can be used[4].

3.12 Order 4(d) of the Garda Síochána (CCTV) Order 2006[5] requires local authorities to undertake to act as a data controller on the application for authorisation for the operation and installation of the CCTV. The Council has done so in respect of the authorisations. Thus, it is a controller pursuant to part (b) of the definition of controller in Section 69(1) of the 2018 Act.

3.13 The sole or primary purpose of the Council's operation of this CCTV is statutorily determined in Section 38(1) of the 2005 Act as *'securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences'*. Section 70 of the 2018 Act provides that Part 5 of the Act applies to automated processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences. This is not a cumulative test, and any one of these purposes is sufficient to bring the processing under the Part 5. Therefore, even though the Council does not use this CCTV to investigate or prosecute criminal offences, it is clear that it records[6] CCTV at these locations for the purpose of securing public order and safety by facilitating the prevention of criminal offences. This purpose alone is sufficient to bring the processing under Part 5 of the 2018 Act.

3.14 Where data are processed for one purpose and then used for another, if the purpose changes with that new use, the GDPR may become applicable. There is no evidence in the inquiry that suggests that the Council processed the CCTV data for any purpose that would exclude the application of Part 5 of the 2018 Act.

4. Materials considered

4.1 The Authorised Officers delivered the Inquiry Report to me on the 4th October 2019. I was also provided with all of the submissions received in compiling the report and the submissions made by the Council in respect of the draft Decision, including:

i. The Data Protection Audit Questionnaire,

[3] Section 38(7) requires the Council to ensure that members of An Garda Síochána have access to the CCTV at all times for, inter alia, the purpose of retrieving information or data recorded by the CCTV.
[4] CCTV is defined in Section 38(14) defines CCTV as *'any fixed and permanent system employing optical devices for recording visual images of events occurring in public places'*. Section 38(1) authorises such systems.
[5] S.I. No. 289/2006 – Garda Síochána (CCTV) Order, 2006.
[6] Pursuant to Section 69(1) of the 2018 Act, Recording data is expressly included within the meaning of 'processing' for the purposes of Part 5 of the 2018 Act.

ii. Kerry County Council's response to the Data Protection Audit Questionnaire,
iii. Kerry County Council's report to accompany the completed Audit Questionnaire,
iv. Kerry County Council CCTV Policy,
v. Kerry County Council CCTV Inventory,
vi. Kerry County Council's replies to preliminary queries from the DPC,
vii. Information request and replies from Kerry County Council,
viii. Kerry County Council's submissions on the draft report,
ix. Kerry County Council's submissions on the redrafted version of Issue 15,
x. Kerry County Council Environment Section's Code of Practice for Use of CCTV Systems,
xi. Kerry County Council's procedure from 1st June 2019 for the secure, transfer of CCTV footage to third parties and within the Data Controller organisation,
xii. An Garda Síochána Authorisations under Section 38(3)(c) of An Garda Síochána Act, 2005,
xiii. Kerry County Council Data Protection Impact Assessment dated 10th October 2018,
xiv. Kerry County Council Data Protection Impact Assessment dated 30th July 2019, and
xv. Submissions made by the Council's Data Protection Officer on 9th March 2020.

4.2 I am satisfied that the audit and inquiry were correctly conducted and that fair procedures were followed throughout including, but not limited to, notifications to the data controller and opportunity for the data controller to comment on a draft Inquiry Report before it was submitted to me as decision-maker.

5. Data controller

5.1 This Decision and the corrective measures herein are addressed to Kerry County Council as the relevant data controller in relation to the findings made.

6. Personal Data

6.1 Section 69 of the 2018 Act defines 'personal data' as:

> *'"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 or an online identifier, or

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

6.2 This Decision concerns CCTV systems located in public places. The CCTV systems routinely process images of members of the public. It is possible to identify individuals from such images, even where an individual's face is not visible. Thus, the data processed by the CCTV systems constitutes 'personal data'.

7. Analysis and findings

7.1 The Authorised Officers identified a total of 15 issues in the course of their inquiry. I have considered each in turn and I also considered the commonality of issues identified. Given that the Council is a controller in each and all of the issues identified, I will group my analysis and findings based on the commonality of issues arising.

7.2 Since the inquiry commenced, the Council has taken steps to address some of the issues identified in the inquiry. This Decision sets out findings as to whether infringements of the 2018 Act have occurred by reference to the dates of the inspections conducted by the Authorised Officers (even if those infringements have since been addressed) or are occurring . Therefore, it is acknowledged that some of the findings in this Decision may since have been addressed by the Council.

A. Lawfulness of the CCTV systems for detecting and taking enforcement action against those engaged in littering and at Amenity Walk ('the Skinny Mile Walkway')

Inquiry Report Issues 1 and 5

7.3 The Council operates CCTV systems at five locations for detecting and taking enforcement action against those engaged in littering. These CCTV systems do not have authorisation under Section 38(1) of the 2005 Act. The Council has powers and duties for the prevention, investigation, detection and prosecution of litter related offences under the Litter Pollution Act 1997, the Waste Management Act 1996 (as amended), and the Local Government Act 2001. It relies on these

functions as a lawful basis for these CCTV systems on the basis that the CCTV systems are necessary for the performance of those functions.

7.4 Section 71(1)(a) of the 2018 Act requires that '*data shall be processed lawfully and fairly*'. Section 71(2) expands on the requirement that personal data be processed lawfully, providing that:

> *'(2) The processing of personal data shall be lawful where, and to the extent that—*
>
> *(a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70 (1)(a) and the function has a legal basis in the law of the European Union or the law of the State, or*
>
> *(b) the data subject has, subject to subsection (3), given his or her consent to the processing.'*

7.5 Section 71 of the 2018 Act must be interpreted alongside Article 8 of the LED. In *National Asset Management Agency v Commissioner for Environmental Information*[7]*,* the Supreme Court interpreted the Irish legislation[8] that implemented Directive 2003/4/EC[9]. The definition of '*public authority*' in the Irish legislation contained additional paragraphs to that in the Directive. The Court held, in relation to interpreting legislation introduced implementing an international treaty:

> *'this specific obligation undertaken by Ireland as a member of the EU requires that the courts approach the interpretation of legislation in implementing a directive, so far as possible, teleologically, in order to achieve the purpose of the directive.'*[10]

The Court went on to hold that:

> *'If even as a matter of purely domestic interpretation, the provisions of those subparagraphs might appear to either fall short of what is required by the Directive, or go further, an Irish court might be required*

[7] National Asset Management Agency -v- Commissioner for Environmental Information [2015] IESC 51.
[8] Statutory Instrument No. 133 of 2007.
[9] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC.
[10] Ibid At paragraph 10.

to adopt another interpretation which is consistent with the provisions of the Directive, if that is possible.'[11]

7.6 In *Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission*[12], the Court of Justice of the European Union confirmed that *'the principal of primacy of EU law requires not only the courts but all bodies of the Member States to give full effect to EU rules'*[13]. This case concerned the duty to disapply national legislation that is contrary to EU law. The duty to interpret national legislation teleologically to achieve the purpose a Directive is equally applicable to all Member State bodies.

7.7 Section 71 of the 2018 Act must be interpreted so far as possible, teleologically, in order to achieve the purpose of the LED. It is a clear purpose of the LED that processing that falls within its scope must be based on Union or Member State law. Article 8 of the Law Enforcement Directive provides for the lawfulness of processing:

> *'1.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) and that it is based on Union or Member State law.*
>
> *2.Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.'*

7.8 Thus, Article 8(1) sets out two criteria that must be fulfilled for processing to be lawful. First, the processing must be necessary for the performance of a task of a competent authority. Second, the processing must be based on Union or Member State law. Where Member State law forms the basis for processing, Article 8(2) elaborates on what must be specified in that law. It must specify the objectives of processing, the personal data to be processed and the purposes of the processing.

7.9 The requirement in Section 71 that data be processed lawfully must be interpreted as requiring that the processing be based on Union or Member State law. It goes beyond requiring that the controller's function alone is based on law. Member State law must specify the objectives of processing, the personal data to be processed and the purposes of the processing as per Article 8(2) of the LED.

---

[11] Ibid at paragraph 11.

[12] Case C-378/17, Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission , judgment of 4 December 2018 (ECLI:EU:C:2018:979).

[13] At paragraph 39.

7.10 The matters that Member State law must specify do not necessarily have to be codified in an Act of the Oireachtas, but they must have a clear legal basis, for example in the common law or statutory instrument. The Member State law must be clear, precise and its application must be foreseeable. Recital 33 of the LED elaborates on the form that such Member State law must take and what must be specified therein:

> *'Where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.'*

7.11 This means that the measures must regulate the processing by providing guidance to controllers and data subjects as to when particular processing is permissible. This is consistent with the case law of the Court of Justice of the European Union. For instance, in Schrems v Data Protection Commissioner[14] the court held (at paragraph 91):

> *'As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.'*

7.12 An Act of the Oireachtas, for example, might implicitly provide for the processing of certain personal data, without expressly listing each category of personal data

[14] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015(ECLI:EU:C:2015:650).

that is to be processed. Such an Act would be sufficient to provide a lawful basis once the objectives, the personal data to be processed and the purposes are clear and foreseeable from that Act.

7.13 The Council's use of CCTV footage cannot lawfully be based on The Litter Pollution Act 1997, the Waste Management Act 1996, and the Local Government Act 2001. I have considered the Council's submission, dated 9 March 2020, in which it stated that:

> *'These acts set out strong powers in relation to the detection of prosecution of offences in relation to issues such as indiscriminate dumping and as the powers of prosecution were the responsibility of the Local Authority, it was considered appropriate that a variety of measures utilised by council officials and litter wardens including the use of cctv would be adequately covered under such a range of legislation.'*

I have carefully considered the full range of legislation and the Council's use of CCTV to detect and take enforcement action against those engaged in littering. These Acts do not regulate this type of processing as is required by Article 8(2) of the LED. Although the Acts provide the Council with certain functions, including of the prevention, investigation, detection and prosecution of litter offences, and that this implicitly provides for the processing of certain categories of personal data, the Acts do not provide for processing of images of members of the public using CCTV footage in this manner. There are no provisions in any of the three Acts that can be said to govern such a wide scope of processing. Even if the Acts did specify for this personal data to be processed, in the absence of significant other amendments, the Acts would be severely lacking in rules that govern the scope and application of such CCTV, including, among others, the criteria that must be fulfilled before installing such CCTV, the supervision of such CCTV once installed, and the termination of the CCTV. Furthermore, the Acts do not specify any procedures for preserving the integrity and confidentiality of personal data processed by such CCTV.

7.14 Section 38 of the 2005 Act regulates the installation and operation of fixed and permanent CCTV for securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. This provision could, potentially, provide a basis for the Council's use of CCTV at these five locations. However, such CCTV systems must, amongst other things, be authorised by the Garda Commissioner. In the absence of such authorisation and general compliance with Section 38, I find that the Council's use of CCTV systems at these locations is unlawful.

7.15 The Council installed 26 CCTV cameras at Amenity Walk. The purpose of the cameras is to secure public order and safety at the walkway. I find that this processing is not based on Union or Member State law in circumstances where the cameras were not authorised by the Garda Commissioner under Section 38 of the 2005 Act. Therefore, I find that the processing of this personal data is not lawful and is in breach of Section 71(1)(a) of the 2018 Act.

Findings

7.16 **I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems at the 5 locations identified.**

7.17 **I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV systems at Amenity Walk.**

7.18 **Notwithstanding the unlawfulness of the CCTV systems at these locations, for completeness, this Decision considers below the remaining issues identified by the inquiry at these locations.**

B. Appropriate signage and general transparency

Inquiry Report Issue 2

Analysis

7.19 The Inquiry Team examined the CCTV signage on display at Garvey's Car Park bottle bank during their visit there. They also examined images of the signage at other bottle bank facilities. This signage is used to communicate certain information to members of the public.

7.20 The principle of transparency flows from the requirement in Section 71(1)(a) of the 2018 Act that data be processed fairly[15]. This principle concerns the provision of information to data subjects related to fair processing, how data controllers communicate to data subjects in relation to their rights and how data controllers facilitate the exercise of those rights. Provisions in respect of these concepts are found in the LED and in Part 5 of the 2018 Act.

7.21 Members of the public visiting Garvey's Car Park bottle bank have their images captured on the CCTV there before the CCTV notices come to their attention as

[15] Although the principle of transparency is not expressly referenced in Section 71(1)(a) nor in the Articles of the LED, Recital 26 of the LED provides that '*Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance…'*

there is no CCTV signage at the approach to the site. In this regard, Section 90 of the 2018 Act requires controllers to ensure that data subjects are provided with certain information, or that information is made available to them, within a reasonable period after the personal data are obtained. Unlike the corresponding requirement under the GDPR[16], there is no requirement in law for any of this information to be provided at the time when the personal data are obtained. In circumstances where CCTV notices are displayed within the car park, therefore, the information is made available to data subjects within a reasonable period after their images are captured on the CCTV footage.

7.22 The content of the CCTV notices that are on display at Garvey's Car Park bottle bank is detailed in the Inquiry Report. Each recycling receptacle displays a notice with *'TCI I bhfeidhm CCTV in use.'* There is also a notice on a poll in the car park that states:

> *'Rabhadh Ceamaraí TCI I bhFeihhm. CCTV Cameras in operation. Tuilleadh eolais, scanáil an cód QR nó teir go kerrycoco.ie/CCTV. To find out more, scan the QR code or visit kerrycoco.ie/CCTV.'*

These notices do not provide any information on the contact details for the data controller, the contact details of the data protection officer of the controller, nor the purposes of the CCTV cameras. Such information must be provided or made available to data subjects pursuant to Section 90(2) (a), (b) and (c) of the 2018 Act. However, Section 90 (3) goes on to stipulate that this information may be made available by means of publication on the website of the controller. As decision maker, I have conducted a search of the kerrycoco.ie/CCTV webpage. I am satisfied that this information is available at that page.

7.23 The information that the Council is obliged to provide or make available to data subjects must be in an easily accessible form. In this regard, section 93(1) of the 2018 Act provides:

> *'Where a controller—*
>
> *(a) provides or makes available information to a data subject under section 90*
>
> *(b) provides or makes available information to, or communicates with, a data subject pursuant to a request under section 91 or 92,*

[16] Article 13 of the GDPR requires that similar information be provided to data subjects at the time when personal data are obtained where the data are collected from the data subject. Article 13 of the LED permits the approach adopted in Section 90 in so far as it does not contain a corresponding requirement that Member States provide for the data to be made available at the time that they are obtained.

*the controller shall take all reasonable steps to ensure the information is provided or made available, or the communication is made, as the case may be, in a concise, intelligible and **easily accessible** form using clear and plain language.' **[emphasis added]***

The Article 29 Data Protection Working Party has given guidance on the meaning of 'easily accessible'[17]:

'The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question…'[18]

7.24 In the circumstances, reasonable steps to ensure that such information is available in an easily accessible form include:

i. Referencing 'kerrycoco.ie/CCTV' on the notices on the recycling receptacle, and

ii. Making the more detailed notice available at a height and location that is immediately apparent and functional to visitors to the car park.

I find that the Council has failed to take such reasonable steps. In reaching this finding, I have had regard to the fact that the notice on the front of each recycling receptacle does not reference the website where further information is available. The more detailed notice was on the opposite end of the car park, on a pole at a height that rendered the QR code to be not easily accessible.

Findings

7.25 **I find that the Council infringed Section 93(1) of the 2018 Act by failing to take all reasonable steps to ensure that the information provided to data subjects, pursuant to Section 90 of the same Act, is provided or made available in an easily accessible form. The availability of this information on the Council's website does not remedy this infringement as the physical signage on the waste receptacle does not reference the website and the other notice is at a height and location where it is not easily accessible to visitors of the car park.**

[17] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (17/EN WP260). Although these guidelines relate to the GDPR, paragraph 1 provides that 'I Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/680, these guidelines also apply to the interpretation of that principle.'

[18] Ibid at paragraph 11.

7.26 **I find that the lack of CCTV signage at the approach to the bottle banks does not infringe the 2018 Act as the 'reasonable period' requirement in Section 90 is complied with in circumstances where the CCTV signage is available within the car park. However, I note that the failure to place the signs in a way that makes the public aware that they are entering a CCTV area is in breach of the Council's own CCTV policy[19].**

7.27 **I find that the lack of information on the face of the CCTV signage regarding the contact details for the data controller, the contact details of the data protection officer of the controller, and the purposes of the CCTV cameras does not infringe Section 90 of the 2018 Act in circumstances where that information is available on the Council's website.**

C. Excessive data collection

Inquiry Report Issues 3 and 9

7.28 The Inquiry Team inspected photographs of the field of vision captured by the CCTV cameras operating at Garvey's Car Park and carried out an onsite inspection. The entire area that is adjacent to the bottle bank facility, including part of the car park, is captured in the field of vision. This results in the recording of images of members of the public who are not using the bottle bank facility. The Council submitted that the wider view is used to minimise indiscriminate dumping in the area adjacent to the recycling centre and to check car registration numbers of those engaged in such dumping.

7.29 The Inquiry Team also inspected the field of vision on the CCTV monitor in Áras an Phobail. The cameras provided full views of private properties and did not use any form of privacy masking in some areas, for example at Kevin Barry Villas, Hawley Park, Mitchell's Avenue towards Mitchell's Road, and the Grotto towards Mitchell's Road. The CCTV cameras also focused on the garden allotment plots at Tobar Naofa.

7.30 Data processed under the LED must comply with the principle of data minimisation. In this regard, Section 71(1)(c) of the 2018 Act requires that '*data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed'.*

[19] The Council's CCTV Policy is available at this link: http://docstore.kerrycoco.ie/KCCWebsite/gdpr/cctvpolicy.pdf

7.31 The concept of what is '*not excessive*'[20] was considered in *Deutsche Post AG v Hauptzollamt Köln*[21]. The Court of Justice of the European Union considered a requirement of the Principal Customs Office in Cologne that applicants for the status of an *authorised economic operator* submit the tax identification numbers of certain persons in charge of the applicant company or its customs matters. The purpose of the numbers was to enable the Office to determine, when responding to an application for AEO status, whether those persons had infringed customs legislation or had a record of serious criminal offences relating to their economic activity over the last three years. The Court acknowledged that the collection of tax identification numbers could enable the customs authorities to have access to personal data that has no connection with the economic activity of the applicant for AEO status. However, the criteria for granting AEO status involved a consideration by the customs authorities of whether those persons had committed such infringements or offences. The Court held that this implies that the customs authorities should have access to data that makes it possible to establish whether the specified infringements or offences have been committed. It held that the collection of tax identification numbers was not excessive to that purpose. This judgment illustrates the breadth of purposes that must be considered for determining what is not excessive.

7.32 It is clear that all purposes for the CCTV systems must be considered when determining whether the data processed is not excessive. The purpose of the CCTV systems at Garvey's Car Park bottle bank facility is to detect and take enforcement action against those engaged in littering. The Council's functions under the Litter Pollution Act 1997 concern not only the prevention of litter, but also the investigation and prosecution of offences under that Act. Therefore, in considering whether the data processed by the Garvey's Car Park bottle bank is excessive, regard must be had to its purpose of identifying offenders and taking enforcement action. Recording CCTV footage in the car park adjacent to the recycling facilities is relevant to investigating and prosecuting littering offences at the facility. There is a high likelihood of motor vehicles being used for illegal dumping. In light of the Council's function of identifying littering offenders, I find that the recording of CCTV footage to check car registration numbers of those engaged in such dumping is not excessive to the Council's purpose of taking enforcement action.

7.33 The purpose of the CCTV systems viewed by the inquiry team at Áras an Phoabil is for securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. Recording private properties is not relevant to this purpose. Where the CCTV focuses on both

[20] The CJEU considered both Article 6(1)(c) of the Data Protection Directive, which provides the standard of '*not excessive*', as well as Article 5(1)(c) of the GDPR, which replaced that standard with the standard of '*limited to what is necessary*' in the GDPR. The LED maintains the standard of '*not excessive*'.

[21] Case C-496/17, Deutsche Post AG v Hauptzollamt Köln, judgment of 16 January 2019 (ECLI:EU:C:2019:26)

private properties and public places, I find that the failure to use any privacy masking makes this processing excessive to its purpose.

7.34 The garden allotment plots at Tobar Naofa is a public place within the meaning of Section 38 of the 2005 Act. Further, the use of CCTV at this location may be relevant to the purpose securing public order and safety under Section 38. However, Section 71(10) obliges the Council to demonstrate, amongst other things, that the data are not excessive in relation to the purposes for which they are processed. I find that the Council has failed to demonstrate that 24 hour recording of the garden allotment plots is not excessive to securing public order and safety at that location.

Findings

7.35 **I find that the Council's recording of the area adjacent to Garvey's Car Park bottle bank facility does not infringe Section 71(1)(c) of the 2018 Act as the wide field of vision of the CCTV systems at Garvey's Car Park is not excessive to its purpose of taking enforcement action against those engaged in littering.**

7.36 **I find that the Council infringed Section 71(1)(c) of the 2018 Act by recording CCTV of private properties, in the absence of any privacy masking, at various locations that feed into the monitoring room at Áras an Phobail.**

7.37 **I find that the Council infringed Section 71(10) by failing to demonstrate that the CCTV at the garden allotment plots at Tobar Naofa is not excessive to its purpose of securing public order and safety.**

D. Lack of written rules or guidelines governing staff access to the CCTV

Inquiry Report Issue 4

7.38 The Environment Section in the Council access CCTV footage at the four recycle bring centres and at a disused vacant lot to prevent and investigate littering offences at these locations. The Council does not have any written rules or guidelines governing the circumstances in which staff members of the Environment Section can review the footage.

7.39 Section 75 of the 2018 Act provides:

> *'(1) A controller shall implement appropriate technical and organisational measures for the purposes of—*
>
> *(a) ensuring that the processing of personal data for which it is responsible is performed in compliance with this Part, and*
>
> *(b) demonstrating such compliance.*
>
> *(2) A controller shall ensure that measures implemented in accordance with subsection (1) are reviewed at regular intervals and, where required, updated.*
>
> *(3) The measures referred to in subsection (1) shall include the implementation of an appropriate data protection policy by the controller, where such implementation is proportionate in relation to the processing activities carried out by the controller.'*

7.40 This requirement extends to implementing appropriate technical and organisational measures to ensure security of the data being processed and to protect against unauthorised or unlawful processing[22]. Section 72(2) of the 2018 Act expressly requires controllers to take steps to ensure that its employees are aware of and comply with those measures.

7.41 Having regard to the harm that might result from members of staff of the Council accessing the CCTV footage in unauthorised or unlawful circumstances, Section 75 of the 2018 Act obliges the Council to implement written rules detailing when staff of the Council can review this CCTV footage. Section 72(2) requires the Council to take steps to ensure that those employees are aware of and comply with those rules.

Findings

7.42 **I find that the Council infringed Sections 75 and 72(2) of the 2018 Act by failing to implement written rules detailing when its staff can review the CCTV footage and by failing to ensure that those employees are aware of and comply with those rules.**

[22] Section 71(f) of the 2018 Act.

E. Use of smartphones or other recording devices in the CCTV monitoring room

Inquiry Report Issues 6 and 12

7.43 The Council has no policy to prohibit the use of personal recording devices to record data from the monitoring screens at the Regeneration Office at Áras an Phobail and [redacted]. Further, there are no signs in the monitoring rooms prohibiting such recording.

7.44 Section 71(1)(f) the 2018 Act obliges the Council to implement appropriate technical or organisational measures to ensure security of data:

> *'(f) the 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—*
>
> *(i) unauthorised or unlawful processing, and*
>
> *(ii) accidental loss, destruction or damage.'*

7.45 Section 78 of the 2018 Act sets out the matters that controllers must have regard to when determining the appropriate technical or organisational measures to implement[23]. Thus, the standard of what is appropriate is scalable, and is dependent on the application of those matters to the particular processing. Regard must also be had to the nature of the burden placed on the controller[24].

7.46 The Council's obligation to implement appropriate technical and organisational measures, in the circumstances, extends to a policy prohibiting the use of personal recording devices to record data from the monitoring screens. There is an express obligation on the Council to implement measures to prevent

[23] Those matters are:
(a) the nature of the personal data concerned;
(b) the accessibility of the data;
(c) the nature, scope, context and purpose of the processing concerned;
(d) any risks to the rights and freedoms of individuals arising from the processing concerned;
(e) the likelihood of any such risks arising and the severity of such risks;
(f) the state of the art and the cost of implementation;
(g) guidelines, recommendations and descriptions of best practice issued by the Commission or the European Data Protection Board.

[24] In *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* Case C-524/06 (ECLI:EU:C:2008:724),the European Court of Justice considered a limitation on the right of access under Article 12(a) of the Data Protection Directive. It considered whether an obligation to keep particular data could represent an excessive burden on a controller. The Court drew an analogy with Article 17 of the Data Protection Directive, which provided for the obligation on controllers to implement appropriate technical and organisational measures. In interpreting that obligation, it noted that account may be taken of the disproportionate nature of measures.

unauthorised copying of the data media[25]. I have had regard to the risks to the rights and freedoms of individuals, and in particular the harm to individuals that could flow from incidents being recorded from the monitoring screens and disseminated amongst the public or media. The CCTV systems process a large quantity of personal data and there is a reasonable risk of unauthorised copying, particularly in the absence of a policy prohibiting same. I have also had regard to the extent of the burden on the controller in implementing such a policy. The policy does not need to ban smartphones from the monitoring rooms entirely, but the recording described in this part must be expressly prohibited.

7.47 Section 72(2) of the 2018 Act expressly requires controllers to take all reasonable steps to ensure that its employees and other persons are aware of and comply with those measures. Such steps should include the placing of signs in the monitoring rooms communicating this prohibition to the Council's employees and other visitors to the rooms.

Findings

7.48 **I find that the Council infringed Section 71(1)(f) of the 2018 Act by failing to implement appropriate organisational measures to prohibit the use of personal recording devices to record data from the CCTV monitoring screens.**

F. Sharing login details resulting in no accurate audit trail

Inquiry Report Issues 7 and 13

7.49 Two employees of the Council have access to the recording hub and monitor at the Regeneration Office at Áras an Phobail. A single generic login was used by both employees to access recordings. [redacted] This resulted in no accurate audit trail of specific user access to the CCTV recordings at either location. The Council implemented measures at both locations to address this issue after the first inspections by the Inquiry Team.

7.50 The Council's obligation to implement appropriate technical and organisational measures to ensure appropriate security of the data includes implementing user specific login details and a system that logs and identifies individual access to CCTV recordings. There is an express obligation on the Council to implement measures to:

[25] Section 77(b)(ii) of the 2018 Act.

'ensure that where a person is authorised to use the automated processing system concerned, he or she has access to personal data on the system only in so far as he or she is so authorised by the controller'[26]

7.51 The possibility of individuals viewing the CCTV for an unauthorised purpose presents a risk to the security of the data. User specific login details and a system that logs individual access protects against this risk by recording when users access the system. Such technical measures are appropriate in light of, inter alia, the quantity of personal data processed by the CCTV, the relative likelihood of unauthorised access in the absence of a user specific log and low burden of implementation.

Findings

7.52 **I find that the Council infringed Section 71(1)(f) of the 2018 Act by failing to implement appropriate technical measures providing for user specific login details that allow for an accurate audit trail for user accesses to the CCTV.**

G. Auditing the audit trails

Inquiry Report Issues 8 and 14

7.53 To the extent that accurate audit trails were produced at Áras an Phobail and [redacted], the Authorised Officers found no evidence of auditing procedures to analyse those trails. The Council did not operate procedures to detect unauthorised access to the systems, and it did not assess the frequency of footage downloads or the systems being accessed.

7.54 The Council's obligation to implement appropriate technical and organisational measures to ensure appropriate security of the data includes implementing regular auditing on the audit trails. Such auditing is essential to detecting any unauthorised accesses and in protecting against the risk identified in Part F.

Findings

7.55 **I find that the Council infringed Section 71(1)(f) of the 2018 Act by failing to implement appropriate organisational and technical measures to ensure regular auditing of the audit trails for the purpose of identifying unauthorised accesses to the CCTV.**

[26] Section 77(b)(vi) of the 2018 Act.

H. Security for transferring CCTV footage to An Garda Síochána

Inquiry Report Issue 10

7.56 On the first inspection at Áras an Phobail, the Authorised Officers established that the Council uses unsecured discs or USB when transferring CCTV footage to An Garda Síochána. On the second inspection date, the Authorised Officers noted that measures had been implemented to address this issue.

7.57 The Council's obligation to implement appropriate technical and organisational measures to ensure appropriate security of the data includes the use of an encrypted transfer mechanism for any necessary transfers to An Garda Síochána. Where the Council is transferring CCTV footage outside of its own internal system, the risk of unauthorised access increases. In considering what appropriate measures must be implemented to protect against this risk, regard must be had to the nature of the personal data that may be contained on CCTV footage relevant to requests from An Garda Síochána. Unauthorised access to such data presents an acute risk to the rights and freedoms of individuals. I have also considered the burden of implementing such encryption.

Findings

7.58 **I find that the Council infringed Section 71(1)(f) of the 2018 Act by failing to implement appropriate organisational and technical measures to ensure that transfers of CCTV footage are protected by encryption.**

I. Record keeping for An Garda Síochána's access to the CCTV footage

Inquiry Report Issue 11

7.59 On the first inspection at Áras an Phobail, the Authorised Officers examined a manual log-book for recording An Garda Síochána's access to the CCTV footage. The book did not record (i) the specific CCTV footage that the Gardaí sought to review or download, or (ii) the purpose for the Gardaí seeking access. On the second inspection date, the Authorised Officers noted that measures had been implemented to address this issue.

7.60 Section 82(1) of the 2018 Act obliges controllers to maintain a data log where it processes personal data by automated means. That log must include, among other things, the disclosure of the personal data, including the transfer of the data, to any other person. Where the log contains such information, pursuant to Section 82(2), it must also contain sufficient information to establish the reason for the disclosure.

7.61 I find that the Council is in breach of its obligations under Section 82(1) by failing to record both (i) the specific CCTV footage that the Gardaí sought to review or download, and (ii) the purpose for the Gardaí seeking access. Compliance with these obligations would not involve a disproportionate effort and would not cause serious difficulties to the Council, and therefore the obligations on the Council are not subject to delay pursuant to Section 82(5).

Findings

7.62 **I find that the Council infringed Section 82 of the 2018 Act by failing to maintain a data log that included (i) the specific CCTV footage that the Gardaí sought to review or download, or (ii) the purpose for the Gardaí seeking access.**

J. CCTV cameras at Mitchel's-Boherbee Community Regeneration Project

Inquiry Report Issue 15

7.63 The Council installed 47 CCTV cameras in January 2007 and December 2008 at Mitchel's-Boherbee Community Regeneration Project. A further 6 CCTV cameras were installed in summer 2018 to cover 15 recently constructed social houses in the area. A Data Protection Impact Assessment (**DPIA**) was completed by the Council on 10 October 2018 for the 6 new cameras. This DPIA was reviewed and revised by the Council on 30 July 2019.

7.64 Section 84(1) of the 2018 Act provides that a DPIA is required where processing *'is likely to result in a high risk to the rights and freedoms of individuals'*. The corresponding requirement for a DPIA under the GDPR gives examples of when a DPIA shall in particular be required, including *'a systematic monitoring of a publicly accessible area on a large scale'*[27]. The CCTV covering the new social houses presents a high risk to the rights and freedoms of the residents and others. I have considered that the 6 new cameras are part of a larger scheme that has been in place for a considerable period of time and were installed to cover 15 new houses in the area. However, the new cameras resulted in a significant increase in the scope of the existing scheme. Therefore, a DPIA was required under Section 84(1) for the 6 new cameras. This DPIA should have been completed prior to carrying out the processing with the new cameras. However, the DPIAs were completed a significant period of time after the processing began in summer 2018.

7.65 Section 84(2) of the 2018 Act sets out what a DPIA must include:

[27] Article 35(3)(c) GDPR

'(2) A data protection impact assessment carried out in accordance with subsection (1) shall include:

(a) a general description of the proposed processing operations to which it relates;

(b) an assessment of the potential risks to the rights and freedoms of data subjects as a result of the proposed processing; and

(c) a description of any safeguards, security measures or mechanisms proposed to be implemented by the controller to mitigate any risk referred to in paragraph (b) and to ensure the protection of the personal data in compliance with this Part.'

7.66 I have reviewed both DPIAs completed by the Council. Based on my review of same, I find that the DPIAs do not contain a sufficient assessment of the potential risks to the rights and freedoms of data subjects. Part 7 of the DPIAs is titled, '*Identify and assess risks*'. However, there is no assessment of the risks associated with recording CCTV in a residential area, including the reasonable expectation of privacy in publicly accessible parts of the area. The DPIAs also fail to describe proposed ways to mitigate such risks.

7.67 Regarding the 47 CCTV cameras installed in 2007 and 2008, a DPIA was not originally required in respect of this processing of personal data because the obligation does not apply to processing that commenced before the 2018 Act was commenced. However, pursuant to Section 71 of the 2018 Act, the Council must ensure that the data it processes is adequate, relevant and not excessive to its purposes, and to ensure that it is in a position to demonstrate same. The Data Protection Working Party has issued guidelines, in respect of the corresponding obligation under the GDPR, stating that *'even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations'*[28].

7.68 I have had regard to the fact that the Council undertook extensive public consultation regarding the CCTV following the preparation of the Tralee RAPID integrated Plan 2006-2009. I have also considered the Council submissions, dated 9th March 2020, in which it submitted that:

[28] Article 29 Data Protection Working Party, *'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679'*, Adopted on 4 April 2017.

'…while a DPIA was not carried out in respect of the scheme at initial development as there was not a legal requirements for a DPIA at that time, the Council is strongly of the view that the level of consultation and assessment carried out meets the requirements of the Act as it would be considered to be of similar process to the DPIA and was indeed an extensive undertaking as part of the overall regeneration programme for the area…'

This Decision accepts that a DPIA was not originally required in respect of the 47 CCTV. However, the obligation on the Council to demonstrate that the data it processes is adequate, relevant and not excessive to its purposes is ongoing and applicable in respect of all of the Council's processing of personal data, regardless of when that processing commenced. The cameras were installed over a decade ago. The scope and nature of this processing of personal data is vast, particularly in circumstances where it covers residential areas. There is an ongoing responsibility on the Council to continually demonstrate that its data processing operations are adequate, relevant and not excessive. Having regard to the vast scope and nature of the CCTV cameras, I find that the Council's failure to conduct a DPIA at any point since the cameras were installed in 2007 and 2008 infringes its accountability obligations under the 2018 Act. In coming to this finding, I have had regard to the extensive consultation process undertaken by the Council following the preparation of the Tralee RAPID integrated Plan 2006 – 2009. However, in light of the ongoing obligation to demonstrate that the processing is adequate, relevant and not excessive, this consultation process, which took place close to a decade ago, is not sufficient. In the absence of a DPIA, the Council failed to demonstrate that the cameras, on an ongoing basis, are still adequate, relevant and not excessive to the purpose of securing public order and safety at those locations.

Findings

7.69 **I find that the Council infringed Section 84(1) of the 2018 Act by installing the six CCTV cameras in summer 2018 without first conducting a DPIA.**

7.70 **I find that the Council infringed Section 84(2) of the 2018 Act by failing to include, in their DPIAs dated October 2018 and July 2019, an assessment of the potential risks to the rights and freedoms of data subjects as a result of the proposed processing. I also find that it further infringed that provision by failing to include a description of any safeguards, security measures or mechanisms proposed to be implemented by the controller to mitigate those risks.**

7.71 **I find that the Council infringed Section 71 of the 2018 Act by failing to demonstrate that the CCTV cameras installed in 2007 and 2008 are adequate, relevant and not excessive to their purposes.**

8. Corrective measures

8.1 Having carefully considered the infringements identified in this Decision, I have decided that it is appropriate to exercise corrective powers in accordance with Section 124(3) of the 2018 Act. I have set out below the corrective powers, pursuant to Section 127(1) of the 2018 Act, which I shall exercise.

1. Pursuant to Section 127(1)(f), I hereby impose a temporary ban on processing by the Council as set out at number 1 in the table below;

2. Pursuant to Section 127(1)(d), I hereby order the Council to bring its processing into compliance with the relevant provisions of the 2018 Act identified in the table below, by taking the relevant action specified in the table; and

3. Pursuant to Section 127(1)(b), I hereby issue a reprimand to the Council in respect of the Council's infringements of the 2018 Act set out in the table below. I issue the said reprimand in light of the number and extent of the infringements identified herein. I consider that the infringements demonstrate a generalised failure by the Council to implement appropriate technical and organisational measures in order to its processing of personal data is in accordance with the 2018 Act.

8.2 In determining the time scale for compliance with the measures specified in the table, I have had regard to the business continuity challenges that the Council may be facing in light of the COVID-19 crisis. As a result, I consider it appropriate to provide for the time scale of 31st August 2020 for most of the measures, as specified in the table. In normal circumstances and were it not for the current pandemic, the timeframe for compliance, as indicated, would have been 2 months.

No.	Finding Number	Action	Time Scale
1	7.16 and 7.17	Section 71(1)(a) of the 2018 Act:	The Council is required to confirm, in writing, to the Data Protection

		I order the Council to temporarily switch off the CCTV cameras at the five locations used for detecting and taking enforcement action against those engaged in littering and the CCTV cameras at Amenity Walk. The processing of personal data through these CCTV cameras may resume only where it is validly based on Union or Member State law. For example, if the Council seeks to rely on Section 38 of An Garda Síochána Act 2005 as a basis for the processing, the CCTV cameras must first comply with the provisions of that Act, including by receiving authorisation from the Garda Commissioner.	Commission [redacted] within 7 days of receiving this Decision that the CCTV cameras at these locations are switched off.
2	7.25	In accordance with the corrective measure specified at Point No. 1 in this table, the CCTV at Garvey's Car Park must be switched off. However, in the event that this processing of personal data lawfully commences again, for example after receiving authorisation from the Garda Commissioner under Section 38, the Council must bring its processing into compliance with Section 93(1) of the 2018 Act by: (i) Referencing 'kerrycoco.ie on the notices on the recycling receptacles, and (ii) Making the more detailed notice available at a height and location that is immediately	Prior to the resumption of processing CCTV footage at Garvey's Car Park.

		apparent and functional to visitors to the car park.	
3	7.36	I order the Council to bring its processing into compliance with Section 71(1)(c) of the 2018 Act by implementing privacy masking to limit the recording of private properties at all locations where such recording occurs, including at Kevin Barry Villas, Hawley Park, Mitchell's Avenue towards Mitchell's Road, and the Grotto towards Mitchell's Road.	Complete task by 31st August 2020.
4	7.37	I order the Council to bring its processing into compliance with Section 71(10) of the 2018 Act by undertaking an appropriate review of the CCTV at the garden allotment plots at Tobar Naofa to assess whether the CCTV is excessive to its purpose and, if not, to demonstrate same. This may be achieved, for example, by conducting a Data Protection Impact Assessment in respect of this processing of personal data.	Complete task by 31st August 2020.
5	7.42	In accordance with the corrective measure specified at Point No. 1 in this table, the CCTV used for detecting and taking enforcement action against those engaged in littering must be switched off. However, in the event that this processing of personal data resumes, for example after receiving authorisation from the Garda Commissioner under Section 38, the Council must bring its processing into compliance with Sections 75 and 75(2) of the 2018 Act by implementing written rules	Prior to the resumption of processing CCTV footage for detecting and taking enforcement action against those engaged in littering.

		detailing when its staff can review the CCTV footage. I further order the Council to ensure that its staff are aware of and comply with those rules.	
6	7.48	I order the Council to bring its processing into compliance with Section 71(1)(f) of the 2018 Act by implementing appropriate organisational measures to prohibit the use of personal recording devices to record data from the CCTV monitoring screens.	Complete task by 31st August 2020.
7	7.52	I order the Council to bring its processing into compliance with Section 71(1)(f) of the 2018 Act by implementing appropriate technical measures for user specific login details that allow for an accurate audit trail for user accesses to the CCTV.	Complete task and submit a short report detailing the action that the Council intends to take to the DPC [redacted] by 31st August 2020.
8	7.55	I order the Council to bring its processing into compliance with Section 71(1)(f) of the 2018 Act by implementing appropriate organisational and technical measures to ensure regular auditing of the audit trails for the purpose of identifying unauthorised accesses to the CCTV.	Complete task and submit a short report detailing the action that the Council intends to take to the DPC [redacted] by 31st August 2020.
9	7.58	I order the Council to bring its processing into compliance with Section 71(1)(f) of the 2018 Act by implementing appropriate organisational and technical measures to ensure that transfers of CCTV footage are protected by encryption.	Complete task and submit a short report detailing the action that the Council intends to take to the DPC [redacted] by 31st August 2020.
10	7.62	I order the Council to bring its processing into compliance with Section 82 of the 2018 Act by maintaining a data log to	Complete task by 31st August 2020.

		include the specific CCTV footage sought by An Garda Síochána and the purpose for same.	
11	7.69, 7.70 and 7.71	I order the Council to bring its processing into compliance with Sections 71 and 84(1) & (2) of the 2018 Act by carrying out a comprehensive Data Protection Impact Assessment in respect of the CCTV systems installed at Mitchel's-Boherbee Community Regeneration Project in January 2007, December 2008, and summer 2018.	Complete task and submit a short report detailing the action that the Council intends to take to the DPC [redacted] by 31st August 2020.

9. Right of appeal

9.1 This Decision is in accordance with Sections 111 and 124 of the 2018 Act. Pursuant to Section 150(5) of the 2018 Act, the Council has the right to appeal against this Decision within 28 days from the date on which notice of this Decision is received by it.

Helen Dixon
Commissioner for Data Protection