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 04/SIU/2018 relating to:

Waterford City and County Council

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: 21st October 2020

Contents

1. Purpose of this Document

1.1 This document is the decision (the **'Decision'**) of the Data Protection Commission (the **'DPC'**) in accordance with Sections 111 and 124 of the Data Protection Act 2018 (the **'2018 Act'**). 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'**). The Authorised Officers who conducted the inquiry provided Waterford City and County Council (the **'Council'**) with the draft Inquiry Report and the final Inquiry Report. The Decision is being provided to the Council pursuant to Sections 116(1)(a) and 126(a) of the 2018 Act in order to give the Council notice of the Decision and the reasons for it, and the corrective powers that I have decided to exercise.

1.2 This Decision contains a list of corrective powers under Sections 115 and 127 of the Data Protection Act 2018 arising from the infringements which have been identified herein by the Decision Maker. 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 The Authorised Officers were authorised on 14 June 2018 to conduct a connected series of own-volition inquiries under Sections 110 and 123 of 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 The inquiry leading to this Decision (the '**inquiry**') 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 on 25 June 2018. The Council responded with the completed questionnaire and a number of attachments.

2.3 The Authorised Officers conducted inspections for the purposes of the next phase of the inquiry. They met with officials from the Council, including the Council's Data Protection Officer, and attended the following locations in February and March of 2019:

i City Hall, Waterford;
ii The IS Server Room in City Hall, Waterford;
iii CCTV cameras at Kilbarry Nature Park;
iv CCTV Recording equipment at Kingfisher Leisure Centre;
v CCTV cameras at Poleberry Walkway; and
vi CCTV camera and monitoring equipment at Williamstown Municipal Golf Course.

2.4 Ultimately the Authorised Officers completed a final Inquiry Report which they submitted to me as Decision-Maker on 24 October 2019. I have considered the Inquiry Report and all relevant correspondence and submissions. The Council was provided with my Draft Decision on 26 March 2020 and was afforded the opportunity to make submissions on the infringements that were provisionally identified therein and the corrective powers that I proposed to exercise. The Council made submissions on 16 April 2020 and I have had regard to those submissions. I have reached final conclusions that infringements of data protection legislation have occurred and that it is necessary to exercise certain corrective powers. Those infringements and corrective powers are set out in this Decision.

2.5 On 2 April 2020, I wrote to the Council regarding the provisional findings in the Draft Decision that were relevant to the functions of An Garda Síochána. I considered it appropriate to invite submissions from an Garda Síochána on those matters and I enclosed an extract from the Draft Decision (containing paragraphs 4.16–4.18, 8.51–8.58, and 8.60–8.63 of the Draft Decision). I asked the Council if it would agree to the DPC providing An Garda Síochána with this extract. The Council replied on 2 April 2020 confirming that the Council had no issue with the extract being shared with An Garda Síochána. I wrote to An Garda Síochána on 2 April 2020 inviting submissions on the matters contained in the extract. On 25 June 2020, An Garda Síochána wrote to the DPC stating that it concurred with the provisional findings in the extract, save in relation to how certain powers had been transferred to the Policing Authority[1], and stating that An Garda Síochána will work with Local Authorities regarding the joint controller relationship.

2.6 The findings made in this Decision include, amongst other things, findings concerning CCTV systems authorised by the Garda Commissioner under

[1] Section 31 of Garda Síochána (Policing Authority and Miscellaneous Provisions) Act 2015.

Section 38 of the Garda Síochána Act 2005 ('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. Topics arising in this Decision

3.1 This Decision considers the processing of personal data through a broad range of technologies, including CCTV systems, body worn cameras, drones, dash cams, and covert cameras. The contexts of the processing operations are equally diverse. The body worn cameras are used for personal safety and to assist in the resolution of complaints. The purposes for the other technologies include preventing, detecting and prosecuting littering offences; public safety; crime prevention and investigation; and preventing anti-social behaviour.

3.2 As a result of the different purposes for processing, two overarching legal regimes must be applied in this Decision. The General Data Protection Regulation (the '**GDPR**') is applicable to the body worn cameras and the Law Enforcement Directive (the '**LED**') is applicable to the other technologies under consideration. Furthermore, in determining the lawful basis for the various processing operations, this Decision must consider a broad range of legislation. The following legislation is considered in this regard: the Litter Pollution Act 1997; the Waste Management Act 1996; the Water Pollution Act 1977; An Garda Síochána Act 2005; Local Authorities (Traffic Wardens) Act 1975; and the Safety, Health and Welfare at Work Act 2005.

3.3 The data protection matters considered in this Decision are also diverse. However, they can be divided into three thematic issues:

(i) The lawful bases for the processing;
(ii) Transparency (including privacy policies and CCTV policies); and
(iii) Accountability and technical and organisational measures.

3.4 As outlined below, this Decision finds that there is no lawful basis for some of the Council's processing of personal data as identified in the inquiry. Notwithstanding the unlawfulness of such processing, for completeness, this Decision proceeds to consider all issues identified by the inquiry regarding transparency and accountability and technical and organisational measures, even in respect of processing that has been found to be unlawful.

4. Legal regimes pertaining to the inquiry and the Decision

4.1 Some of the processing of personal data by the Council detailed in this Decision falls to be regulated under the GDPR and some falls under the LED.

4.2 The 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'*

4.3 The 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:

> *'This Part applies, subject to subsection (2), 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.'*

4.4 Therefore, the LED will apply to automated processing if the following two steps are fulfilled:

i. The processing is carried out by or on behalf of a '*controller*', as defined in Section 69 of the Act.
ii. The processing is 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.

(i) Controller

4.5 Regarding the first limb of this test, there are two distinct routes to fulfilling the definition of 'controller', defined in Section 69 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;'*

4.6 Part (a) of the definition of controller applies only to competent authorities. '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…'*

This definition of 'Competent authority' is broad. The use of the word '*or*' is disjunctive, meaning that competence for any one or more of preventing, investigating, detecting or prosecuting criminal offences is sufficient to bring public authorities within the definition of '*Competent authority*'. It is well-established in statutory interpretation *'that generally it is assumed that "or" is intended to be used disjunctively and the word "and" conjunctively'*[2]. There is no basis for departing from the ordinary meaning of the word 'or' and it cannot have

[2] Per Lord Salmon, Federal Steam Navigation Co. Ltd. v Department of Trade and Industry, [1974] 1 WLR, at page 524.

been the intention of the Oireachtas to bring about a conjunctive interpretation. The definition of 'Competent authority' is not context specific. However, in order to constitute a 'controller' under part (a) of the definition, a competent authority must also determine the purposes and means of the processing, alone or jointly.

4.7 Part (b) of the definition of 'controller' details how, in alternative to the part (a) route, controllers can be nominated by, or in accordance with criteria specified in EU or national law. There is no requirement under part (b) that the entity or individual is a competent authority. However, the means and purposes of the processing must be determined by EU or national law.

(ii) Purpose of the Processing

4.8 The second limb of the test requires that the processing is 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.

4.9 To satisfy this limb of the test, the primary purposes of the processing must reflect those law enforcement purposes. One must look to the specific reasons for the processing. It is not sufficient that the data being processed could in theory also be used for law enforcement purposes on a secondary basis. The specific reasons for the processing must reflect those law enforcement purposes.

4.10 In *Puskar v Finance Directorate of the Slovak Republic*[3] the Court of Justice of the European Union (**'CJEU**') considered the scope of the Data Protection Directive[4], specifically the directive's non-application to processing operations concerning the activities of the State in areas of criminal law[5]. This case considered the inclusion of an individual's name on a list of persons that the Finance Directorate considered 'front-men' in company director roles. The data at issue were processed for the purpose of collecting tax and combating tax fraud. However, that data could be used in criminal proceedings if infringements were identified. The Court considered the purposes of the processing and held that the data were not collected '*for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law*'[6]. On that basis, the criminal law exclusion was not applicable, and the Data Protection Directive was held to apply to that processing

[3] Case C-73/16, Peter Puskar v Finance Directorate of the Slovak Republic, judgment of 27 September 2017 (ECLI:EU:C:2017:725).

[4] Directive 95/45/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] That exclusion is provided for in Article 3(2) of the Directive.

[6] At paragraph 40.

4.11 In this case the CJEU adopted a strict interpretation of the scope of the criminal law exclusion in the Data Protection Directive. For that exclusion to apply, it is not sufficient that the data could potentially be used in criminal proceedings. Rather, the data must have been collected for the specific purpose of the pursuit of criminal proceedings. A similarly strict interpretation of the application of the LED and Section 70 of the 2018 Act is warranted. Thus, processing is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences only if the controller's reasons for the processing specifically reflects one or more of those purposes. It is not sufficient that the data could potentially also be used for law enforcement purposes if those purposes did not form part of the controller's specific reasons for processing.

Processing that falls under the GDPR

4.12 The GDPR is applicable to the Council's processing of personal data by means of body worn cameras. This processing is for the purposes of protecting the personal safety of traffic wardens and to assist in the resolution of complaints. The recordings are not used for the resolution or investigation of traffic offences. The Council's policy on the use of body worn cameras states that the personal safety of the traffic wardens is enhanced as '*once a member of the public is informed that an exchange is being recorded it is far less likely that they will attempt to physically harm a traffic warden*'[7]. Although the data processed through the body worn cameras has the potential for subsequent use in criminal investigations and prosecutions[8], this does not form part of the purposes for this processing. Therefore, this processing is not for the specific purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties. The second limb of the test for the LED to apply is not satisfied and the GDPR is applicable.

Processing that falls under the LED

4.13 Aside from the processing by means of body worn cameras, this Decision finds that the remainder of the processing of personal data identified in the Inquiry Report falls under the LED. The final Inquiry Report took the view that the GDPR is applicable to the CCTV systems at Poleberry Walkway, at Williamstown Municipal Golf Course, and the CCTV that the Council operates pursuant to Section 38 of An Garda Síochána Act 2005. However, this Decision finds that the GDPR is in fact not applicable to the processing of personal data through those systems. Instead, the LED, incorporated through Part 5 of the 2018 Act, is applicable. The analysis in respect of this finding is as follows.

[7] At paragraph 3.5.

[8] This is expressly acknowledged in the Council's policy at paragraph 3.4.

4.14 Regarding the Council's use of dash cams, drones, and covert surveillance, the Council is a '*controller*' within part (a) of that definition. The Council is a competent authority because it enjoys competence for the prevention, investigation, detection, and prosecution of certain offences under the Litter Pollution Act 1997 and the Waste Management Act 1996. Furthermore, it enjoys a general competence regarding the prevention of crime, when performing its functions, under Section 37(1) of An Garda Síochána Act 2005[9]. It determines the purposes and means of the processing carried out by means of dash cams, drones, and covert surveillance.

4.15 The purposes of the processing through dash cams, drones, and covert surveillance bring that processing under the LED. The dash cams are used to detect and prosecute littering offences. The drones are used to monitor compliance in permitted waste sites, to prevent dumping on illegal waste sites, and to demonstrate waste for prosecution purposes. The covert cameras are used to detect illegal littering and dumping. Thus, each piece of technology is used with the specific purpose of preventing, investigating, detecting and/or prosecuting criminal offences.

4.16 The CCTV systems operated by the Council pursuant to Section 38 of An Garda Síochána Act 2005 also fall under the LED. The Council is a 'Controller' within part (b) of that definition. The purposes and means of the processing are determined by Section 38 of An Garda Síochána Act and the delegated legislation made pursuant to it. Section 38(1) 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[10] and the systems that can be used[11].

4.17 The Council is nominated as controller of this processing by Article 4(d) of the Garda Síochána (CCTV) Order 2006[12], which 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.

[9] 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.'

[10] 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.

[11] 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.

[12] S.I. No. 289/2006 – Garda Síochána (CCTV) Order, 2006.

4.18 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'*. The second step in the test for applying the LED requires the processing to be 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[13] 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.

4.19 The CCTV systems operated by the Council at Poleberry Walkway and at Williamstown Municipal Golf Course, which have not been authorised under An Garda Síochána Act 2005, also fall under the LED. The Council is a controller of this personal data within part (a) of that definition in Section 69. As we have seen, the Council is a competent authority. It determines the purposes and means of the processing at Poleberry Walkway and at Williamstown Municipal Golf Course. It decided to install those CCTV systems for public safety/crime prevention and investigation and the prevention of crime and anti-social behaviour respectively. 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. Thus, the Council is a controller within the meaning of Section 69.

4.20 The purpose of the processing at Poleberry Walkway and at Williamstown Municipal Golf Course brings that processing under the LED. The CCTV at both locations are used for preventing criminal offences. The result is that the LED, incorporated through Part 5 of the 2018 Act, is applicable to these CCTV systems.

4.21 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.

[13] 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.

5. Materials considered

5.1 The Authorised Officers delivered the Inquiry Report to me on 24th 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 completed Data Protection Audit Questionnaire;
ii The Council's draft CCTV policy;
iii CCTV Inventory from February 2019;
iv Letter from [redacted] the Council, dated 26 September 2019;
v Garda Commissioner Authorisation dated 7 December 2006;
vi Garda Commissioner Authorisation dated 9 January 2008;
vii The Council's Traffic Warden Risk Assessment for Body Worn Cameras;
viii The Council's Draft Data Protection Impact Assessment for Body Worn Cameras;
ix The Council's Draft Policy on use of Body Worn Cameras;
x The Council's final Data Protection Impact Assessment for Body Worn Cameras;
xi The Council's Final Policy on use of Body Worn Cameras;
xii The Council's Data Protection Impact Assessment for Dash Cams;
xiii The Council's Policy on use of Dash Cams;
xiv The Council's Data Protection Impact Assessment for Drones – Environment;
xv The Council's Draft Policy on Drones – Environment;
xvi The Council's Final Policy for Drones – Environment;
xvii The Council's Final Policy for Drones – Water;
xviii The Council's Data Protection Impact Assessment for Drones – Water;
xix The Council's Draft Policy on Trail Cameras;
xx The Council's Data Protection Impact Assessment for Trail Cameras;
xxi The Council's Final Policy on Trail Cameras;
xxii Email from [redacted] the Council, to the Special Investigations Unit dated 22 October 2019;
xxiii Images of the Council's CCTV signage;
xxiv Email from [redacted] the Council, to me dated 8 November 2019;
xxv Data Processor Agreement between the Council and [redacted], dated 3 September 2018;
xxvi Email from [redacted] the Council, to me dated 16th April 2020;
xxvii Letter from [redacted] the Council, to me dated 16th April 2020;

xxviii Document titled, *'Corrective Actions + WCCC Response'*, submitted to the DPC on 16th April 2020;

xxix The Council's Policy Sheet for the use of Dash cams – Litter Enforcement, dated September 2019; and

xxx A screenshot of the Council's website and Privacy Statement, submitted to the DPC on 16th April 2020.

5.2 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.

6. Data controller

6.1 This Decision and the corrective measures that are identified herein are addressed to the Council as a data controller in relation to the findings made.

7. Personal Data

7.1 '*Personal data*' is defined under the GDPR as *'any information relating to an identified or identifiable natural person'*[14]. Section 69 of the 2018 Act implements a similar definition of '*Personal data*' under the LED[15].

7.2 This Decision concerns CCTV systems, body worn cameras, dash cams, drones, and covert cameras. All of these devices capture visual images of individuals. It is possible to identify individuals from such images. Thus, the data processed by the devices includes '*personal data'*.

8. Analysis and findings

8.1 The Authorised Officers identified a total of 12 issues in the course of the 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.

[14] Article 4 GDPR.

[15] 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;'

8.2 Since the inquiry commenced, the Council has taken steps to address some of the issues identified in the inquiry. This Decision makes 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 issues leading to the findings in this Decision may since have been addressed by the Council.

A. Body Worn Cameras: Lawful Basis & Accountability

Regime: GDPR
Inquiry Report Issue: 1 and 2

8.3 The Council's traffic wardens wear body worn cameras for personal safety and to assist in the resolution of complaints. The cameras are switched off by default and only record where they are switched on by a traffic warden. The Council's policy is that the wardens should use their own judgement and activate the camera where they feel it is needed, but that the camera should not be used where no threat or difficulty exists. The Council informed the Authorised Officers that it relies on Articles 6(1)(d) and 6(1)(e) of the GDPR as the lawful bases for this processing.

8.4 Article 6(1) of the GDPR provides:

> *'Processing shall be lawful only if and to the extent that at least one of the following applies:*
> *…*
> *(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
> *(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
> *…'*

8.5 The 'vital interests' basis in Article 6(1)(d) applies where the processing is necessary to protect an interest that is essential for the life of a person. Recital 46 of the GDPR provides:

> *'The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be*

manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.'

8.6 The 'vital interests' basis should generally only be relied upon where the processing cannot be based on another legal basis. The document titled *'Data Protection Impact Assessment on the use of Body Worn Cameras by Traffic Wardens'*, conducted by the Council in September 2019, at Step 4, relies on the Safety, Health and Welfare at Work Act 2005 only as a lawful basis. In circumstances where the Council is relying on Article 6(1)(e), it is appropriate to first consider whether the processing can be based on that provision.

8.7 To rely on Article 6(1)(e), the processing must be necessary for the performance of a task vested in the Council. That task must be carried out in the public interest or in the exercise of official authority. Furthermore, pursuant to Article 6(3), the basis for the processing must be laid down by Union or Member State law. The Council relies on the Safety, Health and Welfare at Work Act 2005 as a lawful basis for the processing. This Act places a duty on employers to ensure the safety, health and welfare of employees. The Council's general obligations to its employees are not tasks carried out in the public interest or in the exercise of official authority. However, the Local Authorities (Traffic Wardens) Act 1975 empowers the Council to make arrangements for its employees to perform the functions of traffic wardens[16]. Thus, it vests in the Council a task that is carried out in the exercise of official authority. There is no requirement for the basis for the processing to be set out in one single legislative measure. Furthermore, the European Data Protection Board's guidelines on processing of personal data through video devices recognises that where the exercise of official authority does not allow for certain processing, *"other legislative bases such as 'health and safety' for the protection of visitors and employees may provide limited scope for processing, while still having regard for GDPR obligations and data subject rights"*[17]. Therefore both the task vested by the Local Authorities (Traffic Wardens) Act 1975, and the duty on the Council to its employees pursuant to the Welfare at Work Act 2005, considered together, are relevant to considering whether the Council has a lawful basis for its use of Body Worn Cameras under Article (6)(1)(e).

[16] This power is provided for at Section 2.

[17] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", Version 2.0, Adopted on 29 January 2020, at page 13.

8.8 In order to rely on legislative measures as a basis for processing personal data, those measures must be clear and precise and their application must be foreseeable to persons subject to them in accordance with the case law of the Court of Justice of the European Union and the European Court of Human Rights. This requirement is restated in Recital 41 of the GDPR:

> *'a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.'*

8.9 This is consistent with the requirement in Article 52(1) of the Charter of Fundamental Rights of the European Union that limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law. In *Schrems v Data Protection Commissioner*[18] the CJEU held that EU legislation interfering with the fundamental rights guaranteed by Articles 7 or 8 of the Charter of Fundamental Rights of the European Union must lay down clear and precise rules governing the scope of the measure:

> *'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.'*[19]

8.10 This requires that the legal basis permitting an interference with those fundamental rights must itself define the scope of the limitation on the exercise of the right concerned. The legal basis must indicate the circumstances in which a measure providing for the processing of personal data may be implemented. Furthermore, in accordance with Article 52(3) of the Charter, account must be taken of the right to respect for private and family life pursuant to Article 8 of the European Convention on Human Rights. In *Fernández Martínez v Spain*[20] the European Court of Human Rights held, in relation to what is required of domestic law interfering with the right in Article 8 of the ECHR, that:

> *'The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law. Secondly,*

[18] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, judgment of 6 October 2015(ECLI:EU:C:2015:650).
[19] At paragraph 91.
[20] [2014] ECHR 615

it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law (see, among other authorities, Kopp v. Switzerland, 25 March 1998, § 55, Reports of Judgments and Decisions 1998-II). The phrase thus implies, inter alia, that domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are entitled to resort to measures affecting their rights under the Convention (see C.G. and Others v. Bulgaria, no. 1365/07, § 39, 24 April 2008).'[21]

8.11 In order to meet the standards of clarity, precision, and foreseeability, the legislation must afford adequate legal protection against arbitrariness and bring clarity to the scope of any discretion conferred on public authorities by that legislation. There must also be sufficient safeguards to ensure that the data subjects' rights are protected. The legislation must allow data subjects to foresee to a reasonable degree, with the assistance of legal advice where necessary[22], the consequences of the law and how the processing of personal data may apply to them. This does not require the law to codify every possible instance of processing of personal data, however, it must set out principles that are capable of being predictably applied to any situation.

8.12 I am satisfied that the Local Authorities (Traffic Wardens) Act 1975 and the Welfare at Work Act 2005, when read together, meet the standards of clarity, precision and foreseeability and sufficiently regulate the Council's processing of personal data by means of Body Worn Cameras. The Acts are sufficiently clear on the scope of the discretion conferred on the Council in respect of its use of body worn cameras. I am satisfied that they permit such processing only in so far as the processing is necessary to ensure the health, safety and welfare of Traffic Wardens. Therefore, the Acts do no permit general and indiscriminate processing, but allow processing through body worn cameras only where a specific threat to health, safety, or welfare arises. In this regard, it is sufficiently clear that the body worn cameras can only be switched on where a specific issue arises. This restriction is reflected in the Council's practice of having the cameras switched off by default and activated only where a threat or difficulty exists. The limited circumstances and conditions under which this processing of personal data may occur are sufficiently foreseeable from the Acts. Therefore, the scope on the limitation on the fundamental rights provided for in Articles 7 and 8 of the Charter is sufficiently defined in the Acts.

[21] At paragraph 117.

[22] See for example Slivenko v Latvia [2003] ECHR 498.

8.13 It is clear that the safety, health and welfare of traffic wardens is relevant to determining the necessity of the Body Worn Cameras under Article 6(1)(e). The necessity test requires a balancing of the personal data being processed against the aims that the processing seeks to achieve. If there is a less intrusive means to achieve those aims, the processing will fail the test. In *Huber v. Bundesrepublik Deutschland*[23] the Court applied the necessity test to a centralised register for foreign nationals resident in Germany. The register assisted national authorities in ascertaining whether an individual had a right of residence. The Court considered the necessity of the centralisation of the data in circumstances where decentralised registers already contained all of the relevant data. It held that the centralisation of that data could be necessary if it contributed to a more effective application of the right of residence. Thus, to satisfy the necessity test, the processing does not have to be absolutely essential to achieving its purpose. If it contributes to the effectiveness of the performance of the task, that may be sufficient to render it '*necessary*'.

8.14 The body worn cameras could contribute to the effectiveness of the performance of Traffic Wardens' functions. The Council claims that the body worn cameras work as an effective deterrent against incidents of violence and aggression towards wardens. If that is the case, the processing of data through the cameras could assist the Council in performing their functions under the Local Authorities (Traffic Wardens) Act, 1975. By contributing to the safety of traffic wardens, the cameras could make the Council more effective in performing their functions under the Act, despite the fact that the cameras are not absolutely necessary for any of those functions. Such effectiveness alone may be sufficient to render the processing '*necessary*' within the meaning of Article 6(1)(e).

8.15 The obligation rests on the Council to demonstrate such necessity. Article 5(2) of the GDPR provides for the principle of accountability. It places an obligation on controllers to demonstrate compliance with, amongst other things, the requirement that data be processed lawfully. To demonstrate lawfulness, the Council must demonstrate that the processing through body worn cameras is necessary pursuant to Article 6(1)(e).

8.16 Article 35(1) of the GDPR provides that a controller must carry out a Data Protection Impact Assessment ('**DPIA**') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. However, this obligation does not apply to processing that commenced before the GDPR came into force, save for certain exceptions. The Council's use of body worn cameras commenced in 2016, and thus, a DPIA was not required at that time. Nonetheless, the Data Protection Working Party has issued guidelines stating that *'even if a DPIA is not required on 25 May 2018, it will be necessary, at the*

[23] Case C-524/06, Huber v. Bundesrepublik Deutschland, judgment of 16 December 2018 (ECLI:EU:C:2008:724).

appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations'[24].

8.17 The Council has failed to demonstrate the necessity of the body worn cameras. It submitted a DPIA from March 2018, a DPIA from September 2019, a Traffic Warden Risk Assessment, and the Policy on use of Body Worn Cameras. None of these documents demonstrate that the body worn cameras are necessary for a task vested in the Council. The DPIA from September 2019, at Step 1, applies a test of necessity, detailing the problem to be addressed and how the cameras address the issue. However, it does not identify a task that is vested in the Council and, therefore, the DPIA does not demonstrate that the processing is necessary for the performance of such a task. Furthermore, the part titled, '*Why existing or less intrusive measures cannot sufficiently address the matter*', does not consider any alternative less intrusive measures. It is not clear whether any alternative measures have been considered by the Council, and, if so, why they have been discounted.

8.18 As noted above, the vital interests basis in Article 6(1)(d) should in principle only be relied upon where the processing cannot be manifestly based on another legal basis. In circumstances where the Council is relying on Article 6(1)(e), it is not appropriate for the Council to simultaneously rely on Article 6(1)(d) as a basis for the processing. Nonetheless, the Council has failed to demonstrate that the processing is necessary to protect the vital interests of the traffic wardens. The DPIA from September 2019 focuses on a legislative basis for the processing, and no consideration is given to the high bar of '*vital interests*'. The failure to consider less intrusive measures also results in a failure to demonstrate the necessity of the processing to protect the vital interests of the traffic wardens.

Findings

8.19 I find that the Council infringed Article 5(2) of the GDPR by failing to demonstrate that the processing of personal data through body worn cameras is lawful, specifically that it is necessary for either of the lawful bases that the Council relies on in Articles 6(1)(d) and 6(1)(e).

B. Lawful Basis: Dash Cams, Drones and Covert Cameras

Regime: Law Enforcement Directive
Inquiry Report Issue: 3, 4 and 5

[24] 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.

8.20 The Council has used dash cams to detect and prosecute littering offences since June 2017. Its vehicles are equipped with cameras that start recording as soon as the engines start. The recordings are automatically overwritten unless an inspector presses the save button on the dash cam. The cameras are placed on the front of the vehicles' windscreens and capture a wide view of the area in front. The Council relies on the Litter Pollution Act 1997 and the Waste Management Act 1996 as a lawful basis for this processing.

8.21 The Council has used drones since summer 2017 to monitor compliance on permitted waste sites and to prevent dumping on illegal waste sites. The drones take aerial photos and videos of the sites. The images allow the scale and type of waste to be clearly demonstrated in prosecutions. The Council relies on the Waste Management Act 1996 and the Water Pollution Act 1977 as a lawful basis for this processing.

8.22 The Council uses 8 covert motion-activated cameras to detect illegal littering and dumping. The cameras are hidden in gateways, on trees, and in unmarked cars. The Council relies on the Litter Pollution Act 1997 as a lawful basis for this processing.

8.23 As outlined in Part 4 of this Decision, the Council's use of dash cams, drones and covert cameras fall under the Law Enforcement Directive, as transposed by Part 5 of the 2018 Act. The Council has functions concerning the prevention, investigation, detection and prosecution of litter and waste related criminal offences pursuant to the Litter Pollution Act 1997, the Waste Management Act 1996 and the Water Pollution Act 1977. Where processing falls under the LED, and where processing is not based on consent, any processing must be based on Union or Member State law. Where Member State law is being relied on as a basis for processing, the law must meet the requirements of clarity, precision and foreseeability as set out in Part 8A of this Decision. Furthermore, the Member State law must also regulate the processing in accordance with Article 8(2) of the LED by specifying the objectives of processing, the personal data to be processed and the purposes of the processing. It is in this context that the Council's use of dash cams, drones and covert cameras falls to be assessed.

8.24 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.'

8.25 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*[25], the Supreme Court interpreted the Irish legislation[26] that implemented Directive 2003/4/EC[27]. 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."*[28]

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 to adopt another interpretation which is consistent with the provisions of the Directive, if that is possible."*[29]

8.26 In *Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission*[30], 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'*[31]. 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.

[25] National Asset Management Agency -v- Commissioner for Environmental Information [2015] IESC 51.
[26] Statutory Instrument No. 133 of 2007.
[27] 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.
[28] Ibid At paragraph 10.
[29] Ibid at paragraph 11.
[30] 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).
[31] At paragraph 39.

8.27 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.'*

8.28 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.

8.29 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.

8.30 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.'

8.31 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 that is to be processed. Such an Act would be sufficient once the objectives, the personal data to be processed and the purposes are provided for in the Act. However, as outlined above, the Member State law must also meet the requirements of clarity, precision, and foreseeability by providing clarity to the scope of any discretion conferred.

8.32 The Council's use of dash cams cannot lawfully be based on the Litter Pollution Act 1997 and the Waste Management Act 1996. These Acts do not regulate this type of processing as 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 dash cams in this manner. There are no provisions in either of the three Acts that can be said to govern such general and indiscriminate processing of images of members of the public by means of dash cams with the aim of catching littering offences on camera. Although the Council's prosecutorial functions implicitly provide for the processing of certain personal data, the vast scope of processing through dash cams is not implicitly provided for in the Acts. Furthermore, neither of the Acts set out provisions that govern the scope or application, or impose minimum safeguards, on the use of dash cams, as required by the case law of the Court of Justice of the European Union. Therefore, this processing of personal data is not validly based on Member State law.

8.33 Regarding the Council's processing of personal data by means of drones, The Waste Management Act 1996 specifies the matters required by Article 8(2) of the LED. Section 14(4)(a)[32] permits authorised persons to *'take such photographs, record such information on data loggers, make such tape, electrical, video or other recordings…'* after entering a premises pursuant to that Section. Where individuals are present on the premises and recorded, this will constitute the processing of personal data. This processing of personal data is implicitly provided for by virtue of the power to make such recordings. The objectives and

[32] As amended by Section 24 of the Protection of the Environment Act 2003.

purposes of the processing are specified in the Act, and include the prevention, management and control of waste. Section 14 also regulates the processing by specifying when such premises can be entered by an authorised person and the criteria that must be fulfilled before entering. The Waste Management Act 1996 meets the requirements of clarity, precision and foreseeability. Therefore, the Council's processing of personal data by means of drones may be validly based on the Waste Management Act 1996.

8.34 Regarding the Council's processing of personal date by means of covert cameras, The Litter Pollution Act 1997, as relied upon by the Council, does not regulate this type of processing as required by Article 8(2) of the LED. We have seen above how this Act provides the Council with certain broad functions. However, the Act does not provide for the Council's processing of images of members of the public. There are no provisions in the Act that can be said to govern such a wide scope of processing. Even if the Act did specify for this personal data to be processed, in the absence of significant other amendments, the Act would be severely lacking in rules that govern the scope and application of such covert cameras, including, among others, the criteria that must be fulfilled before installing such covert cameras, the supervision of such covert cameras once installed, and the termination of the covert cameras. Furthermore, the Act does not meet the requirements of clarity, precision, and foreseeability by providing clarity to the scope of any discretion conferred.

Findings

8.35 I find that the Council's processing of personal data by means of dash cams and covert cameras infringed Sections 71(1)(a) and 71(2) of the 2018 Act because there is no lawful basis for such processing of personal data in European Union law or the law of the State.

C. Lawful Basis: CCTV Cameras at Poleberry Walkway

Regime: Law Enforcement Directive
Inquiry Report Issue: 8

8.36 The Council operates 22 CCTV cameras at the Poleberry Walkway for the purposes of '*public safety/crime prevention and investigation'*. These CCTV systems do not have authorisation under Section 38 of the Garda Síochána Act 2005.

8.37 For processing under the LED to be lawful, the processing must be necessary for the performance of a task of a competent authority and 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.

8.38 The Council has not identified any provision of Union or Member State law that provides a basis for its processing of personal data by means of CCTV in this manner. Section 38 of An Garda Síochána Act 2005 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 22 locations. However, such CCTV systems must, amongst other things, be authorised by the Garda Commissioner. In the absence of such authorisation, the Council's use of CCTV systems at these locations is unlawful.

Findings

8.39 I find that the Council infringed Sections 71(1)(a) and 71(2) of the 2018 Act by unlawfully processing personal data through CCTV cameras at Poleberry Walkway without a lawful basis for such processing in European Union law or the law of the State.

D. Lawful Basis: CCTV Camera at Williamstown Municipal Golf Course

Regime: Law Enforcement Directive
Inquiry Report Issue: 10

8.40 The Council operates a CCTV camera inside the boundary of Williamstown Municipal Golf Course that monitors a nearby halting site. The camera does not focus into the site, but it does capture movement at the entrance to the cul-de-sac leading to the site. The Council's stated purpose for the camera is the prevention of crime and anti-social behaviour. The CCTV camera has not been authorised under Section 38 of An Garda Siochána Act 2005.

8.41 Section 69 of the 2018 Act defines special categories of personal data as including '*personal data revealing the racial or ethnic origin of the data subject*'. Irish Travellers are an ethnic group. Monitoring the entrance to cul-de-sac leading to the halting site, over a period of time, would tend to distinguish the residents of the site from other visitors to it. By identifying the residents of the halting site, it is possible to identify their ethnic origin. Therefore, this Decision finds that the CCTV camera at Williamstown Municipal Golf Course processes special category personal data.

8.42 Section 73 of the 2018 Act provides that the processing of special category personal data shall be lawful only where Section 71 is complied with and one of the 9 conditions in Section 73(1)(b) is met. This Decision finds that the Council's CCTV camera is unlawful in the absence of a basis for the processing in Union or Member State law. Even if this camera had a basis in Union or Member State law, for example, if it was authorised under Section 38 of An Garda Siochána Act 2005, that processing would still have to pass a necessity test for securing public order and safety by facilitating the deterrence, prevention, detection and prosecution of offences.

8.43 The necessity test requires a balancing of the personal data being processed against the aims that the processing seeks to achieve. This Decision finds that the camera processes special category personal data. The processing of special category data weighs heavily against the aims of any such processing. Furthermore, even with Section 38 authorisation, the Council would be obliged to identify a condition in Section 73(1)(b) before carrying out such processing.

Findings

8.44 I find that the Council infringed Sections 71(1)(a), 71(2) and 73 of the 2018 Act by unlawfully processing personal data through the CCTV camera at Williamstown Municipal Golf Course without a lawful basis for such processing in European Union law or the law of the State.

E. Use of drones: Demonstrating Lawfulness

Regime: Law Enforcement Directive
Inquiry Report Issue: 4

8.45 In circumstances where the Council is relying on the Waste Management Act 1996 as a lawful basis for its use of drones, Section 71(10) of the 2018 Act obliges it to ensure that it can demonstrate that the processing is, among other things, lawful. In order for this processing to be lawful, it must be necessary for the performance of the Council's functions of preventing, investigating, detecting and prosecuting waste related criminal offences[33]. This requires a balancing of the personal data being processed against the aims that the processing seeks to achieve. If there is a less intrusive means to achieve those aims, the processing will fail the test. The obligation rests on the Council to demonstrate that the use of drones is capable of achieving those aims and that no less intrusive means exists. A DPIA is a useful tool in demonstrating this.

[33] Section 71(2)(a) of the 2018 Act.

8.46 I welcome that the Council finalised a DPIA in respect of this processing in September 2019. However, this DPIA had not been completed when the inquiry leading to this Decision began. This alone is not an infringement of the Council's obligations under the 2018 Act because the requirement to carry out a DPIA did not exist when that processing began. However, the obligation under, Section 71(10) of the 2018 Act, to demonstrate that processing of personal data is in compliance with Section 71(2) of that Act, applied from the commencement of the 2018 Act on 25 May 2018[34]. I find that the Council failed to demonstrate that the use of drones was capable of achieving its aims and that no less intrusive means existed between 25 May 2018 and the date on which the DPIA was finalised in September 2019.

Findings

8.47 I find that the Council infringed Section 71(10) of the 2018 Act by failing to ensure that it was in a position to demonstrate that it's processing of personal data by means of drones was lawful from 25 May 2018 until the DPIA was adopted in September 2019, insofar as the Council did not demonstrate that the use of drones is capable of achieving its aims and that no less intrusive means exist.

F. Use of Drones: Appropriate Technical and Organisation Measures in the Final Policy

Regime: Law Enforcement Directive
Inquiry Report Issue: 4

8.48 The Council adopted a final policy regarding the use of drones in September 2019. This policy does not make provision for the requirements of Section 14 of the Waste Management Act 1996, which details the circumstances in which the Council can take photographs, videos and other recordings.

8.49 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.*

[34] S.I. No. 174/2018, Data Protection Act (Commencement) Order 2018.

(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.'

8.50 The requirement to implement appropriate technical and organisational measures includes measures to protect against unauthorised or unlawful processing[35]. The Council relies on the Waste Management Act 1996 as a lawful basis for its use of drones, thus, its processing must comply with the provisions of that Act. A failure to comply, in particular, with Section 14 of the Waste Management Act 1996 would render the processing unlawful.

8.51 The Council has failed to communicate the statutory pre-requisites for making recordings under the Act in the Policy. For example, Section 14(4)(a) permits recordings by authorised persons only. The policy does not specify that the drones should be operated only by individuals who are authorised persons within the meaning of the Act. Further, Section 14(4)(a) allows such recording only where premises have been entered or vehicles boarded pursuant to Section 14. The policy does not implement the requirements that Section 14 imposes for entering a premises, including that the authorised person has reasonable grounds for believing that there may be a risk of environmental pollution. The final policy on the use of drones should communicate these pre-requisites to the Council's staff to protect against the risk of the drones being used in contravention of the Act. In the absence of such provisions in the policy, there is a heightened risk of unlawful and unauthorised processing.

Findings

8.52 I find that the Council infringed Section 75 of the 2018 Act by failing to communicate the statutory pre-requisites of the Waste Management Act 1996 in its final policy on the use of drones. This omission constitutes a failure to implement appropriate organisational measures to protect against unauthorised and unlawful processing.

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

G. CCTV Live Feed to [redacted]

Regime: Law Enforcement Directive
Inquiry Report Issue: 6

8.53 The Council monitors 40 CCTV cameras at their Information Systems Server Room in City Hall, and provides live feeds of 18 of those cameras to [redacted]. All 18 of those cameras were authorised under Section 38(3)(c) of An Garda Síochána Act 2005.

8.54 An Garda Síochána and the Council are joint controllers of this processing of personal data. The purposes and means of this processing are determined by An Garda Síochána Act 2005 and the delegated legislation made pursuant to it. The definition of '*controller*' in Section 69 of the 2018 Act anticipates that controllers can be nominated by law in such circumstances.

8.55 The law nominates both An Garda Síochána and the Council as controllers. Section 38(7) provides that Gardaí shall have access to the CCTV for the purpose of *'controlling the operation of the CCTV on behalf of the Garda Commissioner'*. Thus, the Act assigns An Garda Síochána as controller of this processing. The Garda Síochána (CCTV) Order 2006[36] provides that applications for authorisations under Section 38(3)(c) must include an undertaking *'by the local authority concerned that it will act as a data controller in respect of the CCTV'*[37]. Thus, the legislation provides that the Council must also undertake the role of controller.

8.56 I note the Council's submission that An Garda Síochána have stated that they will not be acting as a joint data controller for the camera system because it does not have full access and control over the system. When the Garda Commissioner authorises CCTV under Section 38, An Garda Síochána are, by virtue of that Section, obliged to act as joint controller. The Garda Commissioner determines where the CCTV is warranted[38], can impose terms and conditions on the Authorisation[39], supervises and controls the operation of the CCTV[40], and may issue directions to authorised persons on an ongoing basis[41]. The Commissioner can revoke an Authorisation with the Policing Authority's consent in certain circumstances, including where the Garda Commissioner's directions have not been complied with. Thus, An Garda Síochana's ongoing supervisory role can

[36] Statutory Instrument 289/2006.
[37] Article 4(d) Statutory Instrument 289/2006.
[38] Section 38(2) An Garda Síochána Act 2005.
[39] Section 38(6) An Garda Síochána Act 2005.
[40] Section 38(7)(a) An Garda Síochána Act 2005.
[41] Section 38(8)(a) An Garda Síochána Act 2005.

lead to the cessation of the processing. An Garda Síochána cannot disregard its obligations under Section 38 after issuing an Authorisation, and it acts as a joint controller where it does so.

8.57 Section 79 of the 2018 Act requires joint controllers to have an agreement in writing that determines their respective responsibilities unless those responsibilities are determined by EU law or the law of the State:

> *'(1) Where 2 or more controllers jointly determine the purposes and means of the processing of personal data (in this Part referred to as "joint controllers"), they shall determine their respective responsibilities for compliance with this Part in a transparent manner by means of an agreement in writing between them, save in so far as the said responsibilities are determined by the law of the European Union or the law of the State.*
>
> *(2) An agreement in writing referred to in subsection (1)—*
>
> *(a) shall include a determination of—*
>
> *(i) the respective responsibilities of the joint controllers concerned as regards the exercise by data subjects of their rights under this Part, and*
>
> *(ii) the respective duties of the joint controllers concerned as regards the provision to a data subject of the information specified in section 90 (2),*
>
> *and*
>
> *(b) may designate a single point of contact in respect of the processing concerned for the data subject to whom it relates, where such designation is not otherwise determined by the law of the State.'*

8.58 The responsibilities covered by Section 79 include, among other things, providing for the right to information under Section 90 and compliance with subject access requests under Section 91. These responsibilities are not provided for in An Garda Síochána Act 2005 or the delegated legislation made pursuant to it[42]. Thus, Section 79 requires an agreement in writing between the Council and the Gardaí. That agreement may designate the Council as a single point of contact for data subjects if the parties deem it appropriate. However, the lack of such agreement infringes Section 79.

[42] Such matters could also be provided for in guidelines issued by the Policing Authority with the consent of the Minister under Section 38(11) of the Garda Síochána Act 2005, however, no such guidelines have yet been issued.

8.59 The lawful basis for the Council's sharing of live-feed CCTV footage with [redacted] can be based on Section 38(7) of An Garda Síochána Act 2005, which provides:

> *'A person given an authorisation under subsection (3)(c) shall ensure that members of the Garda Síochána have access at all times to the CCTV to which that authorisation relates for the purpose of—*
>
> *(a) supervising and controlling the operation of the CCTV on behalf of the Garda Commisioner, or*
>
> *(b) retrieving information or data recorded by the CCTV.'*

8.60 Sharing data constitutes processing of data. For processing under the LED to be lawful, the processing must be necessary for the performance of a task of a competent authority and the processing must be based on Union or Member State law[43]. The Council is under a duty to provide access to the CCTV to members of An Garda Síochána. Thus, the processing is based on Member State law. These CCTV systems are installed to facilitate the deterrence, prevention, detection and prosecution of offences, and the footage is shared with the Gardaí not only to allow the Gardaí to supervise and control it, but also to allow them to retrieve data recorded by the CCTV. Thus, it is clear that the purpose of the sharing includes An Garda Síochána's task of preventing, investigating, detecting or prosecuting criminal offences. The final step is to apply the necessity test for the live feed in relation to this purpose. If the necessity test is passed, all of the requirements of Section 71(2) of the 2018 Act would be fulfilled, meaning that the processing through the live feed would be lawful.

Findings

8.61 I find that the Council infringed Section 79 of the 2018 Act by failing to implement an agreement in writing with An Garda Siochána detailing the issues required by that Section.

H. CCTV: Access Logs for Remote Access

Regime: Law Enforcement Directive
Inquiry Report Issue: 7

8.62 When the Council's employees access the CCTV system, a log is created of the individual's username, the time of access, and the footage accessed. However,

[43] See Part 7C of this decision.

where the footage is accessed remotely from [redacted], no unique user identification is logged, and the accesses are simply recorded as '*Garda*'.

8.63 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 record, among other things, the consultation of the personal data by any person[44]. The identification of the person who consulted the data must be included on the log in so far as possible.[45]

8.64 Given that An Garda Síochána and the Council are joint controllers in respect of this processing of personal data, and in the absence of an agreement in writing between them pursuant to Section 79 of the 2018 Act, the DPC finds that they are both responsible for ensuring that a user-specific log is maintained in respect of all accesses to the CCTV system. This Decision finds that the Council has infringed its obligations under Section 82 by failing to record unique user identification for remote accesses from [redacted].

8.65 Compliance with Section 82(1) and (2) would not involve a disproportionate effort and would not cause serious difficulties to the Council, and therefore the obligations on the Council cannot be delayed pursuant to Section 82(5).

Findings

8.66 I find that the Council infringed Section 82(1) and (2) of the 2018 Act by failing to maintain a data log that recorded user specific accesses of the CCTV from [redacted].

I. CCTV: Secondary Processor at Poleberry Walkway

Regime: Law Enforcement Directive
Inquiry Report Issue: 9

8.67 The Council engaged [redacted] to provide CCTV services at Poleberry Walkway. [redacted] is a processor of the personal data and there is a written agreement with the Council that reflects this. [redacted] are partners in the [redacted]. [redacted] monitors 8 of the 22 CCTV cameras on the Poleberry Walkway. These cameras cover an area in which an alarm is triggered to signify encroachments beyond a particular part of the walkway.

[44] Section 82(1)(b) of the 2018 Act.
[45] Section 82(2)(c) of the 2018 Act.

8.68 Section 80(2)(d)(ii) of the 2018 Act requires that written agreements between controllers and processors must provide that the processor shall procure the services of another processor only where authorised to do so in advance and in writing by the controller. I find that the [redacted] is a *'secondary processor'* as its services have been procured by [redacted]. Flowing from this, advanced authorisation in writing is required from the Council. The inquiry team found no evidence that the requirement to obtain the written authorisation of the Council was adhered to.

8.69 Clause 6.1 of the agreement between the Council and [redacted] provides:

> *'6.1 The Data Processor shall not engage any third parties to process the Person Data ("Sub-Processors") without obtaining the written, specific authorisation from the Data Controller.'*

8.70 Clause 6.2 of the agreement between the Council and [redacted] provides:

> [redacted] *are partners in a Grade A IS228 remote monitoring centre* [redacted] *for the real time recording within the monitoring station of footage on reactive monitored cctv sites i.e. on trespass within a protected area an intruder would activate a detector putting the site live to the control room for processing and to take action accordingly via an announcement to the intruders and requesting security services and Gardai to attend when necessary.'*

Clause 6.4 provides:

> '*The Data Processor confirms at the time of entering into this Data Processor Agreeement that it does not use any Sub-Processors*'.

8.71 Clause 6 of the written agreement between the Council and [redacted] does not satisfy the requirements of Section 80(2)(d)(ii). Although Clause 6.1 necessitates written authorisation for secondary processors, the provisions of Clauses 6.2 and 6.4 create ambiguity as to the status of [redacted] regarding the processing of personal data through the CCTV. The clause is not sufficiently clear to provide a general authorisation to procure the services of [redacted] and does not constitute the Council's advance authorisation in writing for the secondary processing. This ambiguity may have contributed to the lack of written authorisation of the Council for the secondary processing. The effect of the ambiguity in Clause 6 is that the agreement between the Council and [redacted] fails to clearly provide

that [redacted] shall procure the services the [redacted], and any other secondary processor, only where authorised to do so in advance by the Council.

Findings

8.72 I find that the Council infringed Section 80(2)(d)(ii) of the 2018 Act by failing to ensure that its contract with [redacted] clearly provided that [redacted] shall procure the services of another processor only where authorised to do so in advance and in writing by the Council.

J. Transparency: CCTV, Drones and Dash Cams

Regime: Law Enforcement Directive
Inquiry Report Issue: 3, 4 & 11

8.73 Section 90 of the 2018 Act obliges the Council 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. Section 90(2) of the 2018 Act lists the information that must be provided or made available:

> '*(a) the identity and the contact details of the controller;*
>
> *(b) the contact details of the data protection officer of the controller, where applicable;*
>
> *(c) the purpose for which the personal data are intended to be processed or are being processed;*
>
> *(d) information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data;*
>
> *(e) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;*
>
> *(f) in individual cases where further information is necessary to enable the data subject to exercise his or her rights under this Part, having regard to the circumstances in which the personal data are or are to be processed, including the manner in which the data are or have been collected, any such information including:*
>
> > *(i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data;*
> >
> > *(ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of*

the giving of the information, the criteria used to determine the said period;

(iii) where applicable, each category of recipients of the data.'

8.74 Section 90(3) expressly provides that the information in paragraphs (a) – (e) may be made available by means of a publication on the controller's website. However, Section 93(1) provides controllers must take all reasonable steps to ensure that such information is, amongst other things, provided or made available in an easily accessible form.

8.75 The Council uses 3 different types of CCTV signs to inform the public that CCTV cameras are in operation: the 'Waterford City Council' signs, the [redacted] signs and the yellow signs. The Council has also made a publication on its website, which makes some of the required information available to data subjects pursuant to Section 90(3). However, the Council's failure to reference the website on the signs infringes its obligation pursuant to Section 93(1) to take all reasonable steps to ensure that the information is made available in an easily accessible form.

8.76 The inquiry found no evidence that appropriate signage has been fitted on official vehicles that use dash cams. The sticker at page 7 of the Council's DPIA on Dash cams gives a warning that dash cam recording is ongoing, but does not contain any further information and does not reference the Council's website. However, the Council submitted to the DPC on 16th April 2020 that staff driving those vehicles carried the document *'Policy sheet for use of Dash cams – Litter Enforcement'* for the purpose of presenting it to any member of the public who made an enquiry regarding the processing. That document references the Council's Policy on the use of Dash Cams and expressly references the Council's website. In those circumstances, I am satisfied that the Council took all reasonable steps to ensure that the information on the website was available in an easily accessible form to individuals who had their images captured by the dash cams.

8.77 Communicating with data subjects who have had their images captured by drones presents challenges. However, in respect of processing under the LED, these challenges may be met by a publication on the controller's website. I have examined the Council's website, including the policies regarding the use of Drones[46]. I have also examined the website in the context of the information required by Section 90(2)(a) – (e) for the Council's use of CCTV cameras and dash cams. I have considered the Privacy Statement, Data Protection Policy, and

[46] Policy regarding use of Drones by Environment Department and Policy regarding use of Drones by Water Services Department.

the policies on dash cams and drones linked on the website[47]. I am satisfied that the information required by Section 90(2)(a) – (d) is available on the website. However, the website does not detail the right of data subjects to lodge a complaint with the DPC and the contact details of the DPC as required by Section 90(2)(e). Although the website, references *'see gdprandyou.ie'*, this is not sufficient for the purposes of Section 90(2)(e). That subsection requires the Council to expressly state that data subjects have the right to lodge a complaint with the DPC.

Findings

8.78 I find that the Council infringed Section 90(2)(e) of the 2018 Act by failing to make available to data subjects information detailing their right lodge a complaint with the DPC and the contact details of the DPC within a reasonable period after their images are captured on the Council's CCTV systems, dash cams and drones.

8.79 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 that it did provide on its website, regarding the use of CCTV, was made available in an easily accessible form by referencing the website on the signs.

K. Data Protection Policies: CCTV, Drones, Dash Cams, Body Worn Cameras and Covert Cameras

Regime: GDPR and Law Enforcement Directive
Inquiry Report Issue: 2 & 12

8.80 The Authorised Officers established that the Council had no data protection policies regarding their use of CCTV, body worn cameras, dash cams, covert cameras and drones at the time of the inquiry. Since the inquiry commenced, the Council has finalised policies, which are available on its website.

8.81 Article 24(1) of the GDPR requires controllers to implement appropriate technical and organisational measures to ensure that their processing complies with the GDPR. Such measures include implementing appropriate data protection policies where proportionate to the processing activities[48]. In considering what measures are appropriate to implement, regard must be had to the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

[47] http://www.waterfordcouncil.ie/departments/corporate/communications/privacy-statement.htm
[48] Article 24(2) GDPR.

8.82 A Data Protection Policy is an important tool for communicating to traffic wardens how and when body worn cameras can be used and for ensuring that this processing is conducted lawfully. Having regard to the risks presented by unlawful use of body worn cameras, the wide scope of such processing in public places, and the nature of the type of data that could potentially be processed, the measures required by Article 24 include a Data Protection Policy. Therefore, the Council infringed Article 24 by failing to adopt a final Data Protection Policy for the cameras prior to September 2019. I note that a policy has now been adopted and is available on the Council's website.

8.83 Regarding processing that falls under the LED, similar obligations exist under Section 75 of the 2018 Act, which provides that:

> *'(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.'*

8.84 Having regard to nature of the processing undertaken by the Council, and in particular the risks to the rights and freedoms of persons, I find that obligation to implement appropriate technical and organisational measures includes an obligation to implement data protection policies for the use of CCTV, dash cams, covert cameras and drones. The Council's failure to implement such policies at the time of the inquiry constitutes an infringement of its duties under Section 75 of the 2018 Act.

Findings

8.85 I find that the Council infringed Article 24(1) of the GDPR by processing personal data by means of body worn cameras prior to implementing a data protection policy for their use.

8.86 I find that the Council infringed Section 75 of the 2018 Act by processing personal by means of CCTV, dash cams, covert cameras and drones prior to implementing data protection policies for their use.

9. Corrective measures

9.1 Having considered the infringements identified in this Decision, I have decided to exercise corrective powers in accordance with Sections 111(3) and 124(3) of the 2018 Act. I have set out below the corrective powers, pursuant to Sections 115(1) and 127(1) of the 2018 Act, which I have decided to exercise:

1. Pursuant to Article 58(2)(d) of the GDPR and Section 115 of the 2018 Act, I order the Council to bring its processing into compliance with the relevant provisions of the GDPR identified in the table below, by taking the relevant action specified at point 7 in the table below;

2. Pursuant to Article 58(2)(b) of the GDPR and Section 115 of the 2018 Act, I issue a reprimand to the Council in respect of the Council's infringements of the 2018 Act set out at point 6 in the table below;

3. Pursuant to Section 127(1)(f), I impose a temporary ban on processing by the Council as set out at points 1, 2, 3 & 4 in the table below;

4. Pursuant to Section 127(1)(d) of the 2018 Act, I order the Council to bring its processing into compliance with the relevant provisions of the 2018 Act identified at points 5 & 9 in the table below, by taking the relevant action specified in the table; and

5. Pursuant to Section 127(1)(b) of the 2018 Act, I issue a reprimand to the Council in respect of the Council's infringements of the 2018 Act set out at points 6, 8, 10, 11 & 12 in the table below. I issue the reprimand in light of the number and extent of the infringements identified.

9.2 In deciding on the corrective powers that are to be exercised in respect of the infringements of Articles 5(2) and 24(1) of the GDPR, I have had due regard to the Commission's power to impose administrative fines pursuant to Section 141 of the 2018 Act. In particular, I have considered the criteria set out in Article 83(2)(a) – (k) of the GDPR. When imposing corrective powers, I am obliged to select the measures that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures, for example re-establishing compliance with

the GDPR or punishing unlawful behaviour (or both)[49]. I find that an administrative fine would not be necessary, proportionate or dissuasive in the particular circumstances in relation to the infringements of Article 5(2) and 24(1) of the GDPR. In coming to this finding, I have had particular regard to the Council's attempts to demonstrate the necessity of the body worn cameras, including through the Data Protection Impact Assessments dated March 2018 and September 2019, which show the unintentional nature of the Council's infringement of Article 5(2). Regarding the infringement of Article 24(1), I have had particular regard to the Council's pre-existing practice of having the body worn cameras switched off by default and the action taken by the Council to mitigate this infringement, including by the introduction of a policy for body worn cameras since the inquiry commenced. I find that the nature, gravity and duration of both infringements is significantly mitigated by how the Council limited the use of the body worn cameras at the time of the infringements and the steps taken by the Council since the inquiry commenced. For the reasons outlined, I find that no administrative fine should be imposed in respect of these infringements.

9.3 For the purpose of outlining the corrective measures, I will group the measures according to the following themes of the infringements:

(i) The lawful bases for the processing;
(ii) Transparency (including privacy policies and CCTV policies); and
(iii) Accountability and technical and organisational measures.

9.4 In determining the time scale for compliance with the measures specified in the table, I have had regard to the Council's submissions and 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 extended time scales for compliance with some of the measures, as detailed in the table below.

(i) <u>Lawful Bases for the Processing</u>

No.	Finding Number	Action	Time Scale
1	8.35	Dash Cams Sections 71(1)(a) and 72 of the 2018 Act I find that there is no lawful basis for the Council's	The Council is required to confirm to the Data Protection Commission [redacted] within 7 days of receiving this

[49] See the Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

		processing of personal data by means of dash cams for law enforcement purposes. I impose a temporary ban on the Council's use of dash cams for law enforcement purposes. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing by a Local Authority in accordance with Article 8(2) of the LED.	Decision that the cameras are switched off.
2	8.35	Covert Cameras Section 71(1)(a) and 72 of the 2018 Act I find that there is no lawful basis for the Council's processing of personal data by means of covert cameras for law enforcement purposes. I impose a temporary ban on the Council's use of covert cameras for law enforcement purposes. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing by a Local Authority in accordance with Article 8(2) of the LED.	The Council is required to confirm to the Data Protection Commission [redacted] within 7 days of receiving the Decision that the cameras are switched off.
3	8.39	CCTV at Poleberry Walkway Section 71 of the 2018 Act I find that there is no lawful basis for the Council's use of CCTV at Poleberry Walkway. I impose a temporary ban on the Council's use of CCTV at this location. This processing must not resume in the absence of authorisation from	In light of the Council's submissions regarding the time required to finalise its current application with An Garda Síochána and how the current COVID-19 crisis is impacting the Council's ability to progress this matter, the Council must confirm in writing by **22nd February 2021** [redacted]

		the Garda Commissioner under Section 38 of An Garda Síochána Act 2005. In the event that such an Authorisation is obtained, the processing should resume only if the Council can demonstrate its lawfulness, including its necessity. A DPIA will be required to achieve this.	[redacted] to the DPC that the CCTV cameras at this location are switched off, unless authorisation under Section 38 of An Garda Síochána Act 2005 is acquired in the meantime.
4	8.44	CCTV at Williamstown Municipal Golf Course Sections 17 and 73 of the 2018 Act I find that there is no lawful basis for the Council's use of CCTV at Williamstown Municipal Golf Course. I impose a temporary ban on the Council's use of CCTV at this location. This processing must not resume in the absence of authorisation from the Garda Commissioner under Section 38 of An Garda Síochána Act 2005. In the event that such an Authorisation is obtained, the processing should resume only if the Council can demonstrate its lawfulness, including its necessity, and that a condition under Section 73(1)(b) is applicable. A DPIA will be required to achieve this.	The Council is required to confirm to the Data Protection Commission within 7 days of receiving the Decision [redacted] that the cameras are switched off, unless authorisation under Section 38 of An Garda Síochána Act 2005 is acquired in the meantime.

(ii) <u>Transparency (including privacy policies and CCTV policies)</u>

No.	Finding Number	Action	Time Scale

5	8.78 and 8.79	Transparency for CCTV and Drones Section 90 and 93(1) of the 2018 Act I order the Council to bring its processing of personal data by means of CCTV and drones into compliance with Section 90 of the 2018 Act by ensuring that data subjects are provided with all of the information required by Section 90(2) of the 2018 Act. This may be achieved by updating the Council's website to add to the information already available there. If the Council intends to rely on publications on its website to comply with Section 90, it must take all reasonable steps to ensure that the information is made available in an easily accessible form. Such reasonable steps include referencing the Council's website on the CCTV signs at the various locations.	Complete tasks and submit a report to the DPC [redacted] detailing the action taken by **22nd February 2021.**
6	8.85 and 8.86	Data Protection Policies Article 24(1) of the GDPR & Section 75 of the 2018 Act I issue a reprimand to the Council for infringing Article 24(1) of the GDPR by processing personal data by means of body worn cameras prior to implementing a data protection policy for their use. I issue a reprimand to the Council for infringing Section 75 of the 2018 Act	N/A

		by processing personal data by means of CCTV, dash cams, covert cameras and drones prior to implementing data protection policies for their use. This reprimand is in addition to the corrective measures at numbers 1 and 2 identified above, imposing a ban on the Council's use of dash cams and covert cameras for law enforcement purposes.	

(iii) Accountability and technical and organisational measures

No.	Finding Number	Action	Time Scale
7	8.19	Body Worn Cameras Article 5(2) GDPR In order to demonstrate the necessity of the processing of personal data by means of body worn cameras for the performance of task carried out in the public interest or in the exercise of official authority, the Council is required to carry out a revised comprehensive DPIA. The DPIA must consider the necessity of the processing for a task that is carried out in the public interest or in the exercise of official authority, for example, the Council's powers under the Local Authorities (Traffic Wardens) Act 1975, considered alongside its obligations under the Safety, Health and Welfare at Work Act 2005. The DPIA must consider	Complete tasks and submit the DPIA [redacted] by **22nd February 2021.**

		alternative less intrusive measures.	
8	8.47	Drones Section 71(10) of the 2018 Act I issue a reprimand to the Council on the basis of the infringement, identified herein, of Section 71(10) of the 2018 Act, by processing personal data by means of drones prior to carrying out a DPIA demonstrating the lawfulness of this processing.	N/A
9	8.52	Drones Section 75 of the 2018 Act I order the Council to bring its processing of personal data by means of drones into compliance with Section 75 of the 2018 Act by implementing appropriate technical and organisational measures to protect against unlawful processing by ensuring that the statutory pre-requisites for making recordings under that Section are communicated in its policy on the use of drones by the Environment Section.	Complete tasks and submit a report to the DPC [redacted] detailing the action taken by **22nd February 2021.**
10	8.61	CCTV Live Feed to Ballybricken Garda Station Section 79 of the 2018 Act I note the Council's submission on 30th October 2019 to the Authorised Officers that the live link to Ballybricken Garda Station has been removed. However, in circumstances where Section 38 of the	N/A

		2005 Act obliges An Garda Síochána to act as a joint controller, an agreement in writing between the Council and An Garda Síochána that satisfies the provisions of Section 79 of the 2018 Act is required irrespective of the availability of the live link. Therefore, I issue a reprimand to the Council on the basis of the infringement of Section 79.	
11	8.66	Access Logs for Remote Access Section 82 of the 2018 Act I issue a reprimand to the Council on the basis of the infringement of Section 82 for the failure to maintain a data log for user specific accesses to the CCTV at the time that the live link was operative.	N/A
12	8.72	Secondary Processor at Poleberry Walkway Section 80 of the 2018 Act I issue a reprimand to the Council for failing to ensure that its contract with [redacted] Limited complied with Section 80(2)(d)(ii) of the 2018 Act. This reprimand is in addition to the corrective measure number 1 identified above, imposing a ban on the Council's use of CCTV at this location.	N/A

10. Right of appeal

10.1 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