In the matter of the General Data Protection Regulation and the Data Protection Act 2018

DPC Case Reference: 07/SIU/2018

In the matter of Sligo County Council

Decision of the Data Protection Commission made pursuant to sections 111 and 124 of the Data Protection Act 2018

Further to an own-volition inquiry commenced pursuant to sections 110 and 123 of the Data Protection Act 2018

DECISION

Decision-Makers for the Data Protection Commission:

Dr Des Hogan, Commissioner for Data Protection and

Mr Dale Sunderland, Commissioner for Data Protection

13 November 2024

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document is a Final 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'). As the two members of the DPC, we perform this function in our roles as the Commissioners and decision-makers in the DPC. The DPC makes this Decision having considered the information obtained in the separate own volition inquiry (the '**inquiry**') conducted by Authorised Officers of the DPC pursuant to sections 110 and 123 of the 2018 Act (the '**Inquiry Team**').The Authorised Officers who conducted the inquiry provided Sligo County Council (the '**Council**') with the Draft Inquiry Report and the Final Inquiry Report.

1.2 The Council was provided with a draft decision on this inquiry (the '**Draft Decision**') on 14 September 2023 to afford the Council an opportunity to make any further submissions, which it deemed necessary. The DPC received submissions from the Council relating to the Draft Decision on 13 October 2023. The Council was provided with a Revised Draft Decision on 20 June 2024 to give it a final opportunity to make any further submissions that it deemed necessary, including as to the proposed findings and the proposed corrective powers. The Council responded on 3 July 2024 to say that it would not be making any further submissions. The DPC has considered the submissions made by the Council in advance of arriving at the Decision in accordance with sections 111 and 124 of the 2018 Act. This 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, the reasons for it, and the corrective powers that the DPC has decided to exercise.

1.3 It is important to point out that the views of the Inquiry Team as expressed in the Draft Inquiry Report and Final Inquiry Report and the findings set out in this Decision are based on the situations that pertained during the inspection phase of the inquiry itself (i.e. on 1 April 2019 and 8 April 2019 when the physical inspections were conducted). For the avoidance of any doubt, this Decision covers the period of the inquiry up to the conclusion of the inspection phase.

1.4 The Decision contains corrective powers under sections 115 and 127 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (the '**GDPR**') arising from the infringements which have been identified herein. The Council is required to comply the corrective powers that are exercised in the Decision and it is open to this office to serve an enforcement notice on the Council in accordance with section 133 of the 2018 Act.

2. Factual Background

2.1 The GDPR and the Law Enforcement Directive (the '**LED**') elaborate on the indivisible, universal values of human dignity, freedom, equality and solidarity as enshrined in

the Charter of Fundamental Rights of the EU ('the Charter') and Article 8 in particular, which safeguards the protection of personal data. Article 8 of the Charter provides:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

2.2 The use of technologies for surveillance purposes by the State can significantly impact the rights and freedoms of individuals. This is particularly the case if the manner in which such technologies are deployed does not comply with data protection law. Authorised Officers from the Special Investigation Unit of the DPC were authorised 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 for law enforcement purposes. In initiating the inquiries, the DPC wished:

(i) To establish whether any data processing that takes place in this context is in compliance with the 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.

2.3 The inquiry leading to this Decision was conducted initially by means of an audit under section 136 of the 2018 Act. This facilitated the Authorised Officers in compiling facts in relation to the deployment of surveillance technologies by the Council. On 15 June 2018, the DPC formally notified the Data Protection Officer of the Council in writing that the DPC intended to conduct an audit of the Council pursuant to section 136 of the 2018 Act. The notice advised the Data Protection Officer that the audit would commence on 25 June 2018 and that the opening phase of the audit would involve the DPC providing a questionnaire to be completed over the following twenty-one days. The notice also advised that once the response to the questionnaire was considered, the Data Protection Officer would be informed about the next phase of the data protection audit which may include, for example, the issuing of a further questionnaire, or on-site inspections by Authorised Officers of the Commission, or meetings (if deemed necessary) with the local authority, or the use of any of the Commission's other statutory powers that may be deemed necessary at the time to advance the inquiry.

2.4 The notice advised that the audit would inquire into the processing of personal data, by or on behalf of the Council, through the use of CCTV and Automated Number Plate Recognition ('**ANPR**') systems and any other technologies that may be used to monitor individuals. The DPC informed the Council that the processing of personal data by means of CCTV security cameras situated on or in local authority offices or other local authority buildings for the purpose of safeguarding persons or property on the premises or in its environs was excluded from the scope of the inquiry. The Council was informed that the information obtained in the inquiry would be relied upon by the DPC in making a decision as to whether the 2018 Act and/or the GDPR has been infringed and if so, whether corrective powers should be exercised.

2.5 On 25 June 2018, the DPC formally notified the Data Protection Officer in writing that the audit of the Council had commenced and enclosed Questionnaire No. 1. A period of twenty-one days was given to the Council to answer Questionnaire No. 1. The DPC received the completed Questionnaire No. 1 with a number of attachments from the Council on 10 August 2018.

2.6 On 4 March 2019, the DPC notified the Data Protection Officer in writing about the next phase of the inquiry which would involve inspections by the Authorised Officers. The notice referred to the Authorised Officers powers of search and inspection pursuant to section 130 of the 2018 Act. It explained that the Authorised Officers would first need to meet with the Data Protection Officer to discuss the Council's replies to the questions in Questionnaire No. 1 and the accompanying attachments submitted to ensure that they have a full and complete understanding of the situation. In terms of inspection work, the DPC stated that as a starting point the Authorised Officers would need to inspect CCTV monitoring centre(s) in operation and they would need to inspect the central point for any CCTV feeds and to inspect at least some of the CCTV camera sites. The DPC signalled that there may be further phases which would deal with the replies to other questions in Questionnaire No. 1.

2.7 Further to this notification to the Data Protection Officer, inspections were carried out by Authorised Officers as follows:

<u>On 1 April 2019</u>

- The first session on this inspection date comprised a meeting with the Data Protection Officer and other officials at County Hall, Riverside, Sligo. In attendance from Sligo County Council were [redacted] (Data Protection Officer), [redacted] (Environment Department), [redacted] (Finance) and [redacted] (Housing).

- The second session of this inspection comprised an on-site inspection at the CCTV control room in a County Council property at Cranmore, Sligo. In attendance from Sligo County Council were [redacted] (Data Protection Officer), [redacted] (Housing) and [redacted] (Community Warden Cranmore).

- Two Authorised Officers of the Data Protection Commission, [redacted] and [redacted], were in attendance throughout both sessions.

On 8 April 2019

- The first session comprised an inspection of CCTV cameras and recording equipment at Sligo Harbour. In attendance were [redacted] (Data Protection Officer) and [redacted] (Harbour Master).

- The second session comprised an inspection of CCTV cameras and recording equipment at the Lidl site and ESB Building. In attendance were [redacted] (Data Protection Officer), [redacted] and [redacted]

- The third session comprised an inspection of CCTV cameras and recording equipment at the Market Yard site. In attendance were [redacted] (Data Protection Officer), [redacted] and [redacted].

- The fourth session comprised an inspection of CCTV cameras and recording equipment at the Supermacs site. In attendance were [redacted] (Data Protection Officer), [redacted] and [redacted].

- The fifth session comprised an inspection of CCTV cameras and recording equipment at Ballisodare Community Centre. In attendance were [redacted] (Data Protection Officer), [redacted] and [redacted].

- Two Authorised Officers of the Data Protection Commission, [redacted] and [redacted], were in attendance throughout all sessions.

The DPC has relied on the information gathered from this inquiry in the context of this Decision.

2.8 The DPC received a CCTV Inventory on 22 March 2019. In summary, the inventory shows that as of the date of the inquiry, the Council deploys the following surveillance technologies:

- 23 CCTV Cameras operated by Housing Department, 19 of these cameras also feed on a live basis into Sligo Garda Station;

- 15 CCTV Cameras at Sligo Harbour;

- 14 Covert Cameras operated by the Environment Department;

- CCTV cameras in operation at 9 bottle bank sites under the control of the Environment Department; and

- 1 ANPR camera in operation at one of these bottle bank sites.

2.9 Ultimately the Authorised Officers completed a final Inquiry Report which they submitted for decision-making on 19 March 2020. The DPC is obliged to consider that Inquiry Report and reach final conclusions regarding any infringements of data protection legislation. As set out above, this document is the Decision of the DPC on this matter and includes the corrective powers that the DPC has chosen to exercise arising from the infringements that are identified herein.

2.10 The findings made in this Decision include, amongst other things, findings concerning a CCTV system authorised by the Garda Commissioner under section 38 of the Garda Síochána Act 2005 (the '**2005 Act**'). This Decision does not consider the criteria used to assess and approve this CCTV system, nor does it consider whether the approval process was correctly undertaken.

2.11 The DPC is satisfied that the audit and inquiry were correctly conducted and that fair procedures were followed throughout, including, but not limited to, notifications to the controller and an opportunity for the controller to comment on a draft inquiry report before it was finalised.

3. Topics arising in this Decision

3.1 This Decision considers the processing of personal data through a range of technologies, including CCTV and ANPR systems. The contexts of the processing operations are diverse and include traffic management, 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 GDPR and the Law Enforcement Directive (the '**LED**'). 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:

(i) Garda Síochána Act 2005 (as amended);

(ii) Litter Pollution Act 1997 (as amended);

(iii) Local Government Act 2001 (as amended);

(iv) Housing Acts 1966 to 2021; and

(v) Waste Management Act 1996 (as amended).

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 the 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 regime 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 supplemented in 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 provides:

> *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 processing of personal data 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 2018 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' in this context, 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....

4.7 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 pubic 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"*[1]. There is no basis for departing from the ordinary meaning of the word 'or' and it cannot have 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

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

part (a) of the definition, a competent authority must also determine the purposes and means of the processing, alone or jointly.

4.8 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

4.9 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.

4.10 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.

4.11 In *Puskar v Finance Directorate of the Slovak Republic*[2] the Court of Justice of the European Union (the '***CJEU***') considered the scope of the Data Protection Directive,[3] specifically the Directive's non-application to processing operations concerning the activities of the State in areas of criminal law.[4] 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.*[5]

On that basis, the criminal law exclusion was not applicable, and the Data Protection Directive was held to apply to that processing.

4.12 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

---

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

[3] 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.

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

[5] Case C-73/16, *Peter Puskar v Finance Directorate of the Slovak Republic*, judgment of 27 September 2017 (ECLI:EU:C:2017:725), at paragraph 40.

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.

a) Processing that falls under the GDPR

4.13 The GDPR is applicable to the Council's processing of personal data in relation to CCTV cameras and ANPR cameras which are used for the primary purpose of security.

4.14 Here, the Council is not processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences.

4.15 Although the data processed through the use of Traffic Management CCTV cameras has the potential for subsequent use by An Garda Síochána for the purposes of facilitating the deterrence, prevention, detection and prosecution of offences, this does not form part of the Council's 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.

b) Processing that falls under the LED

4.16 The LED is applicable to the remainder of the processing operations that fall for consideration in this Decision. These processing operations include:

a. The use by the Housing Department of CCTV cameras at certain housing estates for the purposes of preventing and detecting anti-social behaviour; and

b. The use by the Environment Department of CCTV cameras and one ANPR camera to prevent and detect illegal dumping in exercising the Council's criminal enforcement functions under the Litter Pollution Act 1997.

(i) *CCTV relating to Housing Estates and Bottle Banks*

4.17 The purposes of the processing of personal data captured through CCTV cameras used by the Housing Department of the Council at housing estates bring that processing under the LED. Personal data collected via those CCTV cameras is used by the Council for the purposes of preventing anti-social behaviour pursuant to legislation applicable to the management of housing estates and for the purposes of preventing, detecting and prosecuting illegal dumping pursuant to legislation applicable to littering and dumping. Thus, each piece of technology is used with the

specific purpose of preventing, investigating, detecting and/or prosecuting criminal offences.

4.18 The CCTV systems operated by the Council at bottle bank facilities, which have not been authorised under the 2005 Act, also fall under the LED. The Council is a controller of this personal data within part (a) of that definition in section 69 of the 2018 Act. As we have seen, the Council is a competent authority. It determines the purposes and means of the processing. It decided to install those CCTV systems for purposes of preventing and detecting illegal dumping. Thus, the Council determines 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 of the 2018 Act.

4.19 Regarding the Council's use of CCTV systems, the Council is a 'controller' within part (a) of that definition under section 69 (above). The Council is a competent authority because it enjoys competence for the prevention of certain anti-social behaviour under the Housing Acts 1966 to 2021 and for the prevention, investigation, detection and prosecution of litter related offences under the Litter Pollution Act 1997 and the Waste Management Act 1996 (as amended). Furthermore, it is subject to a general duty to have regard to the importance of taking steps for the prevention of crime, when performing its functions, under section 37(1) of the 2005 Act.

(ii) *CCTV authorised under section 38 of the 2005 Act*

4.20 The CCTV systems operated by the Council pursuant to section 38 of the 2005 Act 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 the 2005 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[6] and the systems that can be used.[7]

4.21 The Council is nominated as controller of this processing by Article 4(d) of the Garda Síochána (CCTV) Order 2006[8], which requires local 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.

---

[6] 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.

[7] 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.

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

4.22 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 Part 5. Therefore, even though the Council does not use this CCTV to investigate or prosecute criminal offences, it is clear that it records 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 the LED and Part 5 of the 2018 Act.

4.23 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 the LED and Part 5 of the 2018 Act.

5. Data Controller

5.1 This Decision and the corrective measures that are contained herein are addressed to the Council as a controller for the processing concerned.

6. Personal Data

6.1 *'Personal data'* is defined under the GDPR as *"any information relating to an identified or identifiable natural person"*.[9] Section 69 of the 2018 Act implements a similar definition of *'Personal data'* under the LED.

6.2 This Decision concerns CCTV systems and ANPR systems. These devices capture visual images of individuals and vehicles. It is possible to identify individuals from such images. Thus, the data processed by the devices includes *"personal data"*.

7. Analysis and Findings

7.1 The Authorised Officers identified a total of 14 issues in the course of the inquiry. This Decision will consider each in turn and also considers the commonality of issues identified.

7.2 Since the inquiry commenced, the Council has taken steps to address some of the issues identified in the inquiry. This Decision sets out findings as to whether infringements of the GDPR and/or the 2018 Act have occurred during the temporal scope of the inquiry (from commencement of the inquiry 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

[9] Article 4 GDPR.

the issues leading to the findings in this Decision may since have been addressed by the Council.

a) Legal bases for the surveillance technologies employed for the purposes of preventing, investigating, detecting or prosecuting crime

i. CCTV Cameras

1. Environment Section: Legal Basis for CCTV Cameras at bottle banks to detect illegal dumping

Regime: LED

Inquiry Report Issue: 3

7.3 CCTV cameras were operated by the Environment Section of the Council at nine bottle bank facilities for the purposes of facilitating enforcement of the Litter Pollution Act 1997. In light of the purposes of the processing, this activity falls under the LED. The DPC must assess whether the Council had a legal basis to process personal data collected via these cameras in these circumstances.

7.4 The Council has powers and duties for the prevention, investigation, detection and prosecution of litter related offences under the Litter Pollution Act 1997 and the Waste Management Act 1996 (as amended). It relied on these functions as a lawful basis for these CCTV systems on the basis that the CCTV systems were necessary for the performance of those functions.

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

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

7.6 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*[10], the Supreme Court interpreted the Irish legislation[11] that

[10] *National Asset Management Agency -v- Commissioner for Environmental Information* [2015] IESC 51.

[11] Statutory Instrument No. 133 of 2007.

implemented Directive 2003/4/EC.[12] 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 pursuant to obligations to implement in national law the Directive, which itself was adopted in compliance with an obligation undertaken by the EU (and Ireland) under 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.*[13]

7.7 **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.*[14]

7.8 In *Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission*[15], the Court of Justice of the European Union confirmed that *'the principle of primacy of EU law requires not only the courts but all bodies of the Member States to give full effect to EU rules'*[16]. 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 intended purpose of a Directive is equally applicable to all Member State bodies.

7.9 Therefore, section 71 of the 2018 Act must be interpreted 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 LED 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.*

---

[12] 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.

[13] Ibid At paragraph 10.

[14] Ibid at paragraph 11.

[15] 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).

[16] At paragraph 39.

7.10 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; and second, the processing must be based on Union or Member State law. Where Member State law forms the basis for processing, Article 8(2) elaborates on what must be specified in that law. It must specify the objectives of processing, the personal data to be processed and the purposes of the processing.

7.11 The requirement in section 71 of the 2018 Act 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.

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

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

7.13 This means that the measures must regulate the processing by providing guidance to controllers and data subjects as to when particular processing is permissible. This is consistent with the case law of the Court of Justice of the European Union. For instance, in *Schrems v Data Protection Commissioner*[17] the Court held (at paragraph 91):

> *As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum*

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

safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.

7.14 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 to provide a lawful basis once the objectives, the personal data to be processed and the purposes are clear and foreseeable from that Act.

7.15 The DPC finds that the Council's use of CCTV footage during the temporal scope of the inquiry could not lawfully be based on the Litter Pollution Act 1997 or the Waste Management Act 1996. The DPC has carefully considered this legislation and the Council's use of CCTV to detect and take enforcement action against those engaged in littering.

7.16 These Acts did not regulate this type of processing as is required by Article 8(2) of the LED. Although the Acts provided the Council with certain functions, including for 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 did not provide for processing of images of members of the public using CCTV footage in this manner. There were no provisions in any of the Acts that could be said to govern such a wide scope of processing. Even if the Acts did specify for this personal data to be processed, in the absence of significant other amendments, the Acts were severely lacking in rules that govern the scope and application of such CCTV, including, among others, the criteria that must be fulfilled before installing such CCTV, the supervision of such CCTV once installed, and the termination of the CCTV. Furthermore, the Acts did not specify any procedures for preserving the integrity and confidentiality of personal data processed by such CCTV.

7.17 Therefore, the DPC finds that the processing of this personal data was not lawful and infringes section 71(1)(a) of the 2018 Act.

7.18 Certain sections of the Circular Economy and Miscellaneous Provisions Act 2022 may be relevant to the issue of whether the Council can process personal data with CCTV cameras for the purposes of countering littering. However, the DPC notes that for the period under inspection this legal basis did not exist. Accordingly, the DPC cannot take these provisions into account in assessing whether the Council had a valid legal basis for processing. In any event, it is important to emphasise that the controller has an obligation to demonstrate that it processes personal data lawfully by identifying the legal basis it relies upon for processing.

7.19 The DPC notes the submission made by the Council in response to the Draft Decision that all CCTV cameras at the relevant bottle bank facilities have been switched off. However, as the CCTV cameras were in operation at the time that the inspection phase was conducted the DPC finds that the Council infringed section 71(1)(a) of the 2018 Act.

Findings

7.20 ***The DPC finds that the Council infringed section 71(1)(a) of the 2018 Act by unlawfully installing and operating CCTV cameras at the nine bottle bank facilities under the control of the Environment Department.***

2) Environment Section: Use of Covert Cameras

Inquiry Report Issue: 2, 6

Regime: LED

7.21 According to the CCTV Inventory, the Environment Section of the Council operated 16 covert CCTV cameras, 2 of which are no longer in use. The purpose of the covert CCTV cameras was to detect illegal littering or dumping.

7.22 The decision to use covert surveillance could be made by any of five staff members in the Environment Section. The Inquiry Team found that each decision to engage in covert surveillance was not made at a senior level within the organisation. Covert surveillance through the use of recording equipment such as CCTV is only permitted on a case-by-case basis where the data is kept for the purposes of preventing, detecting or investigating offences. Therefore, it is incumbent on the Council to have appropriate safeguards in place for any exceptional surveillance the Council plans to carry out. While the DPC does not wish to be prescriptive, this may include steps such as a written protocol, sign off by multiple members and good overview practices. In the absence of any similar safeguards, it is the DPC's view that the Council lacked a lawful basis to carry out such surveillance.

7.23 Furthermore, the Inquiry Team found no evidence that the Council had a formal policy document or formal protocol in relation to the use of covert surveillance. Section 75(1) of the 2018 Act requires the implementation of appropriate technical and organisational measures to ensure that data processing is performed in accordance with Part 5 of the Act 2018 and for demonstrating such compliance. The organisational measures include the requirement at section 75(3) of the 2018 Act to implement an appropriate data protection policy, where such implementation is proportionate in relation to the processing activities carried out by the controller. As outlined above, the Council must also have a legal basis for processing of personal data in accordance with section 71(1)(a) of the 2018 Act.

7.24 Section 84 of the 2018 Act provides that where, having regard to its nature, scope, context and purposes, a type of processing, and in particular a type of processing using new technology, is likely to result in a high risk to the rights and freedoms of individuals, the controller that is proposing to carry out the processing shall conduct an assessment of the likely impact of the proposed processing operations on the protection of personal data (referred to as a "data protection impact assessment") prior to carrying out the processing. The Inquiry Team found that no data protection impact assessment or equivalent exercise was carried out by the Council prior to the deployment of covert CCTV cameras.

7.25 The DPC notes the submission made by the Council in response to the Draft Decision that all covert cameras that were in operation at the time of the inquiry are no longer in operation and that the Council is in the process of updating its CCTV Policy to include a protocol on covert surveillance. The DPC also notes the Council's commitment to ensure that if covert surveillance is resumed in the future, the protocol will specify that a DPIA must be carried out and decisions regarding covert surveillance must be made at senior management level. However, as the CCTV cameras were in operation at the time the inquiry was conducted the DPC finds the Council has infringed sections 71(1)(a), 75(1), 75(3) and 84 of the 2018 Act.

Findings

7.26 ***The DPC finds that the Council infringed sections 71(1)(a), 75(1), 75(3) and 84 of the 2018 Act in the operation of covert CCTV cameras at the relevant sites.***

3) Environment Section: Legal Basis for ANPR Cameras to detect illegal dumping

Regime: LED

Inquiry Report Issue: 4

7.27 ANPR Cameras are cameras that use optical character recognition technology to automatically read vehicle registration plates.

7.28 An ANPR camera was installed at Ballisodare Community Centre where a bottle bank facility has been in operation since June 2018. Two CCTV cameras were installed at the site, one of which has ANPR capability.

7.29 ANPR cameras capture images of vehicle number plates and may also capture images of individuals within the relevant vehicles, depending on how the cameras operate. It is possible for an individual to be identified from ANPR footage, either because they are directly identifiable where images of them are captured by the ANPR cameras, or indirectly because a controller can link the vehicle number plate with an identifiable individual, such as the registered owner of the vehicle. As a result, the use of ANPR cameras involves the processing of personal data. It is necessary to assess whether the Council has a legal basis to process personal data collected via the ANPR camera at Ballisodare Community Centre in these circumstances.

7.30 During the inquiry, the Inquiry Team probed the purpose for the inclusion of an ANPR camera at the Ballisodare Community Centre bottle bank facility. It was explained by the Council to the Inquiry Team that the CCTV camera supplier presented the Council with a deal for the supply of both a standard CCTV camera and an ANPR camera together.

7.31 In order to lawfully process personal data for law enforcement functions, a controller must satisfy the requirements of sections 71(1)(a) and 71(2) of the 2018 Act, which provide that in the absence of the consent of the data subject, the processing must be necessary for the performance of a function of a controller 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, which has a legal basis in the law of the EU or Ireland.

7.32 The principle of data minimisation which is set out in section 71(1)(c) of the 2018 Act requires that personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed. Furthermore, data protection by design and default requirements are set out in section 76 of the 2018 Act. Section 76 requires, among other things, the implementation of technical and organisational measures in relation to, among other things, the amount of personal data collected for the processing concerned.

7.33 The DPC considers that the capturing of images of vehicles, their drivers and passengers as they enter and exit the area of Ballisodare Community Centre by ANPR camera is not 'necessary' for the performance by the Council of its law enforcement functions, as less intrusive means were possible. In these circumstances, it is the view of the DPC that the Council was not entitled to rely on section 71(2)(a) as its legal basis for processing personal data and that the Council also breached its data minimisation obligations.

7.34 The DPC notes the Council's submission that it no longer operates ANPR cameras at any location. However, as the Council operated ANPR cameras at the time of the inspection phase of the inquiry without a valid legal basis, the DPC finds that the Council infringed section 71(1)(a) of the 2018 Act. Furthermore, the DPC finds that the Council infringed sections 71(1)(c) and 76(2) of the 2018 Act as the use of the ANPR camera technology is neither necessary nor proportionate to the purpose the Council seeks to achieve at Ballisodare Community Centre.

Findings

7.35 ***The DPC finds that the Council infringed sections 71(1)(a) of the 2018 Act by installing and operating an ANPR camera at the above-mentioned location without a clear legal basis to do so.***

7.36 ***The DPC finds that the Council infringed sections 71(1)(c) and 76(2) of the 2018 Act as the use of the ANPR camera technology is neither necessary nor proportionate to the purpose it seeks to achieve at Ballisodare Community Centre.***

4) Sharing live feed of CCTV cameras with An Garda Síochána

Regime: LED

Inquiry Report Issue: 1

7.37 At the time of the inspection on 1 April 2019, it was established that 'live' or 'real time' access to nineteen CCTV camera feeds had been given to An Garda Síochána at Sligo Garda Station. An Garda Síochána is a different controller. All nineteen cameras were authorised under section 38(3)(c) of 2005 Act. In the event that An Garda Síochána requires a copy of CCTV footage from any of these cameras, a Council official in the Housing Department performs the download. The Council understands

that An Garda Síochána use the CCTV feeds for law enforcement functions such as crime detection and investigation.

7.38 As the primary purpose for installing cameras was securing public order and safety and they were authorised under section 38(3)(c) of the 2005 Act, the applicable framework for assessing the legality of processing by the Council is the LED.

7.39 With regard to the rationale for the sharing of live CCTV feeds with Sligo Garda Station, the Council informed this inquiry by email on 14 May 2019 that at the time of the application for the CCTV scheme in 2006, live feeds to Sligo Garda Station were requested through the Joint Policing Committee.[18] Since an application for authorisation to the Garda Commissioner was made under section 38 of the 2005 Act in respect of the traffic management cameras and the Council accordingly was bound by section 38(7) of the 2005 Act to ensure that members of An Garda Síochána had access to the CCTV cameras, the DPC finds that the Council did not infringe section 71(1)(a) of the 2018 Act by sharing the live feed with Sligo Garda Station.

Findings

7.40 ***The DPC finds that the Council was obliged under section 38(7) of the 2005 Act, to ensure that members of An Garda Síochána had access at all times to the CCTV to which that authorisation relates and as such, has not infringed section 71(1)(a) of the 2018 Act by sharing the live feed of CCTV cameras with An Garda Síochána.***

5) Housing Department CCTV Cameras

Regime: LED

Inquiry Report Issue: 11

7.41 The Housing Department of the Council installed four CCTV cameras in the following areas: two cameras in the Caltragh Estate, one in Doorly Park (which was not working at the time the Inquiry Report was drafted) and one in Martin Savage Terrace (which was also not working at the time the Inquiry Report was drafted). For the purposes of this Decision, only the cameras which were functional at the time of the investigation are considered. The Council confirmed that none of these CCTV cameras have been authorised by the Garda Commissioner under section 38 of the 2005 Act. It was established on the date of the inspection that the two CCTV cameras in the Caltragh Estate were installed about one year previously because of a high level of anti-social behaviour in the estate. It was stated that the other two CCTV cameras at Doorly Park and Martin Savage Terrace were erected by the Architects

[18] Section 36 of the Garda Síochána Act 2005 provides for the establishment of joint policing committees in accordance with guidelines issued under section 35. Under section 38(1) the Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. Section 38(3) provides that authorisation may be provided to, inter alia, persons who meet the established criteria and whose application for authorisation in respect of a specified area within the administrative area of a local authority has been approved by the local authority after consulting with the joint policing committee for that administrative area.

Department of the Council in 2016 without any prior research having been done on the need for them.

7.42 When asked about the legal basis for the four CCTV cameras, the Council acknowledged that there was no legal basis for any of the cameras at the time. It indicated that it was considering seeking Garda Commissioner authorisation under section 38 of the 2005 Act in respect of the two CCTV cameras in the Caltragh Estate and it stated that it had no plans to repair the other two CCTV cameras which were not working at the time.

7.43 In the circumstances, the DPC considers that the Council does not have a legal basis for the processing of personal data by these CCTV cameras. In order to have such a legal basis, the Council would need to be in a position to demonstrate that the operation of the CCTV schemes was *necessary* in order to satisfy the legal obligation in question. This aspect of matters requires the carrying out of a data protection impact assessment or equivalent exercise. Based on the information provided to the inquiry, however, no such assessment or equivalent exercise was carried out by the Council prior to the deployment of CCTV cameras at the council estates listed above.

7.44 The DPC notes the Council's submission that CCTV cameras at Doorly Park and Martin Savage Terrace are no longer operational. The DPC further notes the Council's submission that it is seeking authorisation from An Garda Síochána under section 38 of the 2005 Act for operation of CCTV cameras at Caltragh Estate and that a DPIA will be carried out on these cameras once authorisation is received. However, as the Council processed personal data via CCTV cameras at the abovementioned sites without a valid legal basis at the time of the inspection, the DPC finds that the Council infringed section 71(1)(a) of the 2018 Act.

Findings

7.45 ***The DPC finds that the Council infringed section 71(1)(a) of the 2018 Act by not having a lawful basis to process personal data collected via CCTV cameras.***

b) Legal bases for the surveillance technologies employed for purposes other than for preventing, investigating, detecting or prosecuting crime

i) CCTV Cameras

1) Sligo Harbour CCTV cameras

Regime: GDPR

Inquiry Report Issue: 7

7.46 At the time of the inspection on 8 April 2019, there were fifteen CCTV cameras operated by the Council at Sligo Harbour. The Council stated that it uses these CCTV cameras for security purposes and to monitor the smooth running of Sligo Harbour. This includes, for example, ensuring that members of the public do not approach ships when they are in port and that when cargo is not obstructed while being transported to ships.

7.47 These CCTV cameras do not fall under the scope of section 38 of the 2005 Act and, therefore, they have not been authorised by the Garda Commissioner for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences.

7.48 The DPC must assess whether the Council has a legal basis to process personal data collected via these CCTV cameras for security purposes and to monitor the smooth running of Sligo Harbour. Article 5(1)(a) GDPR provides that personal data must be "...processed lawfully, fairly and in a transparent manner in relation to the data subject". In order to lawfully process personal data using CCTV cameras, a controller must satisfy at least one of the conditions in Article 6(1) of the GDPR. If the controller cannot do so, then its processing of personal data will be contrary to the requirement under Article 5(1)(a) of the GDPR to ensure that personal data is processed lawfully.

7.49 The Council did not cite any legal basis for the operation of these cameras.

7.50 The deployment of wide-spread video devices has significant potential to impact on the rights and freedoms of data subjects, while also, naturally, having the potential to bring significant benefits in the context of security and managing operations. In those circumstances, any lawful basis providing for the deployment of such technology must be sufficiently clear, precise and foreseeable as to limit the scope for arbitrariness in the deployment of the CCTV and to provide adequate protection to data subjects. A clearly defined lawful basis is also necessary to restrict the scope of the discretion of the Council to install CCTV cameras and to reduce the likelihood of arbitrary interferences with personal data subjects' right to the protection of their personal data.

7.51 The Council did not cite any legislative basis for processing personal data via CCTV cameras for security purposes and to monitor the smooth running of Sligo Harbour.

In these circumstances, the DPC finds that the Council cannot rely on Article 6 of the GDPR as its legal basis for processing personal data in this context.

7.52 The DPC notes the Council's submission that it has appointed a new Data Protection Officer and is in the process of updating its CCTV Policy, which will include a Privacy Notice in relation to the Harbour. The DPC also notes the Council's submission that it will seek to employ a suitable legislative basis for processing personal data collected via CCTV cameras at Sligo Harbour. However, as the Council did not rely on an appropriate legal basis at the time of the inspection phase of the inquiry, the DPC finds that it infringed Article 5(1)(a) GDPR.

Findings

7.53 **The DPC finds that the Council infringed Article 5(1)(a) of the GDPR by not having a lawful basis to process personal data collected via these CCTV cameras for the purposes of security and to monitor the smooth running of Sligo Harbour.**

c) Appropriate signage and general transparency
i) CCTV Cameras at Sligo Harbour

Regime: GDPR

Inquiry Issue: 7

7.54 The Inquiry Team noted that none of the signage in Sligo Harbour informed the public that the Council is the data controller nor did it provide contact details for the Council. Some signs gave no purpose for the use of CCTV. The sign which gave details of the purposes of CCTV was erected by Coleman Electronics. However, this sign was not sufficiently large to enable passing drivers to read it. One of the important considerations in terms of fair processing of personal data is an emphasis on transparency whereby any information and communication relating to the processing of personal data shall be easily accessible, easy to understand and that clear and plain language be used. This concerns, in particular, information provided to data subjects on the identity of the data controller, and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons and their right to obtain confirmation and communication of personal data concerning them which are being processed.

7.55 The DPC must assess whether the Council complied with its transparency obligations in connection with its collection and processing of personal data via these CCTV cameras in these circumstances.

7.56 Article 5(1) of the GDPR provides that personal data shall be:

> *processed lawfully, fairly and in a transparent manner in relation to the data subject...*

7.57 Article 12 of the GDPR expands on the requirements of the principle of transparency. Article 12(1) provides:

> *The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

7.58 Article 13 of the GDPR imposes an onus on the controller to provide this information at the time the personal data was obtained.[19]However, due to the volume of information that is required to be provided to the data subject it is permissible for the Council to adopt a "layered approach".[20]EDPB Guidelines provide that the most important information should be included in the first layer. For CCTV surveillance, the first layer normally will be a sign which is placed at a reasonable distance from where the monitoring occurs.[21]The rationale for this is to allow the data subject "*to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.*"[22]The content of the sign should include the details of the purposes of the processing, the identity of the controller and the existence of the rights of the data subject.[23]The contact details of the Data Protection Officer and a reference to the more detailed second layer of information and where and how to find it should also be included. [24]

7.59 The EDPB Guidelines also give details on what the content of the second layer should be:

> *The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer... In addition to these options, and also to*

---

[19] This is in contrast to the requirement of Article 13 of the LED which permits this information to be provided within a reasonable period after the controller obtains the personal data. This wording has been transposed in section 90 of the 2018 Act.

[20] EDPB Guidelines 3/2019 on processing of personal data through video devices (adopted on 10th July 2019) page 21.

[21] Ibid page 22.

[22] Ibid page 26.

[23] Ibid.

[24] Ibid.

make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.[25]

7.60 The DPC finds that the Council infringed Article 13(1) of the GDPR by failing to provide data subjects whose personal data was being collected via these CCTV cameras at Sligo Harbour with details of the identity of the controller, the contact details of the data protection officer, the purposes of the processing and details on where further information required to be given by Article 13 can be obtained[26] at the time the personal data was processed. The EDPB Guidelines make clear this information is required to be provided in the first layer of information. In other words, this information should be included on signs in the vicinity of the cameras, which the Council failed to do.

7.61 Article 13(3) of the GDPR also requires the Council to provide information to data subjects when the Council intends to use the personal data for a purpose other than that for which it was collected. As the Council provided the personal data to An Garda Síochána to be used by An Garda Síochána for law enforcement purposes, there was an obligation on the Council to notify the data subject of this intention at the time the personal data was collected. By not providing any information to data subjects regarding this secondary purpose in the signs, the DPC finds that the Council infringed Article 13(3) of the GDPR.

7.62 The DPC notes the Council's submission that it will install signage informing data subjects of the processing of personal data through CCTV cameras at Sligo Harbour so as to ensure compliance with Articles 13(1) and 13(3) of the GDPR. However, as this signage was not present at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed Articles 13(1) and 13(3) GDPR.

Findings

7.63 ***The DPC finds the Council infringed Articles 13(1) and 13(3) of the GDPR in failing to erect signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras at Sligo Harbour.***

---

[25] Ibid page 27.

[26] For example, by including a reference on signage to the relevant section of the Council's website or including a QR code to the website.

ii) ANPR Camera at Ballisodare Community Centre

Regime: LED

Inquiry Report Issue: 5

7.64 The Inquiry Team noted that one sign was in place to notify the public that CCTV was in operation at Ballisodare Community Centre. The sign was located on the wall of the Community Centre close to the CCTV cameras. The signage read as follows: *"CCTV In Operation. Protected by Power Right. 071 9145107"*. Power Right was the service provider that installed the CCTV system. The signage was deficient in that it did not indicate the purpose for which CCTV recording was taking place nor did it inform the general public that the Council was the data controller or give contact details for the data controller.

7.65 The DPC must assess whether the Council complied with its transparency obligations in connection with its collection and processing of personal data via these CCTV cameras in these circumstances.

7.66 The principle of fair processing of personal data is set out in section 71(1)(a) of the 2018 Act and the requirements in relation the data subject's right to certain information are set out at section 90(1) of the 2018 Act.

7.67 Given the level of data collection and data processing that is carried out by the ANPR camera at Ballisodare Community Centre in particular, the general public should be specifically informed that an ANPR camera is in operation at the site and the purpose for which it is used.

7.68 The absence of appropriate signage providing information to data subjects concerning the existence of the CCTV camera such as the identity and contact details of the controller, the contact details of the data protection officer of the controller (where applicable) and the purpose for which the personal data are intended to be processed or are being processed, amounts to a breach of the Council's obligations under sections 71(1)(a) and 90(1) of the 2018 Act.

7.69 The DPC notes the Council's submission that there are no longer CCTV cameras in operation at Ballisodare Community Centre. However, CCTV cameras were in operation at the time of the inspection phases of the inquiry and in the absence of appropriately worded and located signage and necessary information in respect of the processing of personal data for purposes related to law enforcement. The DPC therefore finds that the Council infringed sections 71(a) and 90(1) of the 2018 Act.

Findings

7.70 ***The DPC finds the Council infringed sections 71(1)(a) and 90(1) of the 2018 Act by failing to erect appropriately worded and located signage or by providing the necessary information to data subjects in respect of the processing of personal data***

collected via these CCTV cameras at Ballisodare Community Centre for purposes related to law enforcement.

iii) CCTV at Forthill Estate

Regime: LED

Inquiry Report Issue: 9

7.71 The Inquiry Team noted that there was no CCTV signage on the approach roads into the Forthill Estate to alert data subjects that their personal data would be processed by a CCTV system once they enter the areas covered by the focus of the cameras. The CCTV cameras at Forthill Estate were authorised by the Garda Commissioner in January 2007 under section 38(3)(c) of the 2005 Act. Section 2.5 of the "Code of Practice for Community Based CCTV Schemes" states: "*Signs should be placed so that the public are aware that they are entering an area which is covered by a CCTV system. These signs should be clearly visible and legible to members of the public*".

7.72 The principle of fair processing is set out in section 71(1)(a) of the 2018 Act and the requirements in relation to the data subject's right to certain information are set out at section 90(1) of the 2018 Act.

7.73 The absence of appropriate signage providing information to data subjects on the approach roads to Forthill Estate concerning the existence of CCTV cameras such as the identity and contact details of the controller, the contact details of the data protection officer of the controller (where applicable) and the purpose for which the personal data are intended to be processed or are being processed, amounts to a breach of the Council's obligations under sections 71(1)(a) and 90(1) of the 2018 Act.

7.74 The DPC notes the Council's submissions that it is in the process of erecting appropriate signage on the approach roads to Forthill Estate in order to comply with its obligations under sections 71(1)(a) and 90(1) of the 2018 Act. However, as this signage was not erected at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed sections 71(1)(a) and 90(1) of the 2018 Act.

Findings

7.75 ***The DPC finds the Council infringed sections 71(1)(a) and 90(1) of the 2018 Act by failing to erect appropriately worded and located signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras at Forthill Estate for purposes related to law enforcement.***

d) Joint controller agreement

i) CCTV Cameras: Live Feed to Sligo Garda Station and Joint Controller Status

Regime: LED

Inquiry Report Issue: 1

7.76 Section 79 of the 2018 Act provides:

> *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.*

7.77 Sligo Garda Station was at the time of the inspection in a position to access the live feeds from 19 CCTV cameras installed by the Council which were authorised under section 38(3)(c) of the 2005 Act. An Garda Síochána also used the feeds from these CCTV cameras for crime detection purposes and have access to the CCTV by way of a live feed to Sligo Garda Station. The DPC must assess whether the Council and An Garda Síochána acted as joint controllers in these circumstances.

7.78 Insofar as CCTV cameras have been authorised by the Garda Commissioner pursuant to section 38 of the 2005 Act, processing falls within a joint controller relationship and a joint controller agreement is required. Article 3(8) of the LED defines 'controller' as meaning '*the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*'.

7.79 Section 38 of the Garda Síochána Act 2005 provides that the Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences. Authorisation may be given to An Garda Síochána or to "*persons who meet the established criteria and whose application for authorisation in respect of a specified area within the administrative area of a local authority has been approved by the local authority after consulting with the joint policing committee for that administrative area.*" Section 38(7) of the 2005 Act provides An Garda Síochána with significant decision-making ability in relation to the personal data captured by the CCTV scheme including, among other things, the supervision and control of the recording of CCTV and the retrieval of any recorded information or data. The Garda Síochána (CCTV) Order 2006 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'.[27] Thus, the legislation provides that the Council must also undertake the role of controller.

7.80 Section 79 of the 2018 Act requires joint controllers to have an agreement in writing unless those responsibilities are determined by EU law or Member State law. Although the 2006 Order and section 38 of the 2005 Act give some details on the operation of the CCTV arrangement,[28] it does not provide for procedures on the respective responsibilities of the controllers to allow data subjects to exercise their rights under section 90 of the 2018 Act. A joint controller agreement governing this relationship is thus necessary. In this regard, the inquiry report noted that - at the time of carrying out the data protection audit - there was no arrangement in place that stated the respective roles and responsibilities of the Council and An Garda Síochána.

7.81 The responsibilities covered by section 79 of the 2018 Act 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 the 2005 Act nor the delegated legislation made pursuant to it. Thus, section 79 requires an agreement in writing between the Council and An Garda Síochána. 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 of the 2018 Act.

Findings

7.82 ***The DPC finds that the Council infringed section 79 of the 2018 Act by failing to implement an agreement in writing with An Garda Síochána detailing the issues required by that section.***

e) Security Measures for CCTV at Sligo Harbour and Cranmore

i) Accessibility of monitoring screens and recording equipment at Sligo Harbour and Cranmore

Regime: GDPR & LED

Inquiry Issue: 7, 13

7.83 The recording equipment and monitor in respect of CCTV cameras at Sligo Harbour are housed in the Security Office at Sligo Harbour. The Inquiry Team noted that there were no security controls in place, such as passwords, to restrict access to the recording systems or to the monitor in the Security Office. As a result, the CCTV system was open and the Council, as the data controller, had no means by which to identify who had accessed the system. The processing operations of the CCTV cameras at Sligo Harbour are governed by the GDPR.

---

[27] S.I. No. 289/2006 - Garda Síochána (CCTV) Order, 2006, s. 4(d)

[28] Ibid s. 4(e).

7.84 On 1 April 2019, the Inquiry Team carried out a physical inspection at the CCTV Control Room which is located in a property controlled by the Council in Cranmore. The feeds from sixteen CCTV cameras appear on the monitoring screen in the Control Room. The sixteen cameras comprise fourteen that were authorised by the Garda Commissioner under section 38(3)(c) of the 2005 Act as well as two cameras at Doorly Park and at Martin Savage Terrace. During the inspection, the Inquiry Team noted that there is no restriction on staff bringing smartphones, cameras or recording devices into the CCTV Control Room while they are on duty. In the absence of a policy and procedure to prohibit staff, or others, from bringing such devices into the Control Room a security vulnerability arose as images appearing on the monitoring screen could easily be recorded and removed from the CCTV Control Room in an unauthorised manner. The processing operations at Cranmore fall within the scope of the Law Enforcement Directive.

7.85 Under Article 5(1)(f) of the GDPR, personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Under Article 32(1) of the GDPR, a controller is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the rights and freedoms of data subjects.

7.86 Sections 71(1)(f) and 72 of the 2018 Act impose equivalent obligations in respect of security measures for processing operations falling within the scope of the Law Enforcement Directive.

7.87 The DPC notes the Council's submission that it is evaluating security measures for CCTV at Sligo Harbour, that it has restricted access to the monitoring centre, and that it has confined access to the camera recording hub to staff members with pre-authorised clearance and in possession of key cards. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed Articles 5(1)(f) and 32(1) GDPR.

7.88 The DPC also notes the Council's submission that it is in the process of erecting signage prohibiting the use of phones or other recording devices in the CCTV monitoring station at Cranmore. However, as this signage was not present at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed section 71(1)(f) and 72 of the 2018 Act.

Findings

7.89 ***The DPC finds that the Council infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to ensure the appropriate security of the CCTV monitoring screens at Sligo Harbour.***

7.90 ***The DPC finds that the Council infringed sections 71(1)(f) and 72 of the 2018 Act by failing to ensure the appropriate security of the CCTV monitoring screens at Cranmore CCTV Control Room.***

ii) Access Logs at Sligo Harbour and Cranmore

Regime: GDPR & LED

Inquiry Report Issue: 7, 14

7.91 The Harbour Master performed the function of downloading footage obtained from CCTV cameras at Sligo Harbour in the Security Office but no log of this downloading activity was recorded. This was a significant deficiency in terms of the need to create and maintain a comprehensive record of downloading activity that recorded the details of the specific footage downloaded, the date of the downloads and the purpose of the downloads. Moreover, the Council was uncertain whether these CCTV systems had the capability to identify, by time and date, access to the CCTV footage by staff.

7.92 Furthermore, during the inspection of the Cranmore CCTV Control Room it was established that the CCTV system had the capability to log all accesses to the system. However, users had not been trained on how to access or operate this functionality. As a result, no active auditing of the audit trails had been carried out to determine whether any unauthorised accesses to the CCTV system has occurred.

7.93 Article 24(1) of the GDPR obliges a data controller to implement appropriate technical and organisational measures for the purposes of ensuring that the processing of personal data for which it is responsible is performed in compliance with the GDPR and for demonstrating such compliance. Good governance requires robust controls and effective oversight including routine scrutinising of, as well as reporting to senior management on, the operation and use of CCTV systems. The practice of "auditing the audit trails" is a key governance measure. The absence of effective auditing results in a lack of regular reporting to senior management of key metrics such as the number of occasions on which the CCTV system was accessed and the number of footage downloads, among other things.

7.94 Article 32(1) of the GDPR requires a controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in connection with the processing of personal data including among other things, the ability to ensure the ongoing confidentiality and integrity of processing systems. The requirement to have an access log or an equivalent security measure can be derived from Article 32(1) of the GDPR. An access log is necessary to demonstrate compliance as there is no other way of verifying whether the purpose the data was processed for was a lawful one and if the person who sought the data was legally entitled to access it.

7.95 Sections 71(1)(f) and 72 of the 2018 Act impose equivalent obligations in respect of security measures for processing operations falling within the scope of the Law Enforcement Directive. Section 72(2) of the 2018 Act provides, inter alia, that a controller shall take all reasonable steps to ensure that persons employed by the controller, or other persons at the place of work concerned comply with the relevant technical or organisational measures.

7.96 The DPC notes the Council's submission confirming the use of paper logs and indicating that it is investigating the introduction of digital logs at Sligo Harbour in the near future. However, as appropriate measures were not present at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed Articles 24(1) and 32(1) of the GDPR.

7.97 The DPC notes the Council's submission confirming it is in the process of developing training for all relevant staff regarding in relation to its CCTV policy including the maintenance of logs at all CCTV monitoring sites. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed section 72(2) of the 2018 Act.

Findings

7.98 ***The DPC finds that the Council infringed Articles 24(1) and 32(1) of the GDPR by failing to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Sligo Harbour.***

7.99 ***The DPC finds that the Council infringed section 72(2) of the 2018 Act by failing to train staff to log accesses on the CCTV system at Cranmore CCTV Control Room.***

iii) Collection of personal data for other purposes at Sligo Harbour

Regime: GDPR

Inquiry Report Issue: 7

7.100 From an inspection of the field of vision captured by the CCTV cameras at Sligo Harbour it emerged that they capture images of people and vehicles that were going about their business beyond the Sligo Harbour area. The DPC must assess whether the Council has complied with its data minimisation obligations in these circumstances.

7.101 The principle of data minimisation is set down in Article 5(1)(c) of the GDPR and requires that personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."* Furthermore, data protection by design and by default requirements are set out in Article 25 of the GDPR. It is the DPC's view that routinely capturing and recording the images of members of the public who are going about their daily business beyond the areas of Sligo Harbour where this is not necessary for the purposes for which the CCTV cameras at Sligo Harbour are used (i.e. security and monitoring the smooth operation of the Harbour) amounts to excessive data collection.

7.102 The DPC notes the Council's submission that it is in the process of implementing measures to ensure that the processing of personal data via CCTV cameras at Sligo Harbour is compliant with Article 25 of the GDPR. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed Articles 5(1)(c) and 25 of the GDPR.

Findings

7.103 ***The DPC finds that the Council infringed Articles 5(1)(c) and 25 of the GDPR by failing to ensure that the processing of personal data via CCTV cameras at Sligo Harbour was not excessive to the purposes for which personal data are processed by the Council in these circumstances.***

f) Security Measures for Environment Department CCTV Cameras
Regime: LED

Inquiry Report Issue: 5

(i) Accessibility of Monitoring Screens at Ballisodare Community Centre, Lidl Site, Market Yard Site, Supermacs Site and the Cranmore Control Room

7.104 *Ballisodare Community Centre* – The Environment Department operated two CCTV cameras located at the entrance to the grounds of Ballisodare Community Centre. The cameras were physically located on the Community Centre building and they focused towards the bottle bank facility. The recording equipment and monitor for the CCTV cameras was kept in the canteen area of the Community Centre.

7.105 The monitoring screen and recording equipment was kept in an open space at the corner of the canteen. The canteen area was unlocked and it was, therefore, open to all users of the Community Centre while in use. The CCTV equipment was not kept in a locked cabinet which presented a security vulnerability. There were no security controls in place, such as passwords, to restrict access to the CCTV recording system or to the CCTV monitor. As a result, the CCTV system was open and the Council had no means by which to identify who has accessed the system. There was no restriction on users of the area in which the CCTV equipment is kept from bringing in smartphones, cameras or recording devices to this area while the monitoring screen was switched on. In the absence of a policy and procedures to prohibit staff, or others, from bringing such devices into the area, a security vulnerability arose as images appearing on the monitoring screen could easily be recorded and removed from the area in an unauthorised manner.

7.106 The Centre building is a County Council building that is leased to the Ballisodare community on a long-term lease. Caretakers, keyholders, etc. at Community Centre are not staff of the Council. Accordingly, the Council did not have sole control of the area in which the monitoring and recording equipment is kept in the Community Centre. As a result, the Council was reliant on the Ballisodare community to ensure

the safety of the equipment. This arrangement between the Council and the Ballisodare community posed a risk of unauthorised access by non-Council staff.

7.107 *Lidl Site* – The Environment Department operated one CCTV camera at the Council's bottle bank facility at the Lidl Site. The camera was physically located across the nearby roadway on a pole in the grounds of an ESB building. The recording equipment for the CCTV camera is kept in a small office that is used as a security and post room in the adjacent ESB building. The Inquiry Team noted that there were no restrictions on access by ESB staff to this office. Downloads of CCTV footage were undertaken by the Litter Warden in this open and unsecured environment. This presented a security vulnerability. There was no restriction on staff or others bringing in smartphones, cameras or recording devices to this office. In the absence of a policy and procedures to prohibit staff, or others, from bringing such devices into the office a security vulnerability arose as images appearing on the monitoring screen could easily be recorded and removed from the office in an unauthorised manner.

7.108 *Market Yard Site* – The Environment Department operated two CCTV cameras at the Council's bottle bank facility at the Market Yard site. The cameras were physically located on the Council building across from the nearby bottle bank facility. The recording equipment for the CCTV cameras was kept in a small room in the Roads Section in the County Council building. The Inquiry Team noted that there was no restriction on access by Roads Section staff to the room in which the recording equipment was kept. This presented a security vulnerability. There was no restriction on staff or others bringing in smartphones, cameras or recording devices to this room. In the absence of a policy and procedures to prohibit staff, or others, from bringing such devices into the room, a security vulnerability arose as images appearing on the monitoring screen could easily be recorded and removed from the room in an unauthorised manner. There were no security controls in place, such as passwords, to restrict access to the CCTV recording system or to the CCTV monitor. As a result, the CCTV system was open and the data controller had no means by which to identify who has accessed the system.

7.109 *Supermacs Site* – The Environment Department operated one CCTV camera at the bottle bank facility at the Supermacs site. The camera was physically located on the Supermacs building and it focused towards the bottle bank facility. The recording equipment and monitor for the CCTV camera was kept in the Supermacs management office within the Supermacs building.

7.110 While access to the Supermacs Management Office was restricted, this office was used by authorised Supermacs staff for several purposes unrelated with the CCTV recording equipment and monitor. Furthermore, Sligo County Council did not have sole control of the office in which the equipment is kept in the Supermacs building. As a result, it was reliant on Supermacs to ensure the safety of the recording equipment and to maintain overall security for the office. This arrangement between Sligo County Council and Supermacs placed the data controller, Sligo County Council,

in a position where it had an unsatisfactory level of control in respect of its CCTV recording and monitoring equipment.

7.111 There was no restriction on users of the Management Office bringing smartphones, cameras or recording devices into this office. In the absence of a policy and procedures to prohibit staff, or others, from bringing such devices into the office, a security vulnerability arose as images appearing on the monitoring screen could easily be recorded and removed from the office in an unauthorised manner.

7.112 Where a controller is processing personal data in circumstances where the LED regime applies, it is subject to security obligations set out in sections 71(1)(f), 72(1) and 78 of the 2018 Act. These require that personal data should be processed in a manner that ensures appropriate security of the personal data, including by implementation of appropriate technical or organisational security measures, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. It is the view of the DPC that by operating in a way where there were inadequate restrictions in place to prevent unauthorised access to the personal data collected via these CCTV systems, the Council infringed its obligations under sections 71(1)(f), 72(1) and 78 of the 2018 Act.

7.113 The DPC notes the Council's submission confirming that all CCTV cameras which were in operation at the nine bottle banks as specified at the time of the audit are no longer in operation and will not be resumed until the relevant provisions of the Circular Economy and Miscellaneous Provisions Act 2022 are commenced. The DPC also notes the Council's submission that it is in the process of evaluating all of its CCTV cameras to insure compliance with sections 71(1)(f), 72(1) and 78 of the 2018 Act and implementing security measures accordingly. However, appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed its obligations under sections 71(1)(f), 72(1) and 78.

Findings

7.114 ***The DPC finds that the Council infringed its obligations under sections 71(1)(f), 72(1) and 78 of the 2018 Act by failing to implement appropriate technical or organisational security measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data collected via the camera feeds from the CCTV systems at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site.***

(ii) Access Logs for CCTV Systems at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site

Regime: LED

Inquiry Report Issue: 5

7.115 For each of these CCTV systems, the Litter Warden performed the function of downloading footage but no log of this downloading activity was maintained. This was a significant deficiency in terms of the need to create and maintain a comprehensive record of downloading activity that records details of the specific footage downloaded, the date of download and the purpose for the downloads. Furthermore, the Council was uncertain whether these CCTV systems had the capability to identify, by time and date, when staff had accessed the CCTV footage. The DPC must assess whether the Council has complied with its security obligations under the 2018 Act in these circumstances.

7.116 Where the LED regime applies, section 75(1) places an obligation on the data controller to implement appropriate technical and organisational measures for the purpose of ensuring that the processing of personal data for which it is responsible is performed in compliance with Part 5 of the Act and for demonstrating such compliance. Furthermore, section 82(1) of the 2018 Act obliges a controller 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. Under section 82(2), the log must contain sufficient information to establish, among other things, the identification of the person who consulted the data, in so far as is possible.

7.117 It is the view of the DPC that by failing to operate a log system whereby, among other things, each individual who accessed the camera feeds could be identified, the Council infringed sections 75(1) and 82(2) of the 2018 Act.

7.118 The DPC notes the Council's submission confirming that all CCTV cameras which were in operation at the nine bottle banks as specified at the time of the audit are no longer in operation and will not be resumed until the relevant provisions of the Circular Economy and Miscellaneous Provisions Act 2022 are commenced. The DPC also notes the Council's submission that it is in the process of evaluating all of its CCTV cameras to insure compliance with sections 75(1) and 82(2) of the 2018 Act and implementing security measures accordingly. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed its obligations under sections 75(1) and 82(2) of the 2018 Act.

Findings

7.119 ***The DPC finds that the Council infringed sections 75(1) and 82(2) of the 2018 Act by failing to maintain a data log that recorded the identity of any individual who***

consulted personal data contained in the CCTV camera views and recorded footage from Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site.

(iii) Collection of personal data for other purposes at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site

Regime: LED

Inquiry Report Issue: 5

7.120 From an inspection of the field of vision captured by each of the CCTV cameras at these locations, it emerged that they captured images of people who were not using the relevant bottle bank facility. The Inquiry Team observed that cameras at these locations captured the following:

a. *Ballisodare Community* Centre – individuals visiting the Community Centre and the adjacent sports field and vehicles entering into and exiting the Community Centre and sports field;

b. *Lidl Site* – passers-by and people entering the Lidl carpark;

c. *Market Yard Site* – passers-by and vehicles using the adjacent roadway; and

d. *Supermacs Site* – individuals using the adjacent laundry facility and vehicles exiting Supermacs.

7.121 The DPC must assess whether the Council has complied with its data minimisation obligations in these circumstances.

7.122 Data processing under the LED regime must comply with the principle of data minimisation. This principle is reflected in section 71(1)(c) of the 2018 Act, which requires that *"data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed."*

7.123 The Council stated that purpose of the processing of personal data via these CCTV systems was to detect illegal dumping. Recording activities on private properties is not relevant to this purpose. Where the CCTV focuses on both private properties and public places, the DPC finds that the failure to use any privacy masking technology to eliminate or reduce the collection of personal data which is not required for the purposes for which this processing is carried out makes this processing excessive to its purpose.

7.124 Section 71(10) of the 2018 Act obliges the Council to be in a position to demonstrate, amongst other things, that the data collected are not excessive in relation to the purposes for which they are processed.

7.125 The DPC finds that the Council infringed section 76(2) of the 2018 Act by failing to implement technical and organisational measures which ensure that only necessary personal data under the designated purposes of the CCTV system is collected. An example of such a measure, is integrating privacy masking into CCTV cameras to

ensure that private dwellings are excluded from the scope of vision of the cameras. Furthermore, it is the view of the DPC that the requirements of section 76(2) of the 2018 Act were not met by the Council specifically with respect to the deployment of the CCTV system at the bottle bank facility at the Community Centre in the absence of any evidence to warrant the installation of such a system.

7.126 The DPC notes the Council's submission confirming that all CCTV cameras which were in operation at the nine bottle banks as specified at the time of the audit are no longer in operation and will not be resumed until the relevant provisions of the Circular Economy and Miscellaneous Provisions Act 2022 are commenced. The DPC notes that these provisions have subsequently commenced. The DPC also notes the Council's submission that it is in the process of evaluating all of its CCTV cameras to insure compliance with sections 71(1)(c), 71(10) and 76(2) of the 2018 Act and implementing security measures accordingly. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed its obligations under sections 71(1)(c), 71(10) and 76(2) of the 2018 Act.

Findings:

7.127 ***The DPC finds that the Council infringed sections 71(1)(c), 71(10) and 76(2) of the 2018 Act by failing to ensure that its processing of personal data via CCTV cameras at the relevant bottle bank facilities is not excessive to its purpose of preventing and detecting illegal dumping.***

g) Accountability

(i) Data Protection Impact Assessments for CCTV and ANPR cameras

Regime: LED

Inquiry Report Issue: 5, 4

7.128 Section 84(1) of the 2018 Act provides that:

> *Where having regard to its nature, scope, context and purposes, a type of processing, and in particular a type of processing using new technology, is likely to result in a high risk to the rights and freedoms of individuals, the controller that is proposing to carry out the processing shall conduct an assessment of the likely impact of the proposed processing operations on the protection of personal data (in this Part referred to as a "data protection impact assessment") prior to carrying out the processing.*

7.129 The Council did not provide the Inquiry Team with any evidence of a data protection impact assessment having been carried out in respect of the use of the CCTV and ANPR cameras at Ballisodare Community Centre in connection with the performance of the Council of its law enforcement functions in relation to the prevention, investigation, detection or prosecution of offences.

7.130 Under Article 35(4) of the GDPR, the DPC has specified circumstances in which a data protection impact assessment is mandatory where the GDPR applies, and these include systematically monitoring, tracking or observing individuals' location or behaviour. It is the view of the DPC that under section 84 of the 2018 Act, a data protection impact assessment is similarly required where surveillance technology will be used for systematically monitoring, tracking or observing individuals' behaviour in circumstances where the LED applies. The Council stated that it was in the process of or intended to conduct data protection impact assessments in respect of its use of CCTV cameras at these bottle bank facilities. However, no such assessments had been carried out at the time of the inspection phase of the inquiry.

7.131 The DPC notes the Council's submission that the CCTV and ANPR cameras are no longer in operation at Ballisodare Community Centre. However, as these cameras were in operation at the time of the inspection phase of the inquiry in the absence of a data protection impact assessment having been carried out, the DPC finds that the Council infringed its obligations under section 84 of the 2018 Act.

Findings

7.132 ***The DPC finds that the Council infringed section 84 of the 2018 Act by failing to carry out a data protection impact assessment for the deployment of CCTV and ANPR cameras at the bottle bank facilities at Ballisodare Community Centre.***

ii) Data protection policy on CCTV

Regime: LED and GDPR

Inquiry Report Issue: 8

7.133 Section 75(1) of the 2018 Act provides that (where the LED applies):

> *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.*

7.134 Section 75(3) further provides that the measures referred to in section 75(1) shall include the implementation of an appropriate data protection policy by the controller, where this is proportionate in relation to the processing activities carried out by the controller.

7.135 Similarly, Article 24(1) of the GDPR provides that (where the GDPR applies) the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR and Article 24(2) of the GDPR provides that, where proportionate, the

measures referred to in Article 24(1) shall include the implementation of appropriate data protection policies.

7.136 In connection with the Council's processing of personal data via CCTV cameras, both for law enforcement purposes and for security purposes, the Inquiry Team noted that, at the time of the inspection, the Council had not finalised or published on the Council website any CCTV policy. The Inquiry Team did note that at the time of the inspection, the Council had a CCTV policy in draft format dated October 2018.

7.137 The DPC is of the view that by failing to implement a finalised CCTV policy, the Council did not have appropriate technical and organisational measures in place for the purpose of ensuring compliance with the 2018 Act with respect to the deployment of CCTV cameras for law enforcement purposes, or compliance with the GDPR with respect to the deployment of CCTV cameras for security purposes.

7.138 The DPC notes the Council's submission that it is in the process of establishing a Data Protection Committee with CCTV oversight responsibilities and that it is updating its CCTV policy, which has been in place since 2019, to include reference to this Committee. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed Article 24 of the GDPR, interpreted in light of Article 24(2) of the GDPR and section 75(1) of the 2018 Act, interpreted in light of section 75(3) of the 2018 Act.

Findings

7.139 ***The DPC finds that the Council infringed Article 24 of the GDPR, interpreted in light of Article 24(2) of the GDPR and section 75(1) of the 2018 Act, interpreted in light of section 75(3) of the 2018 Act, by failing to have appropriate technical and organisational measures in place for the purpose of ensuring compliance with the GDPR and the 2018 Act, respectively.***

ii) Records of Processing Activities

Regime: LED and GDPR

Inquiry Report Issue: 10

7.140 A data controller is obliged to maintain records of processing activities for which it is responsible. This is a requirement under Article 30 of the GDPR and separately under section 81 of the Data Protection Act 2018 in respect of law enforcement activities. The data controller is obliged to cooperate with the supervisory authority and to make those records available to it on request.

7.141 On the inspection date of 1 April 2019, Sligo County Council was unable to produce records of processing activities under its GDPR functions or under its law enforcement functions. The Council confirmed that no such records had been created.

7.142 The DPC notes the Council's submission that operational Council CCTV camera locations have been digitally mapped and that an application is being developed to capture the location of all Council CCTV monitors. The DPC also notes the Council's submission that paper logs are being maintained and that the Council is investigating the development of digital logs. However, as appropriate measures were not in place at the time of the inspection stage of the inquiry, the DPC finds that Council infringed Article 30 of the GDPR and section 81 of the 2018 Act.

Findings

7.143 ***The DPC finds that the Council infringed Article 30 of the GDPR and section 81 of the 2018 Act by failing to create and maintain a record of processing activities with respect to each category of data processing activity undertaken by the Council.***

h) Data minimisation and data protection by design and default

i) Focus of CCTV cameras on private areas

Regime: LED

Inquiry Report Issue: 12

7.144 On 1 April 2019, the Inquiry Team carried out a physical inspection at the CCTV control room which is located in a County Council property in Cranmore. The feeds from sixteen CCTV cameras appeared on the monitoring screen in this Control Room. The sixteen CCTV cameras comprised fourteen that were authorised by the Garda Commissioner under section 38(3)(c) of the 2005 Act, in authorisations granted in 2007 and 2018, as well as two cameras at Doorly Park and at Martin Savage Terrace (referred to in Issue No. 11 above). The Inquiry Team examined the live views from the CCTV cameras that appeared on the monitoring screen.

a. From examining these live views it was apparent that some of the pan, tilt and zoom cameras did not automatically return to a pre-set position after the Council official had carried out monitoring activity at the monitoring screen. As a result, on the day of the inspection it was noted that some cameras had not been redirected to their original positions but instead they were left to focus in some instances directly on the front of houses, front gardens, front doors and bedroom windows. There were no privacy masking solutions - such as the blurring or blocking out of images - in operation when the cameras focused on these houses and therefore residents or members of the public in the area would not enjoy the level of privacy they would expect in this regard.

b. Apart from the aforementioned camera re-positioning issue, the Inquiry Team also noted that some CCTV cameras ordinarily focused in some instances into front gardens, back gardens and bedroom windows. One camera focused on a roadway with a clear view of a playground to the left. No privacy masking

solutions were used on the CCTV system. It was clear to the Inquiry Team, therefore, that in some instances CCTV cameras were focused on private spaces or spaces where members of the public would have an expectation of privacy and that insufficient measures had been taken to preserve the privacy of those spaces by means such as privacy masking.

7.145 Data processing under the LED regime must comply with the principle of data minimisation. This principle is reflected in section 71(1)(c) of the 2018 Act, which requires that *"data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed."*

7.146 The DPC notes the Council's submission that it is in the process of implementing technical measures at the CCTV Control Room in Cranmore. However, as appropriate measures were not in place at the time of the inspection phase of the inquiry, the DPC finds that the Council infringed section 71(1)(c) of the 2018 Act.

Findings

7.147 ***The DPC finds that at the time of the inspection, the Council failed to comply with section 71(1)(c) of the 2018 Act in capturing excessive data with the aforementioned CCTV cameras.***

i) Data Retention

i) Retention of personal data collected via CCTV camera at the Supermacs Site

Regime: LED

Inquiry Report Issue: 5

7.148 The Council had informed the Inquiry Team that footage recorded via the CCTV cameras operated by the Council is retained for 30 days. On examining the CCTV recording equipment at the Supermacs Site, the Inquiry Team found that footage dating back to October 2018 (a period of approximately six months) remained accessible on the system.

7.149 The principle of storage limitation is set out at section 71(1)(e) of the 2018 Act, which provides that personal data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed. The DPC is of the view that the Council infringed this requirement by retaining CCTV footage for 6 months after it was recorded via the CCTV camera at the Supermacs Site.

7.150 The DPC notes the Council's submission that it notes the DPC's intention to order the deletion of data retained for longer than 30 days and that staff training will include retention periods. However, as this was not the case at the time of the inspection

phase of the inquiry, the DPC finds that the Council infringed its obligations under section 71(1)(e) of the 2018 Act.

Findings

7.151 ***The DPC finds that the Council infringed its obligations under section 71(1)(e) of the 2018 Act in respect of the retention of personal data for longer than is necessary for purposes for which that data are processed via the CCTV cameras at the Supermacs Site.***

ii) Retention of personal data collected via CCTV camera at the Sligo Harbour

Regime: GDPR

Inquiry Report Issue: 7

7.152 The Inquiry Team was verbally informed that in line with the Council's draft CCTV policy, footage recorded via the CCTV cameras at Sligo Harbour was retained for 30 days. Searches conducted during the inspection revealed that footage dating back to 25 February 2019 (a period of 42 days) remained accessible on the system.

7.153 The principle of storage limitation is set out at Article 5(1)(e) of the GDPR, which provides that personal data shall be kept in a form that permits the identification of the data subject for no longer than is necessary for the purposes for which the data are processed. Therefore, the DPC is of the view that the Council infringed this requirement by retaining CCTV footage for this period without demonstrating a compelling need for same.

7.154 The DPC notes the Council's submission that it notes the DPC's intention to order the deletion of data retained for longer than 30 days and that staff training will include retention periods. However, as this was not the case at the time of the audit, the DPC finds that the Council infringed its obligations under Article 5(1)(e) of the GDPR.

Findings

7.155 ***The DPC finds that the Council infringed its obligations under Article 5(1)(e) of the GDPR in respect of the retention of personal data for longer than is necessary for purposes for which that data are processed via the CCTV cameras at Sligo Harbour.***

8. Decision on Corrective Powers

8.1 The DPC has set out above, pursuant to sections 111(1)(a) and 124(1)(a) of the 2018 Act, its decision to the effect that the Council has infringed the Articles of the GDPR and sections of the Data Protection Act 20018 listed in the following table.

Statutory Provision	**Instances of the Infringement**
S. 71(1)(a) of the 2018 Act	The DPC finds that the Council has infringed this section by:

	Unlawfully processing personal data via CCTV cameras at nine bottle bank facilities by the Environment Section of the Council; Unlawfully engaging in covert surveillance at the nine bottle bank facilities under the control of the Environment Department ; Unlawfully operating an ANPR camera at Ballisodare Community Centre; Unlawfully operating two cameras in the Caltragh Estate;
Ss. 75(1) and 75(3) of the 2018 Act	The DPC finds that the Council has infringed these sections by: Failing to implement a data protection policy in respect of when covert surveillance may be used by the Council.
S. 84 of the 2018 Act	The DPC finds that the Council has infringed this section by: Failing to carry out a data protection impact assessment in advance of using covert surveillance.
Ss. 71(1)(c) and 76(2) of the 2018 Act	The DPC finds that the Council has infringed these sections by: Engaging in excessive collection of personal data by use of an ANPR camera in a manner which was not necessary to perform its function at Ballisodare Community Centre.
Article 5(1)(a) GDPR	The DPC finds that the Council has infringed Article 5(1)(a) GDPR by: Not having a lawful basis to process personal data via CCTV Cameras at Sligo Harbour for the purpose of monitoring the operation of Sligo Harbour.
Articles 13(1) and 13(3) GDPR	The DPC finds that the Council has infringed these Articles by: Failing to erect signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras at Sligo Harbour.
Sections 71(1)(a) and 90(1)	The DPC finds that the Council has infringed these sections by: Failing to erect appropriately worded and located signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras at Ballisodare Community Centre for purposes related to law enforcement.
Sections 71(1)(a) and 90(1) of the 2018 Act	The DPC finds that the Council has infringed these sections by: Failing to erect appropriately worded and located signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras at Forthill Estate for purposes related to law enforcement.

Section 79 of the 2018 Act	The DPC finds that the Council has infringed this section by: Failing to implement an agreement in writing with An Garda Síochána detailing the issues required by that section in respect of cameras installed by the Council which were authorised under section 38(3)(c) of the 2005 Act.
Articles 5(1)(f) and 32(1) GDPR	The DPC finds that the Council has infringed these Articles by: Failing to ensure the appropriate security of the CCTV monitoring screens at Sligo Harbour.
Sections 71(1)(f) and 72 2018	The DPC finds that the Council has infringed these sections by: Failing to ensure the appropriate security of the CCTV monitoring screens at Cranmore CCTV Room.
Articles 24(1) and 32(1) GDPR	The DPC finds that the Council has infringed these Articles by: Failing to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Sligo Harbour
Section 72(2) of the 2018 Act	The DPC finds that the Council has infringed this section by: Failing to train staff to log accesses on the CCTV system at Cranmore CCTV Control Room.
Articles 5(1)(c) and 25 of the GDPR	The DPC finds that the Council has infringed these Articles by: Failing to ensure that the processing of personal data via CCTV cameras at Sligo Harbour is not excessive to the purposes for which personal data are processed by the Council in these circumstances.
Sections 71(1)(f), 72(1) and 78 of the 2018 Act	The DPC finds that the Council has infringed these sections by: Failing to implement appropriate technical or organisational security measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage of personal data collected via the camera feeds from the CCTV systems at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site.
Sections 75(1) and 82(2) of the 2018 Act	The DPC finds that the Council has infringed these sections by: Failing to maintain a data log that recorded the identity of any individual who consulted personal data contained in the CCTV camera views and recorded footage from Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site.
Sections 71(1)(c), 71(10) and 76(2) of the 2018 Act	The DPC finds that the Council has infringed these sections by: Failing to ensure that its processing of personal data via CCTV cameras at the relevant bottle bank facilities is not excessive to its purpose of preventing and detecting illegal dumping.
Section 84 of the 2018 Act	The DPC finds that the Council has infringed this section by:

	Failing to carry out a data protection impact assessment for the deployment of CCTV and ANPR cameras at the bottle bank facilities at Ballisodare Community Centre.
Article 24 of the GDPR interpreted in light of Article 24(2) of the GDPR and Section 75(1) of the 2018 Act, interpreted in light of Section 75(3) of the 2018 Act,	The DPC finds that the Council has infringed this Article and section by: Failing to have appropriate technical and organisational measures in place for the purpose of ensuring compliance with the GDPR and the 2018 Act, respectively.
Article 30 of the GDPR and Section 81 of the 2018 Act	The DPC finds that the Council has infringed this Article and section by: Failing to create and maintain a record of processing activities with respect to each category of data processing activity undertaken by the Council.
Section 71(1)(c) of the 2018 Act.	The DPC finds that the Council has infringed this section by: Failing to comply with the principle of data minimisation set out in section 71(1)(c) of the 2018 Act.
Section 71(1)(e) of the 2018 Act	The DPC finds that the Council has infringed this section by: The retention of personal data for longer than is necessary for purposes for which that data are processed via the CCTV cameras at the Supermacs Site.
Article 5(1)(e) of the GDPR	The DPC finds that the Council has infringed this Article by: The retention of personal data for longer than is necessary for which that data are processed via the CCTV cameras at Sligo Harbour.

8.2 Under sections 111(2) and 124(2) of the 2018 Act, where the DPC makes a decision (under sections 111(1)(a) and 124(1)(a)), it must, in addition, make a decision as to whether a corrective power should be exercised in respect of the controller or processor concerned and, if so, the corrective power to be exercised. The remaining question for determination in this Decision is whether or not any of those infringements merit the exercise of any of the corrective powers set out in Article 58(2) GDPR and Section 127(1) of the 2018 Act and, if so, which corrective powers.

8.3 Article 58(2) GDPR sets out the corrective powers that supervisory authorities may exercise in respect of non-compliance by a controller or processor. In deciding whether to exercise those powers, Recital 129 provides guidance as follows:

> ...each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case...

8.4 The applicable corrective powers in relation to any of the infringements falling under the LED/Part 5 of the 2018 Act are those set out at Section 127(1) of the 2018 Act.

8.5 Having carefully considered the infringements identified in this Decision, the DPC has decided to exercise certain corrective powers in accordance with sections 115 and 127 of the 2018 Act and Article 58(2) GDPR. In summary, the corrective powers that the DPC has decided are appropriate to address the infringements in the particular circumstances are:

I. Orders to the Council pursuant to Article 58(2)(d) GDPR and section 127(1)(d) of the 2018 Act to bring its processing operations into compliance with GDPR in the manner specified below;
II. Orders to the Council pursuant to Article 58(2)(f) GDPR and section 127(1)(f) imposing a temporary ban on processing operations in the manner specified below;
III. A reprimand to the Council pursuant to section 127(1)(b) of the 2018 Act in respect of its infringement of section 79 of the 2018 Act and
IV. Administrative fines for the infringements of 5(1)(c), 5(1)(e), 5(1)(f), 25, 30 and 32(1) GDPR.

8.6 Set out below are further details in respect of each of the corrective powers that the DPC has chosen to exercise and the reasons why it has decided to exercise them. The analysis in respect of whether an administrative fine is merited in light of the Council's infringements of the GDPR will be detailed subsequently in this Decision.

9. Orders to Bring Processing into Compliance and Temporary Ban on Processing

9.1 Article 58(2)(d) GDPR provides that a supervisory authority shall have the power

> to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period

9.2 Section 127(1)(d) of the 2018 Act provides that the Commission may

> order the controller or processor to bring processing into compliance with a relevant provision, in a specified manner and within a specified period

9.3 In circumstances where it has found that the processing at issue was not in compliance with the GDPR and the 2018 Act, the DPC considers it is appropriate to make orders pursuant to Article 58(2)(d) GDPR and Section 127(1)(d) of the 2018 Act. Therefore, the DPC orders the Council to bring the relevant processing (as further detailed below) into compliance with the GDPR and 2018 Act through implementing appropriate technical and organisational measures to ensure a level of security

appropriate to the risks. The Council must perform the necessary risk assessment to inform the measures that it must implement.

9.4 Article 58(2)(f) GDPR and Section 127(1)(f) of the 2018 Act provide that a supervisory authority shall have the power to *"impose a temporary or definitive limitation including a ban on processing."*

9.5 In light of the findings herein that the Council does not have a lawful basis to process certain personal data with the use surveillance technologies, including CCTV cameras, ANPR cameras, and covert cameras, the DPC imposes a temporary ban on the processing (as further detailed below).

9.6 It is the DPC's view that these orders are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR and 2018 Act. In this regard, the DPC acknowledges the Council's on-going remedial actions, as outlined in submissions throughout the Inquiry.

9.7 The orders that the DPC imposes are set out in the table below.

i. Lawful Bases for the Processing

No.	Action	Time Scale
1.	Environment Section CCTV Cameras at Bottle Banks used for law enforcement purposes Section 71(1)(a) of the 2018 Act The DPC finds no lawful basis for the Council's processing of personal data by means of CCTV cameras at sites of bottle banks. The DPC imposes a temporary ban on the Council's use of CCTV at these locations. This processing must not resume, unless, and until, there is a basis for it in EU or Member State Law.	The Council is required to confirm to the Data Protection Commission within 90 days of receiving the final Decision that the cameras are switched off, unless another legal basis for the processing can be pinpointed in the meantime.
2.	Use of Covert Cameras Section 71(1)(a) of the 2018 Act The DPC finds that there is no lawful basis for the Council's use of covert camera surveillance. The DPC imposes a temporary ban on the Council's use of covert camera surveillance. This processing must not resume, unless, and until, there is a basis for it in EU or Member State Law.	The Council is required to confirm to the Data Protection Commission within 90 days of receiving the final Decision that the cameras are switched off, unless another legal basis for the processing can be pinpointed in the meantime.
3.	Use of ANPR Camera to Detect Illegal Dumping Section 71(1)(a) of the 2018 Act The DPC finds that there is no lawful basis for the Council's use of an ANPR camera at Ballisodare Community Centre. The DPC imposes a temporary ban on the Council's use of the ANPR camera. This processing must not resume, unless, and until, there is a basis for it in EU or Member State Law.	The Council is required to confirm to the Data Protection Commission within 90 days of receiving the final Decision that the camera is switched off, unless another legal basis for the processing can be pinpointed in the meantime.
4.	Housing Department CCTV Cameras Section 71(1)(a) of the 2018 Act The DPC finds that there is no lawful basis for the Council's processing of personal data by means of CCTV cameras at the Caltragh Estate. The DPC imposes a temporary ban on the	The Council is required to confirm to the Data Protection Commission within 90 days of receiving the final Decision that the cameras are switched off, unless another legal basis for the processing can be pinpointed in the meantime.

	Council's use of CCTV at this location. This processing must not resume, unless, and until, there is a basis for it in EU or Member State Law.	
5.	Sligo Harbour CCTV Cameras Article 5(1)(a) GDPR The DPC finds that there is no lawful basis for the Council's processing of personal data by means of CCTV cameras at Sligo Harbour. The DPC imposes a temporary ban on the Council's use of CCTV at this location. This processing must not resume, unless, and until, there is a basis for it in EU or Member State Law.	The Council is required to confirm to the Data Protection Commission within 90 days of receiving the final Decision that the cameras are switched off, unless another legal basis for the processing can be pinpointed in the meantime.

ii. <u>Transparency</u>

No.	Action	Time Scale
6.	Sligo Harbour CCTV Cameras Articles 13(1) and 13(3) GDPR The DPC orders the Council to bring its processing by means of CCTV cameras into compliance with Article 13 of the GDPR by ensuring that all data subjects are provided with all the information required by Articles 13(1) and 13(3) of the GDPR. This must be achieved by installing signage in the vicinity of where the Sligo Harbour CCTV cameras are operating which gives data subjects advanced notice of the processing, the purposes of the processing and the identity of the controller.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at Sligo Harbour, prior to commencing processing this Order must be complied with.
7.	Ballisodare Community Centre Sections 71(1)(a) and 90(1) of the 2018 Act The DPC orders the Council to bring its processing by means of CCTV cameras (including the ANPR camera) into compliance with sections 71(1)(a) and 90(1) of the 2018 Act by ensuring that all data subjects are provided with all the information required by section 90(2) of the 2018 Act. This must be achieved by installing signage in the vicinity of where the Ballisodare	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at Ballisodare Community Centre, prior to commencing processing this Order must be complied with

	Community cameras are operating which gives data subjects notice of the processing, the purposes of the processing and the identity of the controller.	
8.	Forthill Estate Sections 71(1)(a) and 90(1) of the 2018 Act The DPC orders the Council to bring its processing by means of CCTV cameras into compliance with sections 71(1)(a) and 90(1) of the 2018 Act by ensuring that all data subjects are provided with all the information required by section 90(2) of the 2018 Act. This must be achieved by installing signage in the vicinity of where the Forthill Estate cameras are operating which gives data subjects notice of the processing, the purposes of the processing and the identity of the controller.	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.

iii. <u>Technical and organisational measures</u>

No.	Action	Time Scale
9.	Use of Covert Cameras Sections 75(1), 75(3) and 84 of the 2018 Act The DPC orders the Council to bring its processing into compliance with the 2018 Act by requiring the Council to implement a Data Protecting Policy which describes the Council's policy on covert cameras. The DPC orders the Council to bring its processing into compliance with the 2018 Act by conducting a data protection impact assessment in advance of recommencing processing of personal data by covert CCTV cameras.	If the Council identifies an appropriate legal basis and intends to recommence processing of personal data with covert cameras, prior to commencing processing these orders must be complied with.
10.	Security Measures for CCTV at Sligo Harbour Articles 5(1)(f) and 32(1) GDPR The DPC orders the Council to bring its processing operations into compliance with the	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at Sligo Harbour, prior to commencing

	2018 Act by implementing security measures so as to restrict access to the CCTV cameras to authorised persons only.	processing this Order must be complied with.
11.	Security Measures for CCTV at Cranmore CCTV Control Room Sections 71(1)(f) and 72 of the 2018 Act The DPC orders the Council to bring its processing operations into compliance with the 2018 Act by installing signs prohibiting staff from using their phones or other devices to take pictures or video or audio recordings of the CCTV monitoring screens in the monitoring centre to ensure compliance with section 71(1)(f) of the 2018 Act.	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.
12.	Collection of personal data for other purposes at Sligo Harbour Articles 5(1)(c) and 25 GDPR The DPC orders the Council to integrate appropriate technical and organisational measures as required by Article 25 GDPR in respect of the CCTV cameras which were subject to surveillance at Sligo Harbour. These technical and organisational measures could include privacy masking.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at Sligo Harbour, prior to commencing processing this Order must be complied with.
13.	Accessibility of Monitoring Screens at Ballisodare Community Centre, Lidl Site, Market Yard Site, and Supermacs Site Sections 71(1)(f), 72(1) and 78 of the 2018 Act The DPC orders the Council to implement measures at these locations to ensure only authorised persons have access to the CCTV cameras.	In respect of CCTV cameras, for which this decision has found the Council lacks a lawful basis, if the Council identifies an appropriate legal basis and intends to recommence processing personal data at the relevant sites, prior to recommencing processing this Order must be complied with. In respect of CCTV cameras for which the Council has a valid lawful basis the Council is required to implement this Order within 120 days of receiving the Final Decision at the relevant sites.

14.	Collection of personal data for other purposes at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site Sections 71(1)(c), 71(10) and 76(2) of the 2018 Act The DPC orders the Council to implement technical and security measures to ensure only the bottle bank facilities are captured by the CCTV cameras. Privacy masking technology could be a means of implementing this Order.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at these locations, prior to commencing processing this Order must be complied with.
15.	Focus of CCTV Cameras on Private Areas from CCTV Control Room in Cranmore Section 71(1)(c) of the 2018 Act The DPC orders the Council to integrate appropriate technical and organisational measures as required by section 76 of the 2018 Act in respect of the CCTV cameras which were subject to surveillance at Cranmore Control Room. These technical and organisational measures could include privacy masking and/or preventing manual control of the CCTV cameras by operators of the monitoring centres.	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.
16.	Access Logs at Sligo Harbour Articles 24(1) and 32(1) GDPR The DPC orders the Council to bring its processing into compliance with the GDPR by requiring the controller to ensure persons who access personal data leave their identity and purpose for which they accessed the data in the log book.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras at Sligo Harbour, prior to commencing processing this Order must be complied with.
17.	Access Logs at Cranmore CCTV Control Room Sections 72(2) of the 2018 Act The DPC orders the Council to implement training measures for the relevant staff to log	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.

	accesses on the CCTV system at Cranmore CCTV Control Room	
18.	Access Logs for CCTV Systems at Ballisodare Community Centre, Lidl Site, Market Yard Site and Supermacs Site Sections 75(1) and 82(2) of the 2018 Act The DPC orders the Council to maintain a data log of persons who have consulted the CCTV cameras at the prescribed locations.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras at these locations, prior to commencing processing this Order must be complied with.

iv. <u>Accountability</u>

No.	Action	Time Scale
19.	Data Protection Impact Assessments CCTV and ANPR cameras at Ballisodare Community Centre Section 84 of the 2018 Act The DPC orders the Council to conduct a data protection impact assessment in respect of use of surveillance at this location.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with the CCTV cameras at these locations, prior to commencing processing this Order must be complied with.
20.	Data Protection Policy on CCTV Article 24 GDPR and Section 75 of the 2018 Act The DPC orders the Council to implement a CCTV policy governing its use of surveillance technology	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.
21.	Records of Processing Activities Article 30 GDPR and Section 81 of the 2018 Act The DPC orders the Council to implement of record of its surveillance processing operations as required under Article 30 GDPR and Section 81 of the 2018 Act	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.
22.	CCTV Live Feeds to Sligo Garda Station Section 79 of the 2018 Act The DPC notes the Council's submission on 27 September 2019 to the Authorised Officers that the live feeds to Sligo Garda Station were being removed. However, in circumstances where section 38 of the 2005 Act obliges An Garda	N/A

	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 feed. Therefore, the DPC issues a reprimand to the Council on the basis of the infringement of section 79.	

v. <u>Data Retention</u>

No.	Action	Time Scale
22.	Retention of Personal Data collected via CCTV cameras at the Supermacs Site Section 71(1)(e) of the 2018 Act The DPC orders the Council to delete personal data that was retained for a longer period than 30 days.	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.
23.	Retention of personal data collected via CCTV camera at Sligo Harbour Article 5(1)(e) of the GDPR The DPC orders the Council to delete personal data that was retained for a longer period than 30 days.	The Council is required to confirm to the Data Protection Commission within 120 days of receiving the final Decision that this Order has been implemented.

9.8 The DPC's decision to impose the orders is made to ensure that full effect is given to the Council's obligations under the GDPR and 2018 Act. The DPC considers that these orders are appropriate, necessary and proportionate in view of ensuring compliance with the GDPR and 2018 Act.

9.9 The DPC considers that these orders are necessary to ensure that full effect is given to the Council's obligations in relation to the infringements outlined above.

9.10 The substance of these orders is the only way in which the defects pointed out in this Decision can be rectified, which is essential to the protection of the rights of data subjects. It is on this basis that the DPC takes the view that this power should be imposed.

9.11 Having regard to the non-compliance identified in this Decision, the DPC considers such orders are proportionate and are the minimum required to guarantee compliance in the future. The DPC is satisfied that the orders are necessary and proportionate.

10. Decision regarding the imposition of an Administrative Fine

10.1 Article 58(2)(i) of the GDPR provides that a supervisory authority shall have the power:

> to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.

10.2 The purpose of administrative fines is to strengthen the enforcement of the rules of the GDPR. Fines sanction non-compliance and seek to re-establish compliance with the GDPR.

10.3 The DPC is empowered solely to impose administrative fines in respect of infringements of the GDPR as opposed to infringements of the Law Enforcement Directive and related provisions of the Data Protection Act 2018. Accordingly, only the infringements of the GDPR in relation to Sligo Harbour are considered in this section.

10.4 As the DPC has identified infringements of the GDPR and 2018 Act above, the DPC will decide whether to impose administrative fines in respect of the infringements of the GDPR. In conducting this assessment, the DPC has had regard to Article 83 GDPR, which sets out 'General conditions for imposing administrative fines.' The DPC has also had regard to EDPB guidelines which are designed to ensure a harmonised approach to fining. These sets of guidelines include the EDPB's Guidelines on the calculation of administrative fines (the EDPB Fining Guidelines),[29] and the Article 29 Working Party's Guidelines on the application and setting of administrative fines (the A29WP Fining Guidelines),[30] which have been endorsed by the EDPB.

10.5 As a first step, the DPC will consider whether to impose a fine by applying the criteria set out in Article 83(2) GDPR. If the outcome of the assessment is that a fine should be imposed, then the DPC will proceed to calculate the amount, by reference to the criteria in Article 83(2) GDPR and by considering the other factors set out in Articles

[29] Guidelines 04/2022 on the calculation of administrative fines under the GDPR, version 2.1, adopted on 24 May 2023.
[30] WP253

83(1)-(9) that apply in this case. In particular, Article 83(1) GDPR requires fines to be effective, proportionate and dissuasive. These principles will inform the calculation of any fine that is imposed in this Decision.

a) Whether to impose an administrative fine

10.6 Article 83(2) GDPR states,

> Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following...

10.7 Article 83(2) goes on to list 11 criteria from (a) to (k) to be taken into account when deciding whether to impose an administrative fine. Those provisions are set out below where they are also applied to the infringements identified herein.

i) Article 83(2)(a) GDPR: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

10.8 Article 83(2)(a) requires consideration of the identified criterion by reference to 'the infringement' as well as 'the processing concerned.' The phrase **'the processing concerned'** in this Article 83(2) analysis should be understood as meaning all of the processing operations undertaken by the Council in respect of the CCTV operation at Sligo Harbour.

10.9 Considering next the meaning of 'infringement', it is clear from Articles 83(3)-(5), that 'infringement' means an infringement of a provision of the GDPR. Above, the Council was found to have infringed Articles 5(1)(a), 5(1)(c), 5(1)(e), 5(1)(f), 25, 30 and 32(1) GDPR. Thus, **'the infringement'**, for the purpose of the DPC's assessment of the Article 83(2) criteria, should be understood (depending on the context in which the term is used) as meaning an infringement of Articles 5(1)(a), 5(1)(c), 5(1)(e), 5(1)(f), 25, 30 and 32(1) GDPR. While each is an individual 'infringement' of the relevant provision, they all concern the processing concerned and, by reason of their common nature and purpose, are likely to generate the same, or similar, outcomes in the context of some of the Article 83(2) assessment criteria. Accordingly, and for ease of review, the DPC will assess all of these infringements simultaneously, by reference to the collective term **'infringements'** unless otherwise indicated.

10.10 As all findings of infringement of 5(1)(f) and 32(1) GDPR concern processing relating to CCTV operations at Sligo Harbour, the DPC will consider the Article 83 GDPR criteria for all of the identified wrongdoing in respect of Article 5(1)(f) and 32(1) jointly.

10.11 As all of the infringements relate to the processing concerned, the considerations and assessments set out below, save where otherwise indicated, should be understood as being assessments of the individual Article 83(2) criteria in the context of the infringements generally.

Taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them

10.12 This section will consider the nature, scope or purpose of the processing concerned, before considering the number of data subjects affected and the level of damage suffered by them.

10.13 The nature of the processing can include:

> the context in which the processing is functionally based (e.g. business activity, non-profit, political party, etc.) and all the characteristics of the processing.'[31]

10.14 Circumstances that can lead to supervisory authorities attributing more weight to this factor include

> where the purpose is to monitor, evaluate personal aspects or to take decisions or measures with negative effects for data subjects, where there is a clear imbalance between the controller and data subjects or where the processing involves children or other vulnerable data subjects.[32]

10.15 The nature of the processing relating to the infringements identified herein is the monitoring of the Harbour area via CCTV cameras to ensure its effective management. The DPC attaches greater weight due to the surveillance of data subjects and as the CCTV cameras also captured persons and vehicles that were not directly proximate to the Harbour area.

10.16 The scope of the processing is assessed

---

[31] EDPB Fining Guidelines [53.b.i].
[32] Ibid.

with reference to the local, national or cross-border scope of the processing carried out and the relationship between this information and the actual extent of the processing in terms of the allocation of resources by the data controller... The larger the scope of the processing, the more weight the supervisory authority may attribute to this factor.[33]

10.17 The scope of the processing relating to the infringements identified herein is moderate being confined to the Council's administration of a local area.

10.18 The purpose of the processing

> will lead the supervisory authority to attribute more weight to this factor. The supervisory authority may also consider whether the processing of personal data falls within the so-called core activities of the controller. The more central the processing is to the controller's or processor's core activities, the more severe irregularities in this processing will be. The supervisory authority may attribute more weight to this factor in these circumstances. There may be circumstances though, in which the processing of personal data is further removed from the core activities of the controller or processor, but significantly impacts the evaluation nonetheless (this is the case, for example, of processing concerning personal data of workers where the infringement significantly affects those workers' dignity).[34]

10.19 The purpose of the processing relating to the infringements identified herein is the management of Sligo Harbour. The purpose of the processing was determined by the Council in order to ensure the security and effective management of the Harbour and, in particular, to ensure the public did not approach the ships or the cargo therein.

10.20 In relation to the **number of data subjects**, the EDPB Fining Guidelines state,

> The higher the number of data subjects involved, the more weight the supervisory authority may attribute to this factor. In many cases, it may also be considered that the infringement takes on 'systemic' connotations and can therefore affect, even at different times, additional data subjects who have not submitted complaints or reports to the supervisory authority. The supervisory authority may, depending on the circumstances of the case, consider the ratio between the number of data subjects affected and the total number of data

[33] EDPB Fining Guidelines, [53].
[34] EDPB Fining Guidelines, [53].

subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.[35]

10.21 The number of data subjects affected by the infringements identified cannot be quantified. 15 CCTV cameras were installed at Sligo Harbour, some of which captured images of vehicles and persons beyond the Harbour, which would indicate that a sizeable number of data subjects may have been affected.

10.22 The **level of damage** is considered by reference to any harm suffered by data subjects or the 'extent to which the conduct may affect individual rights and freedoms.' The EDPB Fining Guidelines note:

> The reference to the 'level' of damage suffered, therefore, is intended to draw the attention of the supervisory authorities to the damage suffered, or likely to have been suffered as a further, separate parameter with respect to the number of data subjects involved (for example, in cases where the number of individuals affected by the unlawful processing is high but the damage suffered by them is marginal). Following Recital 75 GDPR, the level of damage suffered refers to physical, material or non-material damage. The assessment of the damage, in any case, be limited [sic] to what is functionally necessary to achieve correct evaluation of the level of seriousness of the infringement as indicated in paragraph 60 below, without overlapping with the activities of judicial authorities as tasked with ascertaining the different forms of individual harm.[36]

10.23 In this case, the possible damage that can result is of a moderate nature. This includes a heightened risk of unauthorised access to data subjects' personal data occurring. The storage of personal data when no longer necessary for their purpose increases the potential damage to data subjects in the event of a data breach and failure to maintain a data log prevents the supervisory authority and the controller itself from ascertaining if illicit access to personal data has occurred.

The nature of the infringements

10.24 The EDPB Fining Guidelines state that the nature of the infringement is 'assessed by the concrete circumstances of the case.' In this assessment, the supervisory authority may:

[35] EDPB Fining Guidelines [53.b.iv].
[36] EDPB Fining Guidelines [53.b.v].

review the interest that the infringed provision seeks to protect and the place of this provision in the data protection framework. In addition, the supervisory authority may consider the degree to which the infringement prohibited the effective application of the provision and the fulfilment of the objective it sought to protect.[37]

10.25 In line with the text of the GDPR, the nature, gravity and duration of the infringements are all assessed by taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.[38]

10.26 The infringement of Article 13 GDPR concerned the Council's failure to provide fundamental information to the data subjects regarding the CCTV surveillance including the:

-identity and contact details of the controller;[39]

-contact details of the data protection officer;[40] and

-legal basis for the processing.[41]

10.27 The nature of the infringements regarding Articles 5(1)(f) and 32(1) GDPR related to the Council's failure to implement adequate security measures to prevent unauthorised access to the recording equipment at the Security Office at Sligo Harbour.

10.28 The nature of the infringements of Articles 5(1)(c) and 25 GDPR concerns the failure by the Council to implement measures to ensure the CCTV cameras in Sligo Harbour only captured data that was relevant to their purposes. It emerged during the course of the investigation that the CCTV cameras at Sligo Harbour captured images of people and vehicles beyond the Sligo Harbour area which was a violation of the data minimisation principle.

10.29 The infringement of Article 30 GDPR relates to an accountability obligation. The Council failed to maintain records of processing activities under its GDPR functions.

10.30 The infringements of Article 5(1)(f) and 32 GDPR concerns a failure to keep access logs detailing the identity of the person who downloaded footage from the CCTV cameras at the Security Office in Sligo Harbour and when such downloading occurred.

---

[37] EDPB Fining Guidelines, [53.a]
[38] Article 83(2)(a).
[39] GDPR, Article 13(1)(a).
[40] GDPR, Article 13(1)(b)
[41] GDPR, Article 13(1)(c).

10.31 The infringement of Article 5(1)(e) GDPR concerns the Council's retention of personal data for longer than was necessary for purposes for which those data were processed via the CCTV cameras at Sligo Harbour.

The gravity of the infringements

10.32 The infringement of Article 13 GDPR in this case is of moderate gravity. The Council has not provided information to data subjects, which would notify them that their personal data would be processed by CCTV cameras in Sligo Harbour by the Council. The Council also failed to meet the requirements on controllers to provide data subjects with information which will permit them to exercise their rights under the GDPR.

10.33 The DPC considers the infringements of Articles 5(1)(f) and 32(1) GDPR to be of a moderate gravity. It was established that there was a lack of security controls in place to restrict access to the recording systems or to the monitor in the Security Office. The Council had no means of identifying who had accessed the system. The possible damage that could result is a heightened risk of unauthorised access to data subjects' personal data occurring. The Council's failure to maintain a data log prevents the supervisory authority and the controller itself from ascertaining if illicit access has occurred.

10.34 The DPC considers the infringement of Article 30 GDPR to be of moderate gravity as the CCTV cameras at Sligo Harbour are the only monitoring equipment falling within the scope of the GDPR.

10.35 The DPC considers the infringement of Article 5(1)(e) GDPR to be moderate in nature. The storage of personal data when no longer necessary for their purpose constitutes an interference with data subjects' rights and heightens potential damage to data subjects in the event of a data breach.

The duration of the infringements

10.36 In relation to the duration of an infringement, the EDPB Fining Guidelines state,

> a supervisory authority may generally attribute more weight to an infringement with longer duration. The longer the duration of the infringement, the more weight the supervisory authority may attribute to this factor.

10.37 The A29WP Fining Guidelines note that duration may be illustrative of:

a) wilful conduct on the data controller's part, or
b) failure to take appropriate preventive measures, or
c) inability to put in place the required technical and organisational measures.

10.38 The duration (as well as the nature and gravity of the infringements) is assessed taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.

10.39 In this case, the duration of the infringements of the GDPR regarding the processing commenced at the application of the GDPR on 25 May 2018. The infringements were ongoing for the entirety of the temporal scope in circumstances where the Council failed to implement appropriate measures required by those provisions for the entirety of that time frame. Therefore, for the purposes of deciding whether to impose an administrative fine, and for calculating the appropriate amount if applicable, the DPC proceeds on the basis that the infringements of Articles 5(1)(c), 5(1)(e), 5(1)(f), 25, 30 and 32(1) GDPR lasted at least from 25 May 2018 at least until the date of the inspection on 8 April 2019.

i. ***Assessment of Article 83(2)(a)***

10.40 Taking account of all of the factors assessed in this section, the DPC assesses the infringements to be moderate in gravity and of a moderate duration. The Council's failure to erect suitable signage to comply with its Article 13 GDPR obligations meant that data subjects would have been unaware of surveillance and unable to exercise their rights. The Council's failure to ensure that appropriate security safeguards were in place and its failure to maintain a data log contributed to a higher risk of unauthorised access to the personal data processed through the CCTV cameras at the Harbour. Furthermore, the infringements were moderate in duration being from the date of entry in force of the GDPR on 25 May 2018 until 8 April 2019. Taking account of all of the factors assessed in this section, the DPC assesses the ongoing infringements to have a moderate gravity and to be of a moderate nature.

ii. Article 83(2)(b) GDPR: the intentional or negligent character of the infringement;

10.41 The A29WP Fining Guidelines state,

> in general, intent includes both knowledge and willfulness in relation to the characteristics of an offence, whereas 'unintentional' means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law.

10.42 The EDPB Fining Guidelines state,

> The intentional or negligent character of the infringement (Article 83(2)(b) GDPR) should be assessed taking into account the objective elements of conduct gathered from the facts of the case. The EDPB highlighted that it is

generally admitted that intentional infringements, 'demonstrating contempt for the provisions of the law, are more severe than unintentional ones'. In case of an intentional infringement, the supervisory authority is likely to attribute more weight to this factor. Depending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral.

10.43 In this case, the DPC finds that the infringements indicate negligence on the part of the Council. The DPC considers that the infringement of Article 13 GDPR was of a negligent character as the Council did not provide an explanation for its failure to erect signage at the time of the inspection on 8 April 2019.

10.44 The DPC considers that the Council was negligent in failing to implement security measures pursuant to Articles 5(1)(f) and 32(1) GDPR when it ought to have been aware of same. The Council was culpable in failing to ensure that persons accessing the footage would be able to be identified at a subsequent point via access logs.

10.45 The DPC considers that the Council was negligent in in infringing its obligations in regard to Articles 5(1)(c) and 25 GDPR. A cursory examination of the range of view of the cameras would have alerted the Council to the fact that the scope of the view was excessive and that adequate security measures to counter this ought to have been implemented.

10.46 The DPC finds that the infringement of Article 30 GDPR was of a negligent nature. The maintenance of a record is a fundamental accountability requirement under the GDPR and the Council has failed to provide an explanation for why a record was not maintained.

10.47 The DPC considers that the infringement of Article 5(1)(e) GDPR was an infringement of negligent character as the Council should have been in a position to ensure compliance with the data retention period specified in its own CCTV policy.

iii. Article 83(2)(c) GDPR: any action taken by the controller or processor to mitigate the damage suffered by data subjects;

10.48 According to the A29WP Fining Guidelines,

> This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but

where they have done all they can to correct their actions when they became aware of the infringement.[42]

10.49 Regarding the infringement of Article 13 GDPR, the DPC considers the fact that the Council had erected a sign at Sligo Harbour, which adverted to the use of cameras as a mitigating factor of low weight in relation to the infringement of Article 13 GDPR. The DPC attributes it a low weight, as the Council was not designated as the controller on the sign and due to the use of small font, it was difficult to read for passers-by. Having regard to these actions for the purpose of Article 83(2)(c) GDPR, the DPC is of the view that the actions provided limited mitigation of the damage to data subjects.

10.50 The DPC can identify no mitigating factors in respect of the other infringements.

iv. Article 83(2)(d) GDPR: the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

10.51 The key question in relation to this provision is whether the Council 'did what it could be expected to do' given the nature, the purposes or the size of the processing, seen in light of the obligations imposed on it by the Regulation.[43]

10.52 As previously stated, the DPC considers that the Council was responsible for failing to implement security measures pursuant to Article 32(1) GDPR when it ought to have been aware of same. There was no restriction on staff bringing smartphones, cameras or recording devices into the CCTV Control Room while on duty which gave rise to a security vulnerability where images appearing on the monitoring screen could easily be recorded and removed from the CCTV Control Room in an unauthorised manner.

10.53 The DPC also considers that the Council was responsible in in infringing its obligations in regard to Article 25 GDPR in respect of the excessive range of view of the CCTV cameras in the Harbour area.

10.54 The DPC further considers the Council's responsible for the infringement of Article 32 GDPR by failing to ensure that persons accessing the footage would be able to be identified at a subsequent point via access logs.

10.55 Against this backdrop, the DPC considers that the Council holds a high degree of responsibility for the infringements and that the absence of sufficiently robust

[42] WP253 pg 12-13

[43] EDPB Fining Guidelines, [77].

technical and organisational measures must be deterred. It is clear that Council did not do 'what it could be expected to do' in the circumstances assessed in this Decision.

10.56 However, in circumstances where these factors form the basis for the finding of the infringement of Article 32 GDPR against the Council, these factors cannot be considered aggravating in respect of the infringements. Therefore, the DPC considers these factors to be neutral in the circumstances.

v. Article 83(2)(e) GDPR: any relevant previous infringements by the controller or processor;

10.57 In line with the EDPB Fining Guidelines, prior infringements are those already established before the decision is issued.

10.58 According to the A29WP Fining Guidelines, '[t]his criterion is meant to assess the track record of the entity committing the infringement.'

10.59 In this case, the Council has not been found to have committed any relevant previous infringements of the GDPR by the DPC or another supervisory authority. However, in the circumstances, this is of no mitigating value considering the brief period of time that passed prior to the inquiry commencing in June 2018.

vi. Article 83(2)(f) GDPR: the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

10.60 The extent to which the Council has cooperated with the inquiry is relevant to consider under this heading. The Council cooperated with the DPC during the course of the inquiry. The DPC does not regard this as a mitigating factor, however, as the Council has a statutory duty to cooperate under Article 31 GDPR.

vii. Article 83(2)(g) GDPR: the categories of personal data affected by the infringement;

10.61 By way of example of the categories that may be relevant to consider here, the A29WP Fining Guidelines suggest considering whether the infringements concern Article 9 or 10 data, whether the data are directly or indirectly identifiable, whether the data are encrypted or whether the processing involves data whose dissemination would cause immediate damage or distress to the individual.[44]

[44] A29WP Fining Guidelines, p14.

10.62 The personal data affected by the infringements was likely to have included recorded images of data subjects and their vehicles including registration details. The DPC does not consider it likely that any special category data, as outlined in Article 9 GDPR, or personal data relating to criminal convictions and offences, as outlined in Article 10 GDPR, would have been processed in the circumstances.

10.63 The DPC therefore considers that these factors are neither mitigating nor aggravating in the circumstances.

viii. Article 83(2)(h) GDPR: the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

10.64 According to the A29WP Fining Guidelines, this section can be used to consider whether the DPC became aware of the infringement 'as a result of investigation, complaints, articles in the press, anonymous tips or notification by the data controller.'

10.65 The A29WP Fining Guidelines also note that,

> The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor. Similarly, a data controller/processor who acted carelessly without notifying, or at least not notifying all of the details of the infringement due to a failure to adequately assess the extent of the infringement may also be considered by the supervisory authority to merit a more serious penalty i.e. it is unlikely to be classified as a minor infringement.[45]

10.66 The EDPB Fining Guidelines state

> In assessing this, particular weight can be given to the question whether, and if so to what extent, the controller or processor notified the infringement out of its own motion, before the infringement was known to the supervisory authority by – for instance – a complaint or an investigation[46]

And also that

[45] A29WP Fining Guidelines, p15.
[46] EDPB Fining Guidelines, [98].

> Where the infringement became known to the supervisory authority by, for instance, a complaint or an investigation, this element should also, as a rule, be considered as neutral.[47]

10.67 In the present inquiry, the DPC became aware of the infringements as a result of an own-volition inquiry. Therefore, the DPC considers this factor is neutral in the circumstances.

ix. Article 83(2)(i) GDPR: where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

10.68 The A29WP Fining Guidelines state

> As opposed to the criteria in (e), this assessment criteria only seeks to remind supervisory authorities to refer to measures that they themselves have previously issued to the same controller or processors 'with regard to the same subject matter'.

10.69 Corrective powers have not previously been ordered against the Council with regard to the subject-matter of this Decision.

x. Article 83(2)(j) GDPR: adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

10.70 This limb of Article 83(2) is not relevant for considering whether an administrative fine should be imposed in respect of the infringements of the GDPR in the present case.

xi. Article 83(2)(k) GDPR: any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

10.71 The DPC is of the view that there are no other aggravating or mitigating factors in respect of the infringements.

B. Decision on whether to impose an administrative fine

10.72 The decision to impose an administrative fine 'needs to be taken on a case-by-case basis, in light of the circumstances of each individual case.'[48]

---

[47] EDPB Fining Guidelines, [99].

[48] A29WP Fining Guidelines, p15.

10.73 Taking into account the assessment of the criteria at (a) to (k) above, the DPC has decided to impose an administrative fine. The infringements were considered above to be of a moderate seriousness by reference to their nature, gravity and duration in line with Article 83(2)(a). Under Articles 83(2)(b) and (g), the DPC found that the Council were negligent to a medium degree with respect to the infringements and that the infringements affected personal data which, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, in particular in relation to the information to be provided to a data subject under Article 13 GDPR. These are aggravating factors indicating that a fine should be imposed. The DPC considers that the measures adopted by the Council under Article 83(2)(c) to mitigate the damage to data subjects is mitigating to a low degree, and this factor does not negate the need for administrative fines in this Inquiry. The DPC considers that the factors assessed in relation to Articles 83(2)(d)-(k) are neither mitigating nor aggravating.

10.74 In order to ensure compliance with the GDPR, it is necessary to dissuade non-compliance. Depending on the circumstances of each individual case, dissuading non-compliance can entail dissuading the entity concerned with the corrective measures, or dissuading other entities carrying out similar processing operations, or both. Where a serious infringement of the GDPR occurs, a reprimand may not be sufficient to deter future non-compliance. In this regard, by imposing financial penalties, administrative fines are effective in dissuading non-compliance. This is recognised by the requirement in Article 83(1) GDPR for a fine, when imposed, to be effective, proportionate and dissuasive. Recital 148 GDPR acknowledges that, depending on the circumstances of each individual case, administrative fines may be appropriate in addition to, or instead of, reprimands and other corrective powers:

> In order to strengthen the enforcement of the rules of this Regulation, penalties, including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

10.75 While the reprimand will assist in dissuading the Council and other entities from similar future non-compliance, in light of the seriousness of the infringements, the DPC does not consider that the reprimand alone is proportionate or effective to achieve this end. The DPC finds that administrative fines are necessary to deter other future serious non-compliance on the part of the Council and other controllers or

processors carrying out similar processing operations. The reasons for this finding include:

a. Each infringement is moderate in nature and gravity, as set out above, pursuant to Article 83(2)(a) GDPR. Infringements of this nature and gravity must be dissuaded both in respect of the individual controller and in respect of other entities carrying out similar processing.

b. Regarding the infringements of Articles 5(1)(c), 13, 25 and 30 GDPR, the DPC considers that the Council's non-compliance with its obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of those data subjects by implementing appropriate measures.

Therefore, the DPC considers that an administrative fine is appropriate and necessary in order to dissuade non-compliance.

10.76 Having regard to the nature, gravity and duration of the infringements, the DPC also considers that administrative fines are proportionate in the circumstances in view of ensuring compliance. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

10.77 The DPC considers that the negligent character of the Council's infringements of Articles 5(1)(c), 13, 25 and 30 GDPR carries weight when considering whether to impose administrative fines, and if so, the amount of those fines. This negligence suggests that administrative fines are necessary to ensure that the Council directs sufficient attention to its obligations under Articles 5(1)(c), 13, 25 and 30 GDPR in the future.

10.78 The DPC considers that administrative fines would help to ensure that the Council and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

10.79 The DPC has also had regard to the mitigating actions taken by the Council. In light of the negligent character of the infringements, and the Council's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines are necessary in the circumstances to ensure future compliance.

10.80 Having considered the nature of the infringements of Articles 5(1)(f) and 32(1) GDPR and the fact there has been no ascertainable security breach arising, on the particular

circumstances of this case, the DPC has decided not to impose a fine for this infringement.

10.81 Having considered the infringement of Article 5(1)(a) GDPR, the DPC takes the view that the orders to bring processing into compliance above at paragraph 9.4 are the most appropriate exercise of corrective powers with respect to that infringement

b) Decision on the amount of the administrative fine

10.82 Above, it was determined that it was necessary to impose an administrative fine. This section calculates the amount of that fine, taking into account the methodology required to be applied by the EDPB Fining Guidelines, based on the assessments of the individual Article 83(2) GDPR criteria that are recorded above.

i) Article 83(3) GDPR

10.83 In accordance with Article 83(3) GDPR:

> If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

10.83 As outlined previously, the infringements identified herein all relate to the processing concerned, i.e. the CCTV programme of the Council and the technical and organisational measures at Sligo Harbour.

10.84 In respect of the interpretation of Article 83(3) GDPR, the DPC is mindful of its obligations of cooperation and consistency in, *inter alia*, Articles 60(1) and 63 GDPR. Accordingly, it is necessary to follow the EDPB's interpretation of Article 83(3) GDPR which was set out in the EDPB's binding decision 1/2021, which was made in relation to an inquiry conducted by the DPC.[49]

10.85 The relevant passages of the EDPB decision are as follows:

> *315.* All CSAs argued in their respective objections that not taking into account infringements other than the 'gravest infringement' is not in line with their interpretation of Article 83(3) GDPR, as this would result in a situation where WhatsApp IE is fined in the same way for one infringement as it would

[49] Inquiry IN-18-12-2.

be for several infringements. On the other hand, as explained above, the IE SA argued that the assessment of whether to impose a fine, and of the amount thereof, must be carried out in respect of each individual infringement found and the assessment of the gravity of the infringement should be done by taking into account the individual circumstances of the case. The IE SA decided to impose only a fine for the infringement of Article 14 GDPR, considering it to be the gravest of the three infringements.

316. The EDPB notes that the IE SA identified several infringements in the Draft Decision for which it specified fines, namely infringements of Article 12, 13 and 14 GDPR, and then applied Article 83(3) GDPR.

317. Furthermore, the EDPB notes that WhatsApp IE agreed with the approach of the IE SA concerning the interpretation of Article 83(3) GDPR. In its submissions on the objections, WhatsApp IE also raised that the approach of the IE SA did not lead to a restriction of the IE SA's ability to find other infringements of other provisions of the GDPR or of its ability to impose a very significant fine. WhatsApp IE argued that the alternative interpretation of Article 83(3) GDPR suggested by the CSAs is not consistent with the text and structure of Article 83 GDPR and expressed support for the IE SA's literal and purposive interpretation of the provision.

318. In this case, the issue that the EDPB is called upon to decide is how the calculation of the fine is influenced by the finding of several infringements under Article 83(3) GDPR.

319. Article 83(3) GDPR reads that if 'a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.'

320. First of all, it has to be noted that Article 83(3) GDPR is limited in its application and will not apply to every single case in which multiple infringements are found to have occurred, but only to those cases where multiple infringements have arisen from 'the same or linked processing operations'.

321. The EDPB highlights that the overarching purpose of Article 83 GDPR is to ensure that for each individual case, the imposition of an administrative fine in respect of an infringement of the GDPR is to be effective, proportionate and dissuasive. In the view of the EDPB, the ability of SAs to impose such deterrent

fines highly contributes to enforcement and therefore to compliance with the GDPR.

322. As regards the interpretation of Article 83(3) GDPR, the EDPB points out that the effet utile principle requires all institutions to give full force and effect to EU law. The EDPB considers that the approach pursued by the IE SA would not give full force and effect to the enforcement and therefore to compliance with the GDPR, and would not be in line with the aforementioned purpose of Article 83 GDPR.

323. Indeed, the approach pursued by the IE SA would lead to a situation where, in cases of several infringements of the GDPR concerning the same or linked processing operations, the fine would always correspond to the same amount that would be identified, had the controller or processor only committed one – the gravest – infringement. The other infringements would be discarded with regard to calculating the fine. In other words, it would not matter if a controller committed one or numerous infringements of the GDPR, as only one single infringement, the gravest infringement, would be taken into account when assessing the fine.

324. With regard to the meaning of Article 83(3) GDPR the EDPB, bearing in mind the views expressed by the CSAs, notes that in the event of several infringements, several amounts can be determined. However, the total amount cannot exceed a maximum limit prescribed, in the abstract, by the GDPR. More specifically, the wording 'amount specified for the gravest infringement' refers to the legal maximums of fines under Articles 83(4), (5) and (6) GDPR. The EDPB notes that the Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 state that the 'occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement'. The guidelines include an example of an infringement of Article 8 and Article 12 GDPR and refer to the possibility for the SA to apply the corrective measure within the limit set out for the gravest infringement, i.e. in the example the limits of Article 83(5) GDPR.

325. The wording 'total amount' also alludes to the interpretation described above. The EDPB notes that the legislator did not include in Article 83(3) GDPR that the amount of the fine for several linked infringements should be (exactly) the fine specified for the gravest infringement. The wording 'total amount' in this regard already implies that other infringements have to be taken into

account when assessing the amount of the fine. This is notwithstanding the duty on the SA imposing the fine to take into account the proportionality of the fine.

326. Although the fine itself may not exceed the legal maximum of the highest fining tier, the offender shall still be explicitly found guilty of having infringed several provisions and these infringements have to be taken into account when assessing the amount of the final fine that is to be imposed. Therefore, while the legal maximum of the fine is set by the gravest infringement with regard to Articles 83(4) and (5) GDPR, other infringements cannot be discarded but have to be taken into account when calculating the fine.

327. In light of the above, the EDPB instructs the IE SA to amend its Draft Decision on the basis of the objections raised by the DE SA, FR SA and PT SA with respect to Article 83(3) GDPR and to also take into account the other infringements – in addition to the gravest infringement – when calculating the fine, subject to the criteria of Article 83(1) GDPR of effectiveness, proportionality and dissuasiveness.

10.86 The impact of this interpretation is that administrative fines are imposed cumulatively, as opposed to imposing a fine for only the gravest infringement. The only applicable limit for the total fine imposed, under this interpretation, is the overall 'cap'. By way of example, in a case of multiple infringements, if the gravest infringement was one which carried a maximum administrative fine of 2% of the turnover of the undertaking, the cumulative fine imposed could also not exceed 2% of the turnover of the undertaking.

10.87 In this case, infringements were identified of Articles 5(1)(c), 13, 25 and 30 GDPR. The gravest infringement is that of Article 13 GDPR. The Council omitted to provide data subjects with fundamental information in this regard, such as its identity, the contact details of the Data Protection Officer or its lawful basis for processing in respect of the surveillance conducted at Sligo Harbour. A lack of transparency leads to a loss of control over personal data, which, in turn, results in damage to data subjects by restricting their ability to make decisions connected with the processing of their personal data.

ii) Categorisation of the infringements

10.88 As noted in the EDPB Fining Guidelines, Articles 83(4)-(6) GDPR indicate the degrees of seriousness accorded to different categories of. Those Guidelines note that

With this distinction, the legislator provided a first indication of the seriousness of the infringement in an abstract sense. The more serious the infringement, the higher the fine is likely to be.

10.89 The categorisation of the infringements under Articles 83(4) or (5) is a relevant consideration in assessing the seriousness of the infringements in this case.

iii) Seriousness of the infringement pursuant to Articles 83(2)(a), (b) and (g) GDPR

10.90 The EDPB Guidelines state that the factors assessed in relation to Articles 83(2)(a), (b) and (g) GDPR indicate the seriousness of the infringement.[50] These factors were assessed above. The guidelines also state that

> This assessment is no mathematical calculation in which the abovementioned factors are considered individually, but rather a thorough evaluation of the concrete circumstances of the case, in which all of the abovementioned factors are interlinked. Therefore, in reviewing the seriousness of the infringement, regard should be given to the infringement as a whole.[51]

10.91 Having regard to these factors as a whole, the infringements are of a medium level of seriousness. Under Article 83(2)(a) the infringements were found to be of a moderate nature and gravity. The infringements were also found to have been of moderate duration. The infringements affected personal data which, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, as assessed under Article 83(2)(g). The Council were also negligent to a medium degree with respect to the infringements, as assessed under Article 83(2)(b). Therefore, balancing these factors, the DPC considers that the infringements were of medium seriousness.

iv) Imposing an effective, dissuasive and proportionate fine

10.92 Article 83(1) GDPR requires a fine to be effective, proportionate and dissuasive in each individual case. As the guidelines also say that this doesn't 'dismiss a supervisory authority from the responsibility to carry out a review of the effectiveness, dissuasiveness and proportionality at the end of the calculation.'[52] Article 83(1) will be considered again at the end of this calculation.

---

[50] EDPB Fining Guidelines, [51].
[51] EDPB Fining Guidelines, [59].

[52] EDPB Fining Guidelines, [64].

v) Aggravating and mitigating circumstances

10.93 In relation to Article 83(2)(c), it was noted that the Council had erected a sign advising data subjects to the use of CCTV in the area. This is considered to be a mitigating factor of low weight.

10.94 In relation to Article 83(2)(d), the DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

10.95 In relation to Article 83(2)(e), it was noted that the Council did not have any previous relevant infringements. This factor is considered to be neither mitigating nor aggravating.

10.96 In relation to Article 83(2)(f), it was noted that the Council had cooperated with the DPC. As the Council has a general obligation to cooperate under Article 31 GDPR, this factor is considered to be neither mitigating nor aggravating.

10.97 In relation to Article 83(2)(h), it was noted that the manner in which the infringement became known to the DPC was via an own-volition inquiry conducted by the DPC. The DPC considers that this factor is neither aggravating nor mitigating in the circumstances.

10.98 In relation to Article 83(2)(i), it was noted that orders had not been previously ordered by the DPC[53] with regard to the same subject matter. This factor is considered to be neither mitigating nor aggravating.

10.99 In relation to Article 83(2)(j), it was found that there were no relevant approved codes of conduct or approved certification mechanisms for consideration. This factor is neither mitigating nor aggravating.

10.100 In relation to Article 83(2)(k), it was noted that there were no additional aggravating or mitigating factors for consideration.

10.101 Taking into account all of the matters arising for consideration as part of the individual assessments required to be carried out pursuant to Article 83(2) together with the requirements of the Fining Guidelines, as detailed above, the DPC imposes, in respect of the Council's infringement of Article 13 GDPR, a fine of **€12,000**. In

---

[53] Paragraph 101 of the EDPB Fining Guidelines says 'as opposed to Article 83(2)(e) GDPR, this assessment only refers to measures that supervisory authorities themselves have previously issued to the same controller or processor with regard to the same subject matter.'

respect of the Council's infringement of Article 5(1)(c) and 25 GDPR, the DPC imposes a fine of **€7,500**. In respect of the Council's infringement of Article 30 GDPR, the DPC imposes a fine of **€10,000**. Overall this amounts to a cumulative fine of **€29,500**.

vi) The relevant legal maximums for administrative fines

10.102 The DPC notes that the Council is a public body. Section 141(4) of the 2018 Act provides that any administrative fine that the DPC decides to impose on public bodies shall not exceed €1,000,000 unless the public body is one that acts as an undertaking within the meaning of the Competition Act 2002. As the administrative fines imposed in this Decision do not exceed that amount, it is not necessary for the DPC to determine whether the Council acts as an undertaking.

vii) Article 83(1) GDPR: Effectiveness, proportionality and dissuasiveness

Effectiveness

10.103 It is the DPC's view that for a fine to be effective, it must be large enough to have a significant effect on the controller or processor such that GDPR compliance, motivated by avoiding such fines in the future, becomes a factor in the entity's governance and management decision-making at the highest level. Furthermore, a sufficiently large fine is necessary to ensure that the fine is not a mere insignificant expense for the controller or processor concerned, and to ensure that the entity does not enjoy an unfair advantage by its ability to absorb even large fines for its infringements of the GDPR. The infringements concern surveillance of the public by a local authority. The personal data subject to processing, by their nature, carry a risk with regard to the fundamental rights and freedoms of data subjects, and should be subject to appropriate safeguards. In that context, the DPC considers that the level of the imposed fines ensure sufficiently effective fines, and no further adjustment is required.

Dissuasiveness

10.104 In order for a fine to be 'dissuasive', it must dissuade both the controller or processor concerned as well as other controllers or processors carrying out similar processing operations from repeating the conduct concerned. The DPC considers that the imposed fines are dissuasive for both. The DPC considers the monetary value of the fines to be sufficient to have such a deterrent effect.

10.105 Each infringement is moderate in nature and gravity as set out pursuant to Article 83(2)(a) GDPR. Infringements that are of a moderate nature and gravity must be strongly dissuaded both in respect of the individual controller and in respect of

other entities carrying out similar processing. Regarding the infringements of Articles 5(1)(c), 13, 25 and 30 GDPR, the DPC considers that the Council's non-compliance with its obligations under these Articles must be strongly dissuaded. Such dissuasive effect is crucial for protecting the rights and freedoms of data subjects by implementing appropriate measures. Therefore, the DPC considers that the administrative fines are appropriate and necessary in order to dissuade non-compliance.

10.106 The DPC considers that the negligent character of the Council's infringements of Articles 5(1)(c), 13, 25 and 30 GDPR carries weight when considering the amount of those fines. The level of negligence suggests that the administrative fines are necessary to ensure that the Council directs sufficient attention to its obligations under Articles 5(1)(c), 13, 25 and 30 GDPR in the future.

10.107 The DPC considers that the amounts of the administrative fines would help to ensure that the Council and other similar controllers take the necessary action to ensure the utmost care is taken to avoid infringements of the GDPR in respect of users' data.

10.108 The DPC has had regard to the fact that the Council had erected a sign at Sligo Harbour, which adverted to the use of cameras, and is a mitigating factor of low weight. In light of the negligent character of the infringements, and the Council's failure to comply with its obligations with regard to data protection, the DPC considers that dissuasive administrative fines to the extent imposed are necessary in the circumstances to ensure future compliance.

Proportionality

10.109 Proportionality is a principle of EU law that requires a measure to pursue a legitimate objective, be appropriate to attain that objective, and not go beyond what is necessary to achieve the objective. The objectives of the administrative fines in this case are to both re-establish compliance with the rules, and to sanction the Council's infringements. As regards the requirement for any fine to be necessary to these objectives, this requires the DPC to adjust the quantum of any fines to the minimum amount necessary to achieve the objectives pursued by the GDPR.

10.110 Having regard to the nature, gravity and duration of the infringements, the DPC considers that the administrative fines are proportionate in the circumstances in view of ensuring compliance. The Council's infringements of Articles 5(1)(c), 13, 25 and 30 GDPR suggested a lack of oversight and the potential failure to adhere to proper data protection principles. The DPC considers that the administrative fines

are proportionate to responding to the Council's infringements of Articles 5(1)(c), 13, 25 and 30 GDPR with a view to ensuring compliance in the future. The DPC considers that administrative fines do not exceed what is necessary to enforce compliance in respect of the infringements identified in this Decision.

11. Right of Appeal

11.1 This Decision is issued in accordance with sections 111 and 124 of the 2018 Act. Pursuant to section 150(5) of the 2018 Act, the Council will have the right to appeal against the Decision within 28 days from the date on which notice of this Decision is received by it. Furthermore, pursuant to section 142 of the 2018 Act, as this Decision includes a decision to impose an administrative fine, the Council will also have the right to appeal against that Decision within 28 days from the date on which notice of the Decision is given to it.

Decision-makers for the DPC:

Dr Des Hogan
Commissioner for Data Protection

Dale Sunderland
Commissioner for Data Protection