

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

DPC Case Reference:
06/SIU/2018


In the matter of Galway 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-Maker for the Data Protection Commission:



Helen Dixon

Commissioner for Data Protection

22 August 2023



**An Coimisiún um
Chosaint Sonraí
Data Protection
Commission**

**Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland**

Contents

1. Introduction.....	3
2. Summary of Factual Background.....	3
3. Topics arising in this Decision.....	7
4. Legal regime pertaining to the inquiry and the Decision	8
5. Data Controller	13
6. Personal Data	13
7. Analysis and findings	14
A. Legal bases for the surveillance technologies employed for the purposes of preventing, investigating, detecting or prosecuting crime.....	14
a) CCTV Cameras	14
b) ANPR Cameras.....	18
B. Legal bases for the surveillance technologies employed for purposes other than for preventing, investigating, detecting or prosecuting crime.....	19
a) ANPR Cameras.....	19
b) Body Worn Cameras.....	21
C. Appropriate signage and general transparency	23
a) CCTV Cameras	23
D. Technical and organisational measures.....	27
a) CCTV Cameras	27
E. DPO Access to CCTV Systems	32
F. Data minimisation and data protection by design and by default.....	33
a) CCTV Cameras	33
G. Accountability	37
a) CCTV Cameras	37
b) ANPR Cameras.....	38
H. Data Retention.....	40
8. Decision on Corrective Powers.....	42
9. Consideration of imposing an Administrative Fine	49
10. Right of Appeal	50

1. Introduction

- 1.1 This document is a decision (the '**Decision**') of the Data Protection Commission (the '**DPC**') in accordance with Sections 111 and 124 of the Data Protection Act 2018 (the '**2018 Act**'). I make this Decision having considered the information obtained in the separate own volition inquiry (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 Galway 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 10 May 2023 to afford the Council a final opportunity to make any further submissions, which it deemed necessary. I received submissions from the Council relating to the Draft Decision on 1 June 2023. I have given consideration to these submissions in advance of arriving at the final Decision. 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 I have 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 views set out in this Decision are based on the situations that pertained during the inspection phase of the inquiry itself (i.e. on 19 November 2018, 5 December 2018 and 19 February 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 exercises by the DPC of 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 will be required to comply with any corrective powers that are exercised in the final Decision and it will be open to this office to serve an enforcement notice on the Council in accordance with Section 133 of the 2018 Act.

2. Summary of Factual Background

- 2.1 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.

- 2.2 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.
- 2.3 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 systems, automated number plate recognition ('ANPR') technology, body worn cameras and any other technologies that may be used to monitor individuals for law enforcement purposes and/or for the purpose of preventing or detecting crime. 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.
- 2.4 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 16 July 2018.
- 2.5 On 2 November 2018, 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 whatever CCTV monitoring centre is in operation and they would need to inspect at least some of the CCTV camera sites.

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

On 19 November 2018

- This day-long inspection comprised a series of meetings, four in total, with the Data Protection Officer and other officials which took place at Áras an Chontae, Cnoc na Radharc, Gaillimh, followed by a physical inspection of the CCTV Viewing Room at Áras an Chontae.
- In attendance from Galway County Council for the first session were [REDACTED] (Data Protection Officer) and [REDACTED] (Vacant Homes Officer). [REDACTED], Director, paid a short courtesy visit at the start of the session.
- In attendance for the second session from Galway County Council were [REDACTED] (Data Protection Officer), [REDACTED] (Vacant Homes Officer) and [REDACTED] (Environmental Unit).
- In attendance for the third session from Galway County Council were [REDACTED] (Data Protection Officer), [REDACTED] (Vacant Homes Officer) and [REDACTED] (Health and Safety Officer).
- In attendance for the fourth session from Galway County Council were [REDACTED] (Data Protection Officer), [REDACTED] (Vacant Homes Officer), [REDACTED] (Tenancy Enforcement Officer), [REDACTED] (Buildings Inspector) and [REDACTED].
- The final session comprised an inspection by the Authorised Officers of the CCTV Viewing Room in Áras an Chontae. In attendance for this session from Galway County Council were [REDACTED] (Tenancy Enforcement Officer) and [REDACTED] (Buildings Inspector).
- Two Authorised Officers of the Data Protection Commission, [REDACTED] and [REDACTED] were in attendance throughout all sessions.

On 5 December 2018

- The first session of the day comprised a meeting at Áras an Chontae with the Data Protection Officer and staff from the Council offices in Ballinasloe. In attendance were [REDACTED] (Data Protection Officer), [REDACTED] (Vacant Homes Officer), [REDACTED] (C&E), [REDACTED] (Community Warden) and [REDACTED] (Assistant Staff Officer).
- The second session of the day comprised a meeting with the Data Protection Officer and staff from the Council offices in Tuam. In attendance were [REDACTED] (Data Protection Officer), [REDACTED] (Vacant Homes Officer), [REDACTED] and [REDACTED].

- The third session of the day comprised a further inspection by the Authorised Officers of the Viewing Room in Áras an Chontae. In attendance for this session from Galway County Council were [REDACTED] (Data Protection Officer) and [REDACTED] (Tenancy Enforcement Officer).
- The fourth session of the day comprised an inspection by Authorised Officers of CCTV cameras at Ballinasloe and the CCTV monitor and recording equipment in the Council offices in Ballinasloe. In attendance from Galway County Council was [REDACTED] (Community Warden).
- Two Authorised Officers of the Data Protection Commission, [REDACTED] and [REDACTED] were in attendance throughout all sessions.

On 19 February 2019

- The first session of the day comprised an inspection of CCTV cameras and recording equipment at Ros a Mhíl Community Centre, Connemara. In attendance were [REDACTED] (Environment Department), [REDACTED] (Environment Department) and [REDACTED] (Community Warden).
- The second session of the day comprised an inspection of CCTV cameras and recording equipment at An Poitín Stil public house at Inverin, Connemara. In attendance were [REDACTED] (Environment Department) and [REDACTED] (Environment Department).
- The third session of the day comprised an inspection of CCTV cameras at Cregmore GAA Club. In attendance were [REDACTED] (Environment Department) and [REDACTED] (Environment Department).
- Two Authorised Officers of the Data Protection Commission, [REDACTED] and [REDACTED] were in attendance throughout all sessions.

I have relied upon some of the information gathered from these inspections in the context of this Decision.

- 2.7 In addition to the completed Questionnaire No.1 which was received on 16 July 2018 the Council submitted a revised version of the completed Questionnaire No.1 on 15 November 2018. The Council also submitted a number of other documents to the DPC during the course of the inquiry.
- 2.8 The DPC received a CCTV Inventory on 4 December 2018. In summary, the inventory shows that as of the date of the inquiry, the Council deploys 56 CCTV cameras as follows:
- 47 cameras are active in various housing estates under the control of Galway County Council.
 - ANPR cameras operate in 2 housing estates in Tuam, namely Parkmore and Tirboy.
 - The Environment Department operate overt cameras at 9 bottle bank recycling centres. This Department (which was also referred to by the Council as the Environment Section and the Environment Unit but which, for consistency, is

referred to throughout this Decision as the Environment Department) also avails of covert technology as a means of surveillance.

- Body worn cameras are used by the Housing Department for the health and safety of staff.

2.9 Ultimately the Authorised Officers completed a final Inquiry Report which they submitted to me as Decision Maker on 4 February 2020. I am obliged to consider that Inquiry Report and reach final conclusions as to whether I identify infringements of data protection legislation. As set out above, this document is my Decision on this matter and includes the corrective powers that I propose to exercise arising from the infringements that are identified herein.

2.10 The findings made in this Decision include, amongst other things, findings concerning CCTV systems used by the Council which were authorised by the Garda Commissioner under Section 38 of the Garda Síochána Act 2005¹. 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 I am satisfied that the audit and inquiry were correctly conducted and that fair procedures were followed throughout including, but not limited to, notifications to the controller and an opportunity for the controller to comment on a draft inquiry report before it was submitted to me as Decision-Maker.

3. Topics arising in this Decision

3.1 This Decision considers the processing of personal data through a range of technologies, including CCTV systems, ANPR and body worn cameras. 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;
- (v) Waste Management Act 1996 (as amended); and

¹ CCTV cameras located at a number of housing estates including in Tuam (Parkmore, Tirboy, Bridge Court, Ahascragh and Crowe Street, Gort) and Ballinasloe.

(vi) Safety Health and Welfare at Work Act 2005 (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);
- (iii) Accountability and technical and organisational measures (including in relation to data minimisation); and
- (iv) Retention.

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 public authorities within the definition of ‘Competent authority’. It is well-established in statutory interpretation “that generally it is assumed that ‘or’ is intended to be used

disjunctively and the word 'and' conjunctively"². There is no basis for departing from the ordinary meaning of the word 'or' and it cannot have been the intention of the Oireachtas to bring about a conjunctive interpretation. The definition of 'competent authority' is not context specific. However, in order to constitute a 'controller' under part (a) of the definition, a competent authority must also determine the purposes and means of the processing, alone or jointly.

- 4.8 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*³ the Court of Justice of the European Union (the 'CJEU') considered the scope of the Data Protection Directive⁴, specifically the Directive's non-application to processing operations concerning the activities of the State in areas of criminal law.⁵ This case considered the inclusion of an individual's name on a list of persons that the Finance Directorate considered 'front-men' in company director roles. The data at issue were processed for the purpose of collecting tax and combating tax fraud. However, that data could be used in criminal proceedings if infringements were identified. The Court considered the purposes of the processing and held that the data were not collected:

*for the specific purpose of the pursuit of such criminal proceedings or in the context of State activities relating to areas of criminal law.*⁶

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

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

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

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

⁶ 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.

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 data must have been collected for the specific purpose of the pursuit of criminal proceedings. A similarly strict interpretation of the application of the LED and Section 70 of the 2018 Act is warranted. Thus, processing is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences only if the controller's reasons for the processing specifically reflects one or more of those purposes. It is not sufficient that the data could potentially also be used for law enforcement purposes if those purposes did not form part of the controller's specific reasons for processing.

Processing that falls under the GDPR

- 4.13 The GDPR is applicable to the Council's processing of personal data in relation to ANPR cameras where they are used for traffic management purposes and body worn cameras where they are used for health and safety purposes.
- 4.14 Here, the Council is not processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences. Although the data processed through the use of ANPR cameras and through body worn 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 these processing activities. Therefore, this processing is not for the specific purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties. The second limb of the test for the LED to apply is not satisfied and the GDPR is applicable.

Processing that falls under the LED

- 4.15 I find the LED is applicable to the remainder of the Council's processing operations that fall for consideration in this Decision. These processing operations include:
- i. The use by the Housing Department of CCTV cameras at numerous housing estates in Tuam and Ballinasloe for the purposes of preventing and detecting anti-social behaviour;
 - ii. The use by the Housing Department of ANPR cameras for the purposes of preventing and detecting anti-social behaviour; and
 - iii. The use by the Environment Department of CCTV cameras to prevent and detect illegal dumping in exercising the Council's criminal enforcement functions under the Litter Pollution Act 1997.

CCTV relating to Housing Estates and Bottle Banks

- 4.16 The purposes of the processing of personal data captured through CCTV cameras used by the Housing Department and the Environment Department of the Council 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.
- 4.17 The CCTV systems operated by the Council at bottle bank facilities, which have not been authorised under the Garda Síochána Act 2005, also fall under the LED. The Council is a controller of this personal data within part (a) of that definition in Section 69 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 the prevention and detection of 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.
- 4.18 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. 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 Garda Síochána Act 2005.

CCTV authorised under Section 38 of the Garda Síochána Act 2005

- 4.19 The CCTV systems operated by the Council pursuant to Section 38 of the Garda Síochána Act 2005 also fall under the LED. The Council is a 'Controller' within part (b) of that definition. The purposes and means of the processing are determined by Section 38 of the Garda Síochána Act 2005 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 CCTV⁷ and the systems that can be used.⁸

- 4.20 The Council is nominated as controller of this processing by Article 4(d) of the Garda Síochána (CCTV) Order 2006⁹, 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.
- 4.21 The sole or primary purpose of the Council's operation of this CCTV is statutorily determined in Section 38(1) of the Garda Síochána Act 2005 as "*securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences*". The second step in the test for applying the LED requires the processing to be for the purposes of the prevention, investigation, detection or prosecution of criminal offences. This is not a cumulative test, and any one of these purposes is sufficient to bring the processing under the Part 5. Therefore, even though the Council does not use this CCTV to investigate or prosecute criminal offences, it is clear that it records CCTV at these locations for the purpose of securing public order and safety by facilitating the prevention of criminal offences. This purpose alone is sufficient to bring the processing under Part 5 of the 2018 Act.
- 4.22 Where data are processed for one purpose and then used for another, if the purpose changes with that new use, the GDPR may become applicable. There is no evidence in the inquiry that suggests that the Council processed the CCTV data for any purpose that would exclude the application of Part 5 of the 2018 Act.

5. Data Controller

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

6. Personal Data

- 6.1 '*Personal data*' is defined under the GDPR as "*any information relating to an identified or identifiable natural person*".¹⁰ Section 69 of the 2018 Act implements a similar definition of '*Personal data*' under the LED.
- 6.2 This Decision concerns CCTV systems, ANPR cameras and body worn cameras. These devices capture visual images of individuals. It is possible to identify individuals from such images. Thus, the data processed by the devices includes "*personal data*".

⁷ Section 38(7) of the Garda Síochána Act 2005 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.

⁸ 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.

⁹ S.I. No. 289/2006 – Garda Síochána (CCTV) Order, 2006.

¹⁰ Article 4 GDPR.

7. Analysis and findings

- 7.1 The Authorised Officers identified a total of 16 issues in the course of the inquiry. I have considered each in turn and I have also considered the commonality of issues identified. Given that the Council is a controller in each and all of the issues identified, I will group my analysis and findings based on the commonality of issues arising.
- 7.2 Since the inquiry commenced, the Council has taken steps to address some of the issues identified in the inquiry. This Decision sets out findings as to whether infringements of the GDPR and/or the 2018 Act have occurred, by reference to the dates of the inspections conducted by the Authorised Officers (even if those infringements have since been addressed), or are occurring. Therefore, it is acknowledged that some of the issues leading to the findings in this Decision may since have been addressed by the Council.

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

a) CCTV Cameras

i) Environment Department: Legal Basis for CCTV Cameras at bottle banks to detect illegal dumping

Regime: LED

Inquiry Report Issue: 7, 8

- 7.3 CCTV cameras are operated by the Environment Department of the Council at five bottle bank facilities as well as at locations such as bogs and remote rural areas for the purposes of facilitating enforcement of the Litter Pollution Act 1997. As the Council is the investigation and prosecution authority in respect of offences under the Litter Pollution Act 1997, this activity falls under the LED. Furthermore, for law enforcement purposes, the Environment Department occasionally engages the services of CU Security to conduct covert surveillance. I must assess whether the Council has 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 relies on these functions as a lawful basis for these CCTV systems on the basis that the CCTV systems are necessary for the performance of those functions.
- 7.5 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*¹¹, the Supreme Court interpreted the Irish legislation¹² that implemented Directive 2003/4/EC.¹³ The definition of ‘public authority’ in the Irish legislation contained additional paragraphs to that in the Directive. The Court held, in relation to interpreting legislation introduced implementing an international treaty:

*this specific obligation undertaken by Ireland as a member of the EU requires that the courts approach the interpretation of legislation in implementing a directive, so far as possible, teleologically, in order to achieve the purpose of the directive.*¹⁴

- 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.*¹⁵

- 7.8 In *Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission*¹⁶, 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’¹⁷. This case concerned the duty to disapply national legislation that is contrary to EU law. The duty to interpret national legislation teleologically to achieve the purpose a Directive is equally applicable to all Member State bodies.

- 7.9 Section 71 of the 2018 Act must be interpreted so far as possible, teleologically, in order to achieve the purpose of the LED. It is a clear purpose of the LED that

¹¹ *National Asset Management Agency -v- Commissioner for Environmental Information* [2015] IESC 51.

¹² Statutory Instrument No. 133 of 2007.

¹³ 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.

¹⁴ *Ibid* At paragraph 10.

¹⁵ *Ibid* at paragraph 11.

¹⁶ 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).

¹⁷ At paragraph 39.

processing that falls within its scope must be based on Union or Member State law. Article 8 of the Law Enforcement Directive provides for the lawfulness of processing:

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

7.10 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. 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 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*¹⁸ the court held (at paragraph 91):

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

7.14 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 Council's use of CCTV footage cannot lawfully be based on the Litter Pollution Act 1997 or the Waste Management Act 1996. I have carefully considered the full range of legislation and the Council's use of CCTV to detect and take enforcement action against those engaged in littering.

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

7.17 Therefore, I find that the processing of this personal data is not lawful and infringes Section 71(1)(a) of the 2018 Act.

¹⁸ Case C-362/14, Maximilian Schrems v Data Protection Commissioner, judgment of 6 October 2015 (ECLI:EU:C:2015:650).

7.18 Although 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, I note that in the most recent update available on Irish Statute Book at the time of issuing this Decision,¹⁹ it stated that sections 5 – 25 and 27 – 40 of the Act have not yet been commenced. I accordingly cannot take these provisions into account in assessing whether the Council has 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 pinpointing the legal basis it relies upon for processing.

7.19 I welcome 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 the inquiry was conducted I find the Council has infringed Sections 71(1)(a) of the 2018 Act.

Findings

7.20 I find that the Council infringed Section 71(1)(a) of the 2018 Act by unlawfully processing data from CCTV cameras at the relevant bottle bank facilities.

ANPR Cameras

Housing Department: Legal Basis for ANPR Cameras to detect anti-social behaviour

Regime: LED

Inquiry Report Issue: 11

7.21 As part of a CCTV upgrade the Council installed ANPR cameras in two housing estates in Tuam, namely Parkmore and Tirboy, as a wider estate enhancement scheme in 2017 to include a traffic management system and to detect possible anti-social behaviour events.

7.22 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 involve the processing of personal data. I must assess whether the Council has a legal basis to process personal data collected via these ANPR cameras in these circumstances.

7.23 The lawful basis relied upon by the Council for the operation of these ANPR cameras to detect possible anti-social behaviour events is Section 71(2)(a) of the 2018 Act. In order to lawfully process personal data for law enforcement functions, a controller must satisfy the requirements of Section 71(2) of the 2018 Act, which provides that

¹⁹ See < https://www.irishstatutebook.ie/eli/isbc/2022_26.html>.

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.

7.24 A test of necessity, by reference to the performance of a function which has a legal basis in the law of the EU or Ireland, should have been undertaken prior to the installation of ANPR or other CCTV cameras by means of a data protection impact assessment or by another equivalent exercise. The Inquiry Team found no evidence of a proportionality test or data protection impact assessment or an equivalent exercise having been carried out to test the necessity for the use by the Council of ANPR cameras for any of its law enforcement functions. Without having conducted such an assessment or exercise, either before or since the installation of the ANPR cameras, there is no evidence that the data processing by means of ANPR or other CCTV cameras is *necessary* for the performance of a function for the purposes of the prevention, investigation, detection or prosecution of criminal offences, which has a legal basis in the law of the EU or Ireland.

7.25 I welcome the submission made by the Council in response to the Draft Decision advising that ANPR cameras were removed from the Parkmore and Tirboy estates in February 2022. However as the ANPR cameras were in operation at the time the inquiry was conducted I find the Council has infringed Sections 71(2)(a) of the 2018 Act.

Findings

7.26 *I find that the Council infringed Section 71(2)(a) of the 2018 Act by processing data from ANPR cameras at the above-mentioned locations without a clear legal basis to do so.*

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

a) ANPR Cameras

i) Legal basis for ANPR Cameras for traffic management:

Regime: GDPR

Inquiry Report Issue: 11

7.27 As part of a CCTV upgrade the Council installed ANPR cameras in two housing estates in Tuam, namely Parkmore and Tirboy, as a wider estate enhancement scheme in 2017 to include a traffic management system and to detect possible anti-social behaviour events.

7.28 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 involve the processing of personal data. I must assess whether the Council has a legal basis to process personal data collected via these ANPR cameras in these circumstances.

- 7.29 *Kopp v Switzerland* is an authority for the proposition that legal bases for surveillance technologies must be particularly precisely worded.²⁰ The lawful basis relied on by the Council for the operation of these cameras is Article 6(1)(e) of the GDPR.
- 7.30 In order for a valid legal basis to exist for such processing under Article 6(1)(e) it would be necessary for the legislature to specifically grant power to the local authority to carry out such processing in a manner which is clear, precise and foreseeable for data subjects subject to the processing. This can be garnered from interpreting Article 6(1)(e) in light of Article 6(3) and Recital 41 GDPR. These latter provisions envisage that any legal basis relied on for processing carried out pursuant to Article 6(1)(e) should be clear precise and foreseeable.
- 7.31 For example, it is important that the legal basis includes matters such as stating the type of data that will be processed, the conditions governing the processing, the means of processing the data and the purpose of the processing, as these will be of assistance in ensuring that the basis meets the requirements of clarity, precision and foreseeability. The case law on the standards of clarity, precision and foreseeability can be summarised as requiring that the Member State law must afford adequate legal protection against arbitrariness and bring clarity to the scope of any discretion conferred on public authorities by that law. This assessment will necessarily depend on the type of processing in question and the legal bases being relied upon. However, the deployment of wide-spread ANPR 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 traffic management. 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 ANPR cameras and to provide adequate protection to data subjects. This is also necessary to restrict the scope of the discretion of the Council to install ANPR cameras and to reduce the likelihood of arbitrary interferences with personal data subjects' right to protection of their personal data.
- 7.32 I accept that the Council has a function in relation to the management of traffic in the county of Galway. However, I must assess whether the Council has a legal basis

²⁰ 25 March 1998, § 55, Reports of Judgments and Decisions 1998-II paragraph 72. See also *Zakharov v Russia* 47143/06 paragraph 229; *Centrum för Rättvisa v Sweden* (2019) 68 E.H.R.R. 2 paragraph 101; and *Big Brother Watch v United Kingdom* 58170/13 62322/14 24960/15 (Grand Chamber) paragraph 333.

to process personal data collected via ANPR cameras in carrying out its traffic management function which addresses the requirements set out above. In order to lawfully process personal data using ANPR cameras, a controller must satisfy at least one of the conditions in Article 6 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.

- 7.33 The Council referred in its submissions to Sections 66 and 67 of the Local Government Act 2001 as its legislative basis for using ANPR cameras for traffic management purposes. While Section 66 empowers a local authority to *“take such measures, engage in such activities or do such things in accordance with law ... at is considers necessary or desirable to promote the interests of the local community”*, it is noteworthy that any such action taken must be *“in accordance with law”*. It is also noteworthy that Sections 66 and 67 of the Local Government Act 2001 do not specifically grant a local authority the power to carry out processing of personal data via ANPR cameras (or any similar technology) in a manner which is clear, precise and foreseeable. In these circumstances, I find that Sections 66 and 67 of the Local Government Act 2001 do not provide the Council with a legislative basis to use ANPR cameras for traffic management purposes in a manner that addresses the requirements of Article 6(1)(e) of the GDPR, interpreted in light of Article 6(3) and Recital 41 of the GDPR and applicable case law.
- 7.34 As the Council has failed to identify any legislation which expressly permits the Council to conduct surveillance of data subjects with ANPR technology, I find that the Council does not have a lawful basis to operate CCTV cameras with ANPR facilities for traffic management purposes.
- 7.35 I welcome the submission made by the Council in response to the Draft Decision advising that ANPR cameras were removed from the Parkmore and Tirboy estates in February 2022. However, as the ANPR cameras were in operation at the time the inquiry was conducted I find the Council has infringed Article 5(1)(a) GDPR.

Findings

- 7.36 ***I find that the Council infringed Article 5(1)(a) GDPR by not having a lawful basis to process personal data with ANPR cameras for the purposes of traffic management.***

b) Body Worn Cameras

i) Body Worn Cameras: Legal Basis

Regime: GDPR

Inquiry Report Issue: 14

- 7.37 The Housing Department of the Council commenced use, on a pilot basis, of a body worn camera for its Housing Tenancy Officer in May 2018. The Council stated that the purpose for the use of the body worn camera was for the health and safety of

the Housing Tenancy Officer who, in the past, has been subjected to threats of violence while conducting official activities. The Council informed the Inquiry Team that the lawful basis for the deployment of the body worn camera in this instance is Article 6(1)(d) of the GDPR (i.e. that the processing is necessary in order to protect the vital interests of the data subject or of another person). In further submissions to the Inquiry Team, the Council also relied upon Article 6(1)(e) of the GDPR as its lawful basis in connection with its health and safety obligations as an employer under the Safety, Health and Welfare at Work Act 2005 (as amended) and the Safety, Health and Welfare at Work (General Application) Regulations 2007.

7.38 The Inquiry Team accepted that the Council has obligations under health and safety legislation in relation to the protection of staff in the workplace. However, I must assess whether the Council has a legal basis under Article 6(1)(d) or 6(1)(e) of the GDPR to use body worn cameras in fulfilling its obligations under health and safety legislation.

7.39 In order to lawfully process personal data using body worn cameras, a controller must satisfy the requirements of Article 6 of the GDPR. In the absence of the consent of the data subject, the obligation lies on the controller to show that the data processing is necessary for the purposes concerned. Therefore, in the scenario where the Council considers that the processing of personal data through the use of body worn cameras is necessary either:

- in order to protect the vital interests of the data subject or of another person (Article 6(1)(d)); or
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)),

it must consider and document whether the use of body worn cameras is necessary for staff health and safety purposes. A necessity test involves the examination of the proposed measure(s), supported by evidence describing the problem to be addressed by the measure(s), how the measure(s) will address the problem and why existing or less intrusive measures cannot sufficiently address the issue. This test of necessity should have been undertaken prior to the commencement of the use of body worn cameras by means of a data protection impact assessment or by another equivalent exercise. A test of necessity is also required for all existing processing operations that are likely to be high risk processing. The Inquiry Team found no evidence of any such necessity test having been carried out. As a result, there is no evidence that the data processing by means of body worn cameras is *necessary* to protect the vital interests of the data subject or of another person, or for the performance of a of a task carried out in the public interest.

7.40 In addition, as set out in paragraphs 7.29 to 7.33, in order for a valid legal basis to exist for an employer to process personal data via body worn cameras under Article 6(1)(e), it would be necessary for the legislature to specifically grant power to employers to carry out such processing in a manner which is clear, precise and

foreseeable for data subjects subject to the processing. In its submissions, the Council cited legislative obligations on employers set out in the Safety, Health and Welfare at Work Act 2005 (as amended) and the Safety, Health and Welfare at Work (General Application) Regulations 2007. While these impose obligations on employers, they do not specifically grant an employer the power to carry out processing of personal data via body worn cameras (or any similar technology) in a manner which is clear, precise and foreseeable. In these circumstances, I find that the provisions of the Safety, Health and Welfare at Work Act 2005 (as amended) and the Safety, Health and Welfare at Work (General Application) Regulations 2007 cited by the Council do not provide the Council with a legislative basis to use body worn cameras for staff health and safety purposes in a manner that addresses the requirements of Article 6(1)(e) of the GDPR, interpreted in light of Article 6(3) and Recital 41 of the GDPR and applicable case law.

7.41 I welcome the submission made by the Council in response to the Draft Decision advising the DPC that Body worn cameras are not in use by the Council at present nor is it intended that they will be used in future. However, as the body worn cameras were in operation at the time the inquiry was conducted I find the Council has infringed Article 5(1)(a) GDPR.

Findings

7.42 ***I find that the Council infringed Article 5(1)(a) of the GDPR by not having a lawful basis to process personal data via body worn cameras for staff health and safety purposes.***

C. Appropriate signage and general transparency

a) CCTV Cameras

i) CCTV Scheme at Tuam

Regime: LED

Inquiry Issue: 4

7.43 In January 2017, the Garda Commissioner authorised the installation of twenty nine cameras on nine poles at three locations in the Tuam area of Galway under Section 38(3)(c) of the Garda Síochána Act 2005. During the course of the inquiry, the Inquiry Team established that no signage in relation to this CCTV scheme was erected on the approach roads to Tuam to alert data subjects that their personal data would be processed by a CCTV system once they entered the area covered by the focus of the cameras.

7.44 I 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. In the Final Inquiry Report, this issue was considered

under the GDPR. Now it is considered under the LED. The differences between these two regimes are set out above in this Decision.

7.45 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 is set out at Section 90(1) of the 2018 Act. Section 90(1) of the 2018 Act provides that:

Subject to subsection (4) and section 94, a controller shall ensure that the data subject is provided with, or, as appropriate, has made available to him or her, the information specified in subsection (2) in relation to personal data relating to him or her within a reasonable period after the date on which the controller obtains the personal data concerned, having regard to the circumstances in which the data are or are to be processed.

Section 90(2) of the 2018 Act provides that:

The information to which subsection (1) applies is:

(a) the identity and the contact details of the controller;

(b) the contact details of the data protection officer of the controller, where applicable;

(c) the purpose for which the personal data are intended to be processed or are being processed;

(d) information detailing the right of the data subject to request from the controller access to, and the rectification or erasure of, the personal data;

(e) information detailing the right of the data subject to lodge a complaint with the Commission and the contact details of the Commission;

(f) in individual cases where further information is necessary to enable the data subject to exercise his or her rights under this Part, having regard to the circumstances in which the personal data are or are to be processed, including the manner in which the data are or have been collected, any such information including:

(i) the legal basis for the processing of the data concerned, including the legal basis for any transfers of data;

(ii) the period for which the data concerned will be retained, or where it is not possible to determine the said period at the time of the giving of the information, the criteria used to determine the said period;

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

- 7.46 The absence of appropriate signage providing information to data subjects on the approach roads to Tuam 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 were intended to be processed or were being processed, amounts, in my view, to a breach of the Council's obligations under Sections 71(1)(a) and 90(1) of the 2018 Act.
- 7.47 I welcome the submission made by the Council in response to the Draft Decision advising the DPC of the Council's intention to erect, subject to DPC approval, appropriately worded and located signage on the approach roads to Tuam. However, as the signage was not erected at the time of the inquiry, I find the Council infringed Sections 71(a) and 90(1) of the 2018 Act.

Findings

- 7.48 ***I find 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 for purposes related to law enforcement.***

ii) Environment Department: CCTV Schemes at Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club

Regime: LED

Inquiry Issue: 4

- 7.49 *Ros a Mhíl Community Centre, Connemara:* It was noted by the Inquiry Team that a small sized CCTV notice was attached to each of two of the bottle banks. While 'Comhairle Chontae na Gaillimhe' appears on the top of each notice and the notices indicate that CCTV is in operation - with the image of a camera on each one - the notices provide no information with regard to the purposes of the CCTV cameras or the contact details for the controller or the data protection officer. Furthermore, there is no CCTV signage on the approach to the bottle-banks, such as at either of the two entrances to the site. As a result, members of the public who use the bottle banks or approach the doorway to the Community Centre have their images captured by one of the CCTV cameras before the CCTV notice is visible to them. In the case of members of the public who use the doorway to the Community Centre but do not use the nearby bottle bank facilities, they may be completely unaware that their activities are captured by the Council's CCTV cameras as the notices are neither sufficiently prominent nor favourably located to be drawn to their attention
- 7.50 *An Poitín Stil, Inverin, Connemara:* It was noted by the Inquiry Team that a small sized CCTV notice is attached to each of two of the bottle banks. While 'Comhairle Chontae

na Gaillimhe' appears on the top of each notice and the notices indicate that CCTV is in operation - with the image of a camera on each one - the notices provide no information with regard to the purposes of the CCTV cameras or the contact details for the controller or the data protection officer. Furthermore, there is no CCTV signage on the approach to the bottle-banks, such as at either of the two entrances to the site. As a result, members of the public who use the bottle banks have their images captured by one of the CCTV cameras before the CCTV notice is visible to them.

- 7.51 *Cregmore GAA Club*: A small sized CCTV notice is attached to each of two of the bottle banks. While 'Comhairle Chontae na Gaillimhe Galway County Council' appears on the top of each notice and the notices indicate that CCTV is in operation - with the image of a camera on each one - the notices provide no information with regard to the contact details for the controller or the data protection officer. Furthermore, there is no CCTV signage on the approach to the bottle-banks, such as at the entrance to the site. As a result, members of the public who use the bottle banks have their images captured by one of the CCTV cameras before the CCTV notice is visible to them.
- 7.52 I 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.
- 7.53 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. The absence of appropriate signage providing information to data subjects on the approach roads to Tuam 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, in my view, to a breach of the Council's obligations under Sections 71(1)(a) and 90(1) of the 2018 Act.
- 7.54 I welcome the submission made by the Council in response to the Draft Decision advising that the CCTV at Ros a Mhíl Community Centre, An Poitín Stil, Inverin, and Cregmore GAA Club have subsequently been switched off and monitoring equipment removed. However, as the required signage was not erected at the time of the inquiry and the CCTV recording was being carried out, I find the Council infringed Sections 71(a) and 90(1) of the 2018 Act.

Findings

- 7.55 ***I find 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 for purposes related to law enforcement.***

D. Technical and organisational measures

a) CCTV Cameras

i) Accessibility of Monitoring Screens at Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club

Regime: LED

Inquiry Report Issue: 9, 15

7.56 *Ros a Mhíl Community Centre, Connemara* - The Environment Department operated two CCTV cameras overlooking recycling bottle banks at Ros a Mhíl Community Centre in Connemara, County Galway. These CCTV cameras were used to detect illegal dumping. The monitoring and recording equipment for these CCTV cameras is kept in a room in the Community Centre. The Council's Community Warden and the Community Centre caretaker (who is not an employee of the Council) have a key to this room. During the summer months, the Community Centre is used as a Gaelscoil and the room is made available to teaching staff. This level of access presents a security vulnerability. The Inquiry Team observed that there were no security controls in place (such as passwords) to restrict access to the CCTV recording system or to the CCTV monitor. The Inquiry Team also observed that there was no restriction on staff or visitors bringing smartphones, cameras or recording devices into the room. On the day of the inspection, the Inquiry Team noted that the curtains on the window of this ground floor room were drawn, preventing passers-by outside from viewing the monitoring screen. However, reliance on the curtains being drawn does not meet a high security standard and the positioning of the monitoring screen at an angle which allows viewing from outside presents a security vulnerability. Furthermore, the Community Warden performs the function of downloading required CCTV footage onto SD cards. No steps are taken to secure personal data which is downloaded to SD cards.

7.57 *An Poitín Stil, Inverin, Connemara* – The Environment Department operated two CCTV cameras overlooking bottle banks in the grounds of a public house, An Poitín Stil, Inverin in Connemara, Co. Galway. These CCTV cameras were used to detect illegal dumping. The monitoring and recording equipment for these CCTV cameras was kept in the 'keg room' at the rear of the bar in An Poitín Stil. The keg room door is unlocked. Access to the keg room is given to staff but as the door of the keg room is unlocked, it may be accessed by patrons of the public house. The keg room is used for general storage as well as for the storage of kegs. The keg room also provides a means of access to a back door leading to the rear of the premises. In addition, a stairway leads from the keg room to the first floor where there are living quarters. Persons using the living quarters can easily access the keg room. This level of access to the keg room presents a serious security vulnerability in relation to the monitoring and recording equipment in the room. The Inquiry Team observed that there were

no security controls in place (such as passwords) to restrict access to the CCTV recording system or to the CCTV monitor. The Inquiry Team also observed that there was no restriction on staff or visitors bringing smartphones, cameras or recording devices into the room while they are on duty.

7.58 *Cregmore GAA Club* – The Environment Department operated one CCTV camera overlooking recycling bottle banks at the car park of Cregmore GAA Club. This CCTV camera was used to detect illegal dumping. The recording equipment for this CCTV camera was kept in a room in the clubhouse of Cregmore GAA Club.

- It emerged that as there is no viewing monitor in the clubhouse, the normal practice was that the Environment Department officials periodically collected the CCTV recorder from the clubhouse and brought it to County Hall where the footage is viewed and downloaded as required. The Inquiry Team were informed that the viewing of footage recorded at the Cregmore site has not occurred over the past three years (preceding the date of the inspection). This situation developed after the Council's I.T. Department introduced a prohibition on devices, such as video recorders, being connected or plugged in to the Council's I.T. systems. Despite this prohibition, the CCTV system at Cregmore GAA Club has been allowed to continue to record footage in the normal way. This arrangement between the Council and Cregmore GAA Club places the controller, the Council, in a position that it has an unsatisfactory level of control in respect of its CCTV recording and monitoring equipment.
- The Council's Community Warden did not have a door key to access the clubhouse. Instead, in order to access the clubhouse, the Community Warden had to call to a neighbouring house where the clubhouse key is kept. The Inquiry Team carried out an inspection at Cregmore GAA Club on 19 February, 2019. This inspection appointment was finalised over two weeks earlier – on 4 March, 2019. However, when the Inquiry Team and the Council officials arrived at Cregmore GAA Club they were unable to access the premises. Efforts by the Council officials to locate the keyholder failed and it emerged that the Council officials have no telephone contact details for the keyholder. Instead, reliance was placed on the expectation that the keyholder will be at home when the Council officials need to access the clubhouse. The failure to gain access to the clubhouse to inspect the recording equipment and the security arrangements in place around it placed the Inquiry Team at a disadvantage on the day of the inspection.
- The Inquiry Team were restricted to examining the outdoor aspects of the CCTV site and it had to rely on information provided by the Council officials who attended at the site. The Inquiry Team observed that the Council officials confirmed that while there is a password on the recording device at Cregmore GAA Club, it is a shared, generic password. As a result, the Council is unable to identify precisely which staff members have accessed the CCTV system.

7.59 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 organisation security measures, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. It is my view 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.

7.60 I welcome the submission made by the Council in response to the Draft Decision advising that CCTV facilities have been turned off as of October 2020, that all data downloaded to SD cards has been deleted, and that a policy regarding the use of personal telephones and smartphones, cameras or recording equipment in the CCTV room will be implemented. However, as these technical and organisational security measures were not implemented at the time of the inquiry, I find that the Council its obligations under Sections 71(1)(f), 72(1) and 78 of the 2018 Act.

Findings

7.61 ***I find that the Council infringed its obligations under Sections 71(1)(f), 72(1) and 78 of the 2018 Act by failing to implement 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara, and at Cregmore GAA Club.***

ii) Access Logs for CCTV Systems at Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club

Regime: LED

Inquiry Report Issue: 9, 15

7.62 The Council officials who attended the inspections were unable to establish whether any of these CCTV systems had the capability to identify, by date and time, accesses by staff. I must assess whether the Council has complied with its security obligations under the 2018 Act in these circumstances.

7.63 Where the LED regime applies, Section 82(1) of the 2018 Act obliges a controller to maintain a data log where it processes personal data. 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, insofar as is possible.

7.64 It is my view that it should have been possible for the Council to operate a log system whereby each individual who accessed the camera feeds would have a separate

username that would enable them to be identified. By failing to do so, the Council infringed Section 82(2) of the 2018 Act.

7.65 I welcome the submission made by the Council in response to the Draft Decision advising that all CCTV cameras at the relevant bottle bank facilities have been switched off and monitoring equipment removed from Ros a' Mhíl Community Centre, An Poitín Stil, Inverin and Cregmore GAA Club as of October 2020. However, as these measures were not implemented at the time of the inquiry, I find the Council infringed Section 82(2) of the 2018 Act.

Findings

7.66 ***I find that the Council infringed Section 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club.***

iii) **Access Logs for CCTV feeds in County Hall and at Tuam Regional Offices**

Regime: LED

Inquiry Report Issue: 2, 5, 15

7.67 During the course of the inspection phase of the inquiry, it was established that access to the CCTV Viewing Room at County Hall, where the camera feeds are located for the Housing Department of the Council, was restricted to the Tenancy Enforcement Officer. The Tenancy Enforcement Officer kept a manual record of each time the room was accessed and the purpose for the access and a manual record of all actions conducted in relation to the camera feeds, including testing of the system and recording requests for downloads. The Inquiry Team concluded that the manual record is the only method employed by the Council to record accesses to the CCTV system. Consequently, as the CCTV system has no electronic audit system in place, it is impossible for the Council to identify precisely what footage the authorised officer has accessed or when this access occurred. The failure to deploy an electronic audit trail on the CCTV system of the Housing Department complete with unique user identification to identify precisely all access to the CCTV system may present a security vulnerability and exposes the Council to, for example, undetected accesses to the CCTV system for non-official purposes or unauthorised personnel. I must assess whether the Council has complied with its security obligations under the 2018 Act in these circumstances.

7.68 During the course of the inspection phase of the inquiry, it was also established that the Garda-authorized community-based CCTV system that is housed in the Tuam Regional Offices had no functionality to electronically log accesses to the recording system on which the footage is kept. Consequently, it is impossible for the Council to identify precisely which staff have accessed or are accessing its CCTV system as no electronic audit system is in place.

- 7.69 Where the LED regime applies, Section 82(1) of the 2018 Act obliges a controller to maintain a data log where it processes personal data. That log must record, among other things, the consultation of the personal data by any person. Under Section 82(2) of the 2018 Act, 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.
- 7.70 It is my view that it should have been possible for the Council to operate an electronic log system whereby each individual who accessed the camera feeds would have a separate username that would enable them to be identified. By failing to do so, the Council infringed Section 82(2) of the 2018 Act.
- 7.71 I welcome the submission made by the Council in response to the Draft Decision advising that access to the CCTV rooms in County Hall and Tuam Regional Offices have had access restricted to designated persons and that logging systems have been implemented at both sites. However, as these measures were not implemented at the time of the inquiry, I find the Council infringed Section 82(2) of the 2018 Act.

Findings

- 7.72 ***I find that the Council infringed Section 82(2) of the 2018 Act by failing to maintain an electronic data log at the CCTV Room in County Hall and at Tuam Regional Offices that recorded the identity of any individual who consulted personal data contained in the CCTV camera views and recorded footage from the locations covered by the CCTV cameras in question.***

(iv) Training and awareness

Regime: GDPR and LED

Inquiry Report Issue: 16

- 7.73 During the course of the inspection phase of the inquiry, the Inquiry Team observed that there appeared to be a generally low level of awareness of data protection law and principles in the Council. For example, the Inquiry Team noted that:
- the Housing Department of the Council commenced use, on a pilot basis, of a body worn camera for its Housing Tenancy Officer in May 2018 without conducting a data protection impact assessment or being aware that such an assessment ought to be conducted; and
 - in relation to the application of privacy masking solutions to CCTV cameras used by the Council in housing estates, the Council appeared to be of the view that the minimisation of the intrusiveness of CCTV cameras did not need to be prioritised because the estates were under the control of the Council.
- 7.74 Under Article 24(1) of the GDPR, where the GDPR applies a controller must implement “*appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with*” the GDPR.

Similarly, under Section 75(1) of the 2018 Act, where the LED applies a controller must 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 accordance with”* the 2018 Act.

7.75 Raising staff awareness of the principles of data protection and their relevance to the operations of the controller is an important element of the organisational measures which ought to be adopted under Article 24(1) of the GDPR and Section 75(1) of the 2018 Act, as applicable.

7.76 In its submissions the Council informed the Inquiry Team that:

- Data protection training was given by a consultant and completed by relevant staff in September – November 2018;
- A full day of comprehensive training on data protection was given by an external body in July 2019 for 21 relevant senior staff across all departments of the Council; and
- A further full day of comprehensive training on data protection was given by an external body in October 2019 for 33 relevant senior staff across all departments of the Council. This included the Housing Tenancy Enforcement Officer and staff from the environment section who involved with CCTV and the resulting processing of personal data.

7.77 It is my view that despite the training that the Council informed the Inquiry Team was provided, the low level of awareness of data protection principles in the Council that was demonstrated by the issues that were uncovered by the Inquiry Team indicates that the Council has not complied with its obligations under Article 24(1) of the GDPR and Section 75(1) of the 2018 Act.

Findings

7.78 I find that the Council infringed Article 24(1) of the GDPR and Section 75(1) of the 2018 Act by failing to implement appropriate technical and organisational measures to ensure that processing of personal data was performed in accordance with the GDPR and the 2018 Act, as applicable.

E. DPO Access to CCTV Systems

i) Housing Department: Restriction on DPO Access to CCTV Viewing Room

Regime: LED

Inquiry Report Issue: 3

7.79 On the first inspection date (19 November 2018), the Inquiry Team noted that the controls which were in place at the CCTV Viewing Room in County Hall prohibited the Data Protection Officer (the ‘DPO’) from access to that room and thereby also

restricted the DPO from having oversight of the data processing which takes place on the CCTV system. The Council submitted that this was a misinterpretation and that the Council's policy was in accordance with the Department of Justice and Equality and An Garda Síochána Code of Practice for Community Based CCTV Schemes, Form No PD001, Section 4.4 which provides that access to the relevant recorded CCTV images should be restricted to a designated person or persons who have been Garda vetted. The DPO's Garda vetting application was pending at this time. I note from the Final Inquiry Report that the DPO accompanied the Authorised Officers to the CCTV Viewing Room on the second inspection date of 5 December 2018.

7.80 In the Final Inquiry Report, this issue was considered under the GDPR. Now it is considered under the LED. The differences between these two regimes are set out above in this Decision.

7.81 Section 88(5) of the 2018 Act outlines the functions of DPO. These include monitoring compliance of the controller with Part 5 of the 2018 Act and monitoring compliance of the controller with any other law of the European Union or law of the State that relates to the protection of personal data. Under Section 88(4) of the 2018 Act, a controller is required to support its DPO in performing his or her functions under Section 88(5), including by ensuring that he or she has access to processing operations carried out by the controller.

7.82 The restriction of the DPO's access to the CCTV Viewing Room prevents the DPO from exercising her statutory functions set out in Section 88(5) of the 2018 Act. It is my view that there are extenuating circumstances for the temporary restriction of access on 19 November 2018. However, I would consider a matter of good practice for the controller to ensure that any prospective DPO complete the Garda vetting process prior to his or her appointment to the position of DPO in circumstances where the performance of DPO functions is contingent on the completion of the vetting process.

Findings

7.83 *I find that the Council did not infringe Section 88(4) of the 2018 Act by prohibiting the DPO from accessing the CCTV Viewing Room at the time of the initial inspection on 19 November 2018.*

F. Data minimisation and data protection by design and by default

a) CCTV Cameras

(i) Housing Department: Focus of CCTV Cameras on private homes

Regime: LED

Inquiry Report Issue: 1, 10

- 7.84 The Housing Department of the Council has deployed CCTV cameras at a number of housing estates for the detection of anti-social behaviour. The Inquiry Team inspected these cameras during the investigation. The Inquiry Team were told that the CCTV system for the Parkmore Estate had the capability to deploy privacy masking solutions, but it was evident that such solutions were not in operation on the dates of the first inspection (19 November 2018), as there was full view on the monitoring screens of all aspects of homes such as front and back gardens, front and back doors and windows. On the date of the second inspection (5 December 2018), the Inquiry Team noted again that homes in Parkmore Estate that were intended to be masked on the monitoring screen were, instead, open to full viewing on the monitoring screen. The Inquiry Team also observed on the monitoring screen views of back gardens at Bridge Court, Ahascragh and front yards at Crowe Street, Gort. Furthermore, the Inquiry Team noted that one particular camera in Parkmore Estate (Camera A – Predator pan, tilt and zoom camera) was capturing CCTV footage from beyond its intended target of the Parkmore Estate which is under the control of the local authority. These CCTV cameras are focused on private spaces rather than public spaces and, accordingly, the cameras have the potential to invade on the privacy of residents of and visitors of the dwelling houses concerned. I must assess whether the Council has complied with its data minimisation obligations in these circumstances.
- 7.85 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.”
- 7.86 The concept of what is “not excessive” was considered in *Deutsche Post AG v Hauptzollamt Köln*.²¹ The CJEU considered a requirement of the Principal Customs Office in Cologne that applicants for the status of an authorised economic operator submit the tax identification numbers of certain persons in charge of the applicant company or its customs matters. The purpose of the numbers was to enable the Office to determine, when responding to an application for AEO status, whether those persons had infringed customs legislation or had a record of serious criminal offences relating to their economic activity over the last three years. The Court acknowledged that the collection of tax identification numbers could enable the customs authorities to have access to personal data that has no connection with the economic activity of the applicant for AEO status. However, the criteria for granting AEO status involved a consideration by the customs authorities of whether those persons had committed such infringements or offences. The Court held that this implies that the customs authorities should have access to data that makes it possible to establish whether the specified infringements or offences have been committed. It held that the collection of tax identification numbers was not excessive

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

to that purpose. This judgment illustrates the breadth of purposes that must be considered for determining what is not excessive.

- 7.87 The alleged purpose of the processing of personal data via these CCTV systems is to detect and reduce incidences of anti-social behaviour at the housing estates in question. Recording activities on private properties is not relevant to this purpose. Where the CCTV focuses on both private properties and public places, I find 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.
- 7.88 In addition, Section 76(2) of the 2018 Act provides that a controller shall, when processing personal data, implement appropriate and technical organisational measures to ensure that only personal data that are necessary for each specific purpose of the processing are being processed. I find 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.
- 7.89 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. I find that the Council has failed to be in a position to demonstrate that the focus of the CCTV cameras on the private dwellings is not excessive to preventing anti-social behaviour Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort.

Findings:

- 7.90 ***I find that the Council infringed Section 71(1)(c) and Section 76(2) of the 2018 Act by processing personal data arising from CCTV recordings directed at private properties, in the absence of any privacy masking technology, at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort.***
- 7.91 ***I find that the Council infringed Section 71(10) of the 2018 Act by failing to demonstrate that its processing of personal data via CCTV cameras at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort, is not excessive to its purpose of preventing anti-social behaviour.***

(ii) Environment Department: Collection of personal data relating to children via CCTV Cameras

Regime: LED

Inquiry Report Issue: 9

- 7.92 During the course of the inspection it came to the attention of the Inquiry Team that during the summer months (June to August inclusive) when the Ros a Mhíl Community Centre is used as a Gaelscoil, up to two hundred minors attend at the premises each day. On inspecting, via the monitoring screen, the field of vision captured by the CCTV cameras, the inspectors established that the CCTV cameras captured the images of these minors as they focused directly on the outdoor resource area that is used by them for various activities (the bottle-banks are sited immediately adjacent to the outdoor resource area and users of the bottle-banks must traverse this area in order to access the bottle-banks). The Community Warden also confirmed this to be the case. In short, a substantial amount of CCTV footage was captured over a three-month period each summer by the Council involving children partaking in day-to-day Gaelscoil outdoor activities that are unrelated in any way to the Council's law enforcement functions under the Litter Pollution Act 1997.
- 7.93 The principle of data minimisation is enshrined at Section 71(1)(c) of the 2018 Act which provides that the personal data collected by a controller shall be adequate, relevant and not excessive in relation to the purposes for which they are processed. I find that the Council infringed section 71(1)(c) 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
- 7.94 In addition, Section 76(2) of the 2018 Act further provides that a controller shall, when processing personal data implement appropriate and technical organisational measures that only personal data that are necessary for each specific purpose of the processing are being processed. I find that the Council infringed section 76(2) of the 2018 Act by failing to implement technical and organisational measures which ensure that only personal data necessary for the performance of the Council's law enforcement functions under the Litter Pollution Act 1997 are collected.
- 7.95 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. I find that the Council has failed to be in a position to demonstrate that the personal data relating to children collected via the CCTV cameras is not excessive to performing the Council's law enforcement functions under the Litter Pollution Act 1997.
- 7.96 I welcome the submission made by the Council in response to the Draft Decision advising that CCTV monitoring equipment has been removed from Ros a' Mhíl Community Centre as of October 2020. However, as this monitoring equipment was in place at the time of the inquiry, I find that the Council infringed its obligations under Sections 71(1)(c), 76(2) and 71(10).

Findings

- 7.97 ***I find that the Council infringed its obligations under Sections 71(1)(c) and 76(2) of the 2018 Act in connection with the capturing of images of children partaking in***

the outdoor activities at a Gaelscoil at Ros a Mhíl Community Centre during the summer months.

7.98 I find that the Council infringed Section 71(10) of the 2018 Act by failing to be in a position to demonstrate that its processing of personal data relating to children via these CCTV cameras is not excessive to performing the Council's law enforcement functions under the Litter Pollution Act 1997.

G. Accountability

a) CCTV Cameras

(i) Data protection impact assessments for CCTV cameras

Regime: LED

Inquiry Report Issue: 8, 9, 10

7.99 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."

7.100 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 cameras at the bottle bank facilities at Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club;
- in respect of the engagement of the services of CU Security to conduct covert surveillance; or
- in respect of the use of intelligent integrated CCTV cameras at Tirboy and Parkmore Estates in Tuam

in each case in connection with the performance by the Council of its law enforcement functions in relation to the prevention, investigation, detection or prosecution of offences.

7.101 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 my view that it is clear 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, for covert surveillance purposes and at these estates. However, no such assessments had been carried out at the time of the inspection phase of the inquiry.

7.1021 find that the Council infringed its obligations under Section 84 of the 2018 Act by failing to have carried out any data protection impact assessments in respect of its use of CCTV cameras at the relevant bottle bank facilities and housing estates. Although no covert surveillance was being carried out at the time that the Inquiry Team carried out its inspections, the Council stated in its submissions that it has “*utilised covert surveillance for the purpose of initiating and successfully pursuing prosecutions based on an evidential collection of data*” and included photographic evidence of illegal dumping to support this. The Council did not provide any evidence of having complied with its obligations under Section 84 of the 2018 Act in respect of covert surveillance and at the time of the inspection, the Inquiry Team found no evidence of a data protection impact assessment or an equivalent exercise having been carried out to test the necessity of the use of covert CCTV cameras.

7.1031 welcome the submission made by the Council in response to the Draft Decision advising that the Council will conduct data protection impact assessments in respect of any proposed future use of CCTV cameras. However, as the Council failed to carry out any data protection impact assessments at the relevant bottle bank facilities and housing estates in respect of the use of CCTV cameras, I find that the Council infringed its obligations under Sections 84 of the 2018 Act.

Findings

7.1041 find 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 cameras at the bottle bank facilities at Ros a Mhil Community Centre, Connemara, An Poitin Stil, Inverin, Connemara and Cregmore GAA Club and at Tirboy Estate and Parkmore Estate and in relation to covert surveillance previously carried out by the Council.

b) ANPR Cameras

(i) Data protection impact assessments for ANPR cameras

Regime: GDPR and LED

Inquiry Report Issue: 11, 12

7.105As set out above at paragraphs 7.21 to 7.36, as part of a CCTV upgrade the Council installed ANPR cameras in two housing estates in Tuam, namely Parkmore and Tirboy, as a wider estate enhancement scheme in 2017 to include a traffic management system and to detect possible anti-social behaviour events.

7.106 As set out above at paragraphs 7.101 and 7.102, under Article 35(1) of the GDPR (where the GDPR applies) and Section 84(1) of the 2018 Act (where the LED applies), a data protection impact assessment is required where ANPR cameras will be used for systematically monitoring, tracking or observing individuals' location or behaviour. Since the Council did not provide the Inquiry Team with any evidence of a data protection impact assessment having been carried out, I find that the Council infringed Article 35 of the GDPR and Section 84(1) of the 2018 Act in these circumstances.

7.107 I welcome the Council's submission that in respect of any future proposal to erect ANPR cameras, a data protection impact assessment will be conducted to determine the appropriate legal basis, necessity and proportionality. However, as an assessment was not carried out in respect of the ANPR cameras in operation at the time of the inquiry, I find that the Council infringed Article 35(1) GDPR and Section 84(1) of the 2018 Act.

Findings

7.108 I find that the Council infringed Article 35(1) of the GDPR and Section 84(1) of the 2018 Act by failing to carry out a data protection impact assessment for the deployment of the ANPR cameras at Tirboy Estate and Parkmore Estate for traffic management and law enforcement purposes, respectively.

(ii) Housing Department: Data protection policy for ANPR cameras

Regime: LED and GDPR

Inquiry Report Issue: 13

7.109 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.

7.110 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.

7.111 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.

7.112 In connection with the Council's processing of personal data via ANPR cameras, both for law enforcement purposes and for traffic management purposes, the Inquiry Team examined the CCTV Policy on the Council's website at the date of authoring the Final Inquiry Report. The CCTV Policy referred as follows to the use of ANPR cameras: "The Council has ANPR cameras in 2 Estates in Tuam and this footage is covered under the provisions of this policy, with similar restrictions to access as the Housing Estate CCTV". No further reference was made in that CCTV Policy to the use of ANPR cameras.

7.113 I am of the view that the CCTV Policy did not adequately demonstrate compliance with the 2018 Act with respect to the deployment of ANPR cameras in the relevant housing estates in Tuam for law enforcement purposes, or compliance with the GDPR with respect to the deployment of ANPR cameras for traffic management purposes.

7.114 I welcome the submission made by the Council in response to the Draft Decision advising the CCTV Policy was updated in December 2020 to include reference to ANPR and a link to the developed SOP. However, as the CCTV policy was not erected at the time of the inquiry, I find 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

7.115 I find 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 appropriately describe the use of ANPR cameras in the CCTV Policy which was in place on the date of authoring of the Final Inquiry Report.

H. Data Retention

Retention of personal data collected via CCTV cameras

Regime: LED

Inquiry Report Issue: 6, 9

7.116 On 5 December 2018 the Inquiry Team carried out an inspection of the community-based CCTV scheme in Ballinasloe. On examining the CCTV recording equipment at the Council's offices in Ballinasloe, the Inquiry Team noted that footage dating back eleven months to January 2018 remained accessible on the system. This footage was retained; however the basis for retention was not that the footage was required for

the investigation or prosecution of suspected offences. Section 4.2 of the Code of Practice for Community Based CCTV Schemes states the following: “CCTV images should be erased and media storage devices re-used after a period of 28 days unless required for the investigation of offences or evidential purposes.”

7.117 On 19 February 2018 the Inquiry Team carried out an inspections of the bottle bank facilities where CCTV cameras are operated by the Council. On examining the CCTV recording equipment:

- at Ros a Mhíl Community Centre, Connemara, the Inquiry Team noted that footage dating back seven weeks to 2 January 2019 remained accessible on the system;
- at An Poitín Stil, Inverin, Connemara, the Inquiry Team noted that footage dating back eight weeks to 26 December 2018 remained accessible on the system.

This footage was retained; however the basis for this retention was not that the footage was required for the investigation or prosecution of suspected offences.

7.118 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. I am of the view that the Council infringed this requirement by retaining CCTV footage for:

- up to 11 months after it was recorded via the CCTV scheme at Ballinasloe;
- up to 7 weeks after it was recorded via the CCTV cameras at Ros a Mhíl Community Centre, Connemara; and
- up to 8 weeks after it was recorded via the CCTV cameras at An Poitín Stil, Inverin, Connemara.

7.119 I welcome the submission made by the Council in response to the Draft Decision advising that all CCTV cameras at bottle bank facilities have been switched off, that the monitoring equipment has been removed from Ros a Mhíl Community Centre, An Poitín Stil, Inverin as of October 2020, and that the Ballinasloe CCTV Scheme cameras are no longer recording. However, as footage was retained by the Council in excess of the prescribed period of time during the inquiry, I find the Council infringed Sections 71(1)(e) of the 2018 Act.

Findings

7.120 I find 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 community-based CCTV scheme at Ballinasloe and the CCTV cameras at Ros a Mhíl Community Centre and at An Poitín Stil, Inverin.

8. Decision on Corrective Powers

8.1 The following table lists the infringements I have found in this Decision.

Statutory Provision	Instances of the Infringement
Section 71(1)(a) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Unlawfully processing data from CCTV cameras at the relevant bottle bank facilities.</p> <p>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 for purposes related to law enforcement.</p>
Section 71(2)(a) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Processing of personal data from ANPR cameras at the Parkmore and Tirboy without a clear legal basis to do so.</p>
Article 5(1)(a) of the GDPR	<p>I have found the Council has infringed this Article by:</p> <p>Not having a lawful basis to process personal data from ANPR cameras for the purposes of traffic management;</p> <p>Not having a lawful basis to process personal data via body worn cameras for staff health and safety purposes.</p>
Section 90(1) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Failing to erect appropriately worded and located signage or provide the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras for purposes related to law enforcement.</p>
Section 71(1)(f) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Failing to implement 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara, and at Cregmore GAA Club.</p>
Section 72(1) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Failing to implement 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara, and at Cregmore GAA Club.</p>

Section 78 of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Failing to implement 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara, and at Cregmore GAA Club.</p>
Section 82(2) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club.</p> <p>Failing to maintain an electronic data log at the CCTV Room in County Hall and at Tuam Regional Offices that recorded the identity of any individual who consulted personal data contained in the CCTV camera views and recorded footage from the locations covered by the CCTV cameras in question</p>
Article 24(1) of the GDPR	<p>I have found the Council has infringed this Article by:</p> <p>Failing to implement appropriate technical and organisational measures to ensure that processing of personal data was performed in accordance with the GDPR</p>
Section 75(1) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Failing to implement appropriate technical and organisational measures to ensure that processing of personal data was performed in accordance with the 2018 Act.</p>
Section 71(1)(c) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Processing personal data arising from CCTV recordings directed at private properties, in the absence of any privacy masking technology, at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort.</p> <p>capturing of images of children partaking in the outdoor activities at a Gaeilscoil at Ros a Mhíl Community Centre during the summer months</p>
Section 76(2) of the 2018 Act	<p>I have found the Council has infringed this section by:</p> <p>Processing personal data arising from CCTV recordings directed at private properties, in the absence of any privacy masking technology, at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort.</p>

	Capturing of images of children partaking in the outdoor activities at a Gaeilscoil at Ros a Mhíl Community Centre during the summer months
Section 71(10) of the 2018 Act	I have found the Council has infringed this section by: Failing to demonstrate that its processing of personal data via CCTV cameras at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort, is not excessive to its purpose of preventing anti-social behaviour. Failing to demonstrate that its processing of personal data relating to children via these CCTV cameras is not excessive to performing the Council's law enforcement functions under the Litter Pollution Act 1997.
Section 84 of the 2018 Act	I have found the Council has infringed this section by: Failing to carry out a data protection impact assessment for the deployment of CCTV cameras at the bottle bank facilities at Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club and at Tirboy Estate and Parkmore Estate and in relation to covert surveillance previously carried out by the Council
Article 35(1) of the GDPR	I have found the Council has infringed this Article by: Failing to carry out a data protection impact assessment for the deployment of the ANPR cameras at Tirboy Estate and Parkmore Estate for traffic management and law enforcement purposes, respectively
Section 84(1) of the 2018 Act	I have found the Council has infringed this section by: Failing to carry out a data protection impact assessment for the deployment of the ANPR cameras at Tirboy Estate and Parkmore Estate for traffic management and law enforcement purposes, respectively.
Article 24 of the GDPR, interpreted in light of Article 24(2) of the GDPR	I have found the Council has infringed this Article by: Failing to appropriately describe the use of ANPR cameras in the CCTV Policy which was in place on the date of authoring of the Final Inquiry Report.
Section 75(1) of the 2018 Act, interpreted in light of Section 75(3) of the 2018 Act	I have found the Council has infringed this section by: Failing to appropriately describe the use of ANPR cameras in the CCTV Policy which was in place on the date of authoring of the Final Inquiry Report.
Section 71(1)(e) of the 2018 A	I have found the Council has infringed this Article by:

	Retaining of personal data for longer than is necessary for purposes for which that data are processed via the community-based CCTV scheme at Ballinasloe and the CCTV cameras at Ros a Mhíl Community Centre and at An Poitín Stil, Inverin.
--	---

8.2 Having considered the infringements that I found in this Decision, I have to exercise corrective powers in accordance with sections 111(3) and 124(3) of the 2018 Act. My 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. I have set out below the corrective powers, pursuant to sections 115(1) and 127(1) of the 2018 Act, which I have decided to exercise.

i. Lawful Bases for the Processing

No.	Action	Time Scale
1.	<p>Infringement of Section 71(1)(a) of the 2018 Act by unlawfully processing data from CCTV cameras at the relevant bottle bank facilities and 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 for purposes related to law enforcement.</p> <p>I find that there is no lawful basis for the Council’s processing of personal data by means of CCTV cameras at the relevant bottle bank facilities. I propose to impose 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, for example an authorisation received from the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act that regulates such processing in accordance with Article 8(2) of the LED.</p>	<p>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 a valid legal basis for the processing can be identified in the meantime.</p>
2.	<p>Infringement of Section 71(2)(a) of the 2018 Act by unlawfully processing data from ANPR cameras at Parkmore and Tirboy housing estates without a clear legal basis to do so.</p> <p>I find that there is no lawful basis for the Council’s processing of personal data by means of CCTV cameras at Parkmore and Tirboy estates. I propose to impose a temporary ban on the Council’s use of CCTV at these locations. This processing must not resume unless, and until,</p>	<p>In respect of any CCTV cameras which have ANPR facilities, all functionality on these CCTV cameras shall be switched off within 90 days of receiving this Decision, unless a valid legal basis for the processing can be identified in the meantime.</p>

	there is a basis for it in EU or Member State Law, for example an authorisation received from the Garda Commissioner pursuant to section 38(3)(c) of the 2005 Act that regulates such processing in accordance with Article 8(2) of the LED.	
3.	<p>Infringement Article 5(1)(a) of the GDPR by not having a lawful basis to process personal data via body worn cameras for staff health and safety purposes.</p> <p>I find that there is no lawful basis for the Council's processing of personal data by means of body worn cameras. I propose to impose a temporary ban on the Council's use of body worn cameras. The processing must not resume unless, and until, there is there is a basis for it in EU or Member State Law.</p>	The Council shall confirm to the DPC within 90 days of receiving the Decision that body-worn cameras are not in use unless a valid legal basis can be identified in the meantime.

ii. Transparency

No.	Action	Time Scale
4.	<p>Infringement of 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 for purposes related to law enforcement.</p> <p>The Council shall 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 for purposes related to law enforcement prior to use of CCTV cameras at these locations.</p>	Complete tasks and submit report to the DPC detailing the action taken within 90 days of receipt of the final decision.

iii. Technical and organisational measures

No.	Action	Time Scale
5.	Infringement of obligations under Sections 71(1)(f), 72(1) and 78 of the 2018 Act by failing to implement 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 Ros a Mhíl	Complete tasks and submit report to the DPC detailing the action taken within 90 days of the receipt of the final decision.

	<p>Community Centre, Connemara, An Poitín Stil, Inverin, Connemara, and at Cregmore GAA Club.</p> <p>The Council shall bring its processing operations into compliance with the 2018 Act by implementing security measures to limit access to the room containing CCTV footage and equipment to authorised persons only.</p> <p>The Council shall implement measures to secure CCTV footage downloaded to SD cards.</p> <p>The Council shall implement a policy regarding the use of personal telephones and smartphones, cameras or recording equipment in the CCTV room.</p>	
6.	<p>Infringement of Section 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 Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club.</p> <p>The council shall create and maintain a data log to identify any individual who consulted personal data contained in the CCTV camera views and recorded footage from Ros a Mhíl Community Centre, Connemara, An Poitín Stil, Inverin, Connemara and Cregmore GAA Club.</p>	<p>Complete tasks and submit report to the DPC detailing the action taken within 90 days of the receipt of the final decision.</p>
7.	<p>Infringement of Section 82(2) of the 2018 Act by failing to maintain an electronic data log at the CCTV Room in County Hall and at Tuam Regional Offices that recorded the identity of any individual who consulted personal data contained in the CCTV camera views and recorded footage from the locations covered by the CCTV cameras in question.</p> <p>The Council shall create and maintain an electronic data log at the CCTV Room in County Hall and at Tuam Regional Offices that recorded the identity of any individual who consulted personal data contained in the CCTV camera views and recorded footage from the locations covered by the CCTV cameras in question.</p>	<p>Complete tasks and submit report to the DPC detailing the action taken within 90 days of the receipt of the final decision.</p>

8.	<p>Infringement Section 71(1)(c) and Section 76(2) of the 2018 Act by processing personal data arising from CCTV recordings directed at private properties, in the absence of any privacy masking technology, at Parkmore Estate, Bridge Court, Ahascragh and Crowe Street, Gort</p> <p>I order 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 monitoring centres. These technical and organisational measures could include privacy masking and/or preventing manual control of the CCTV cameras by operators of the monitoring centres.</p>	<p>Complete tasks and submit report to the DPC detailing the action taken within 90 days of the receipt of the final decision.</p>
----	--	--

iv. Accountability

No.	Action	Time Scale
9.	<p>The Council infringed Section 71(10) of the 2018 Act by failing to be in a position to demonstrate that its processing of personal data relating to children via these CCTV cameras is not excessive to performing the Council's law enforcement functions under the Litter Pollution Act 1997.</p> <p>The Council shall cease processing of personal data relating to children via CCTV cameras at the Gaelscoil at Ros a' Mhíl Community Centre until a data protection impact assessment has been carried out and any necessary safeguards are implemented, as required.</p>	<p>CCTV cameras to be switched off within 90 days of the receipt of the final decision.</p>
10.	<p>Infringement of Article 35(1) of the GDPR and Section 84(1) of the 2018 Act by failing to carry out a data protection impact assessment for the deployment of the ANPR cameras at Tirboy Estate and Parkmore Estate for traffic management and law enforcement purposes, respectively.</p> <p>The Council shall carry out data protection impact assessments at Tirboy Estate and Parkmore Estate prior to any future deployment of ANPR cameras for traffic management and</p>	<p>If the Council identifies an appropriate legal basis and intends to recommence processing personal data with ANPR cameras, prior to commencing processing Order 10 must be complied with.</p>

	law enforcement purpose under an appropriate legal base.	
11.	<p>Infringement of 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 appropriately describe the use of ANPR cameras in the CCTV Policy which was in place on the date of authoring of the Final Inquiry Report.</p> <p>I issue a reprimand to the Council for failing to accurately describe its use of ANPR cameras in the CCTV policy.</p>	N/A

v. Data Retention

No.	Action	Time Scale
12.	<p>Infringement of 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 community-based CCTV scheme at Ballinasloe and the CCTV cameras at Ros a Mhíl Community Centre and at An Poitín Stil, Inverin.</p> <p>The Council shall retain personal data in the form of CCTV for no longer than a period of 28 days unless required for the investigation of offences or evidential purposes.</p>	<p>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 a valid legal basis for the processing can be identified in the meantime</p>

9. Consideration of imposing an Administrative Fine

9.1 Article 58(2)(i) of the GDPR empowers me, as Decision-Maker, in addition to other corrective powers exercised, to impose an administrative fine on a controller who infringes the GDPR. Section 141(4) of the 2018 Act provides that an administrative fine shall not exceed €1,000,000 where the controller subject to the fine is a public authority or public body and does not act as an undertaking within the meaning of the Competition Act 2002. I find the Council is a public body and does not act as an undertaking within the meaning of the Competition Act 2002. Therefore, the fining cap of €1,000,000 applies.

9.2 In deciding on the corrective powers that are to be exercised in respect of the infringements of Articles 5(1)(a) and 35(1) of the GDPR, I have had due regard to the Commission's power to impose administrative fines pursuant to Section 141 of the

2018 Act. In particular, I have considered the criteria set out in Article 83(2)(a) – (k) of the GDPR. When imposing corrective powers, I am obliged to select the measures that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures, for example re-establishing compliance with the GDPR or punishing unlawful behaviour (or both).²² In all circumstances of the infringements at issue in the inquiry, I find that an administrative fine would not be necessary, proportionate or dissuasive. In this context, I have considered the Council's infringement of Article 5(1)(a) GDPR by its processing of personal data through ANPR cameras without a valid legal basis, the Council's infringement of Article 5(1)(a) GDPR by processing data from body worn cameras without a valid legal basis, and the Council's infringement of Article 35(1) GDPR by failing to carry out a data protection impact assessment for the deployment of the ANPR cameras at Tirboy Estate and Parkmore Estate for traffic management and law enforcement purposes. Furthermore, I have given due consideration to the fulsome response of the Council in acknowledging the infringements and expeditiously addressing the matters identified.

10. Right of Appeal

10.1 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 has the right to appeal against this Decision within 28 days from the date on which notice of this Decision is received by it.

²² See the Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.