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

DPC Case Reference: 05/SIU/2018

In the matter of Kildare 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

16 January 2023

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Contents

1. Introduction

1.1 This document (the '**Decision**') is a decision made by 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 Authorised Officers who conducted the inquiry provided Kildare County Council (the '**Council**') with the Draft Inquiry Report and the Final Inquiry Report.

1.2 It is noted that after the Council was issued with the Draft Inquiry Report on 26 June 2019, and arising from the provisional views expressed therein by the Inquiry Team, the Council conducted a number of data protection impact assessments ('**DPIAs**'). 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 12 September 2018 and 7 November 2018 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.

1.3 The Council was provided with a draft decision on this inquiry (the '**Draft Decision**') on 8 November 2022 to give it a final opportunity to make submissions. I received submissions from the Council relating to the Draft Decision on 20 December 2022. 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.

1.4 The Decision contains corrective powers under Sections 115 and 127 of the 2018 Act and Article 58(2) of the General Data Protection Regulation (the '**GDPR**') arising from the infringements which have been identified herein by the Decision Maker. The Council will be required to comply with these corrective powers that are exercised in this 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 in June 2018 to conduct a connected series of own-volition inquiries under Sections 110 and 123 of the 2018 Act into a broad range of issues pertaining to surveillance technologies deployed by state authorities, in particular, the various local authorities and An Garda Síochána 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**'), Body Worn Cameras and any other technologies that may be used to monitor individuals. The DPC informed the Council that the processing of personal data by means of CCTV security cameras situated on or in local authority offices or other local authority buildings for the purpose of safeguarding persons or property on the premises or in its environs was excluded from the scope of the inquiry. The Council was informed that the information obtained in the inquiry would be relied upon by the DPC in making a decision as to whether the 2018 Act and/or the GDPR has been infringed and if so, whether corrective powers should be exercised.

2.4 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. A revised completed version of Questionnaire No. 1 was submitted to the DPC on 23 August 2018.

2.5 On 10 August 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(s) is in operation

and they would need to inspect at least some of the CCTV camera sites, starting with [redacted] centre. The DPC signalled that there may be further phases which would deal with the replies to other questions in Questionnaire No. 1.

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

12 September 2018

- This inspection and meeting with the Data Protection Officer took place at Kildare County Council, Áras Chill Dara, Devoy Park, Naas, Co. Kildare.
- Two Authorised Officers of the Data Protection Commission, [redacted] and [redacted] were in attendance throughout.
- [redacted], Kildare County Council was in attendance throughout.
- [redacted], Kildare County Council was in attendance for the morning session.
- [redacted] was in attendance during the inspection of the traffic management centre in Áras Chill Dara and during the outdoor inspection of a number of CCTV cameras in Naas town.

7 November 2018

- The first session of this inspection took place at the Housing Department of Kildare County Council at Áras Chill Dara, Devoy Park, Naas, Co. Kildare.
- Two officials of the Housing Department, [redacted] and [redacted], were in attendance during the first session.
- The second session of this inspection took place at the [redacted] which is located at the [redacted]. This was followed by on-site inspections of CCTV cameras in three housing estates in [redacted]
- Two Authorised Officers of the Data Protection Commission, [redacted] and [redacted] were in attendance throughout all sessions.
- [redacted], Kildare County Council was in attendance throughout all sessions.

Some of the information gathered from this inquiry was relied upon by the Decision-Maker in the context of this Decision.

2.7 The DPC received a revised version of the CCTV Inventory for Kildare County Council on 25 September 2018. In summary, the inventory shows that as of the date of the inquiry, the Council deploys 105 CCTV cameras as follows:

- A total of 94 CCTV cameras located in various areas of County Kildare feed into the Traffic Management Centre at Áras Chill Dara in Naas, Co. Kildare. 73 of these cameras also feed on a live basis into Naas Garda Station.
- 88 of the 94 CCTV cameras are used to assist monitoring and management of traffic conditions on the regional and local road network throughout the county. Two of these 88 CCTV cameras have ANPR capability – one is

located at the entrance of [redacted] and the second is located at the exit of that car park. Both ANPR cameras were installed as a counting mechanism for a future Vehicle Messaging System for Naas Town.

- 2 of the 94 CCTV cameras are located in [redacted] and are used for reducing the incidence of anti-social behaviour.
- 2 of the 94 CCTV cameras are located in [redacted] and are used for security purposes.
- 2 of the 94 CCTV cameras are located in [redacted] and are used for security purposes.
- There are 11 CCTV cameras in operation that do not feed into the Traffic Management Centre. 6 of these CCTV cameras are located in the [redacted] and are used for reducing the incidence of anti-social behaviour.
- 3 of the 11 CCTV cameras are located in the [redacted] and are authorised under Section 38(3)(c) of the Garda Síochána Act 2005 (‘**2005 Act**’) by the Garda Commissioner. These are the only CCTV cameras operating in County Kildare that have been authorised by the Garda Commissioner.
- 2 of the 11 CCTV cameras are located in Bring Centres in Kildare Town and Newbridge and are used to detect littering offences.

2.8 Ultimately the Authorised Officers completed a final Inquiry Report which they submitted to me as Decision-Maker on 10 December 2019. 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 have decided to exercise arising from the infringements that are identified herein.

2.9 The findings made in this Decision include, amongst other things, findings concerning a CCTV system authorised by the Garda Commissioner under Section 38 of the Garda Síochána Act 2005[1]. 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.

2.10 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 and ANPR. The contexts of the processing operations are diverse and include traffic management, public safety, crime prevention and investigation and preventing anti-social behaviour.

[1] CCTV cameras located in the [redacted].

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;

(ii) Roads Act 1993 (as amended);

(iii) Housing (Miscellaneous Provisions) Act 1997;

(iv) Housing (Miscellaneous Provisions) Act 2009;

(v) Housing (Miscellaneous Provisions) Act 2014; and

(vi) Litter Pollution Act 1997.

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

(i) The lawful bases for the processing;

(ii) Transparency (including privacy policies and CCTV policies); and

(iii) Accountability and technical and organisational measures.

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

4. Legal regime pertaining to the inquiry and the Decision

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

4.2 The GDPR is the legal regime covering the processing of personal data in the European Union. As a regulation, the GDPR is directly applicable in EU member states. The GDPR was supplemented in Irish law by the 2018 Act. However, Article 2(2)(d) of the GDPR provides that:

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

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

"This Part applies, subject to subsection (2), to the processing of personal data by or on behalf of a controller where the processing is carried out—

(a) for the purposes of—

(i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or

(ii) the execution of criminal penalties,

and

(b) by means that—

(i) are wholly or partly automated, or

(ii) where the personal data form part of, or are intended to form part of, a relevant filing system, are not automated."

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

(i) The processing is carried out by or on behalf of a 'controller', as defined in Section 69 of the 2018 Act.

(ii) The processing is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or the execution of criminal penalties.

(i) Controller

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

(a) a competent authority that, whether alone or jointly with others, determines the purposes and means of the processing of personal data, or

(b) where the purposes and means of the processing of personal data are determined by the law of the European Union or otherwise by the law of the State, a controller nominated—

(i) by that law, or

(ii) in accordance with criteria specified in that law;

4.6 Part (a) of the definition of controller applies only to competent authorities. 'Competent authority', for the purposes of Part 5, is defined in Section 69(1) as including:

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

4.7 This definition of 'competent authority' is broad. The use of the word 'or' is disjunctive, meaning that competence for any one or more of preventing, investigating, detecting or prosecuting criminal offences is sufficient to bring pubic authorities within the definition of *'Competent authority'*. It is well-established in statutory interpretation *"that generally it is assumed that 'or' is intended to be used disjunctively and the word 'and' conjunctively"*[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 Directive[4], specifically the Directive's non-application to processing operations concerning the activities of the State in areas of criminal law.[5] This case considered the inclusion of an individual's name on a list of persons that the Finance Directorate considered 'front-men' in company director roles. The data at issue were processed for the purpose of collecting tax and combating tax fraud. However, that data could be used in criminal proceedings if infringements were identified. The Court considered the purposes of the processing and held that the data were not collected

---

[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.

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

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

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 CCTV cameras and ANPR cameras which are used for the primary purpose of traffic management.

4.14 Here, the Council is not processing personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences. The Council's policy on the use of CCTV cameras for traffic management purposes states that the

Traffic Management CCTV cameras are set at a height and orientation to enable the staff of the TMC to monitor traffic flows and detect and respond to incidents, congestion or other matters impacting efficient and safe operation of the road network. The CCTV cameras are not set with the intention of capturing personal data such as vehicle registrations or facial images as this is not necessary for the fulfilment of the traffic management functions of the Road Authority.[7]

4.15 Although the data processed through the use of Traffic Management CCTV cameras has the potential for subsequent use by An Garda Síochána for the purposes of securing public order and safety in public places and by facilitating the deterrence, prevention, detection and prosecution of offences[8], this does not form part of the Council's purposes for this processing. Therefore, this processing is not for the specific purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal penalties. The second limb of the test for the LED to apply is not satisfied and the GDPR is applicable.

---

[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.

[7] Attachment C: Traffic Management Centre (TMC) – Lawful basis, proportionality and necessity of CCTV use, page 2.

[8] This is expressly acknowledged in the Council's policy, Attachment C: Traffic Management Centre (TMC) – Lawful basis, proportionality and necessity of CCTV use, page 2.

Processing that falls under the LED

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

i. The use by the Housing Department of CCTV Cameras at [redacted] for the purposes of preventing anti-social behaviour;

ii. The transfer of CCTV footage to An Garda Síochána via [redacted]; and

iii. The use of the Council of CCTV cameras to detect illegal dumping in exercising its criminal enforcement functions under the Litter Pollution Act 1997.

CCTV relating to Housing Estates and Caravan Parks

4.17 The purposes of the processing of personal data captured through CCTV cameras used by the Housing 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 purpose of preventing, detecting and prosecuting illegal dumping pursuant to legislation applicable to littering and dumping. Thus, each piece of technology is used with the specific purpose of preventing, investigating, detecting and/or prosecuting criminal offences.

4.18 The CCTV systems operated by the Council at [redacted], 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 prevention or abatement of anti-social behaviour in a local authority housing estate. Thus, the Council determines the purposes for operating the CCTV systems at those locations. It also determines the means of the processing by determining how the data are processed. It controls who has access to the footage, when the footage is deleted, and which images to capture. Thus, the Council is a controller within the meaning of Section 69 of the 2018 Act.

4.19 Regarding the Council's use of CCTV systems, the Council is a 'controller' within part (a) of that definition under Section 69 (above). The Council is a competent authority because it enjoys competence for the prevention of certain anti-social behaviour under the Housing (Miscellaneous Provisions) Acts 1966 to 2014. 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

4.20 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 CCTV[9] and the systems that can be used.[10]

4.21 The Council is nominated as controller of this processing by Article 4(d) of the Garda Síochána (CCTV) Order 2006[11], 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.

4.22 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.

4.23 Where data are processed for one purpose and then used for another, if the purpose changes with that new use, the GDPR may become applicable. There is no evidence in the inquiry that suggests that the Council processed the CCTV data for any purpose that would exclude the application of 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"*.[12] Section 69 of the 2018 Act implements a similar definition of '*Personal data*' under the LED.

---

[9] Section 38(7) requires the Council to ensure that members of An Garda Síochána have access to the CCTV at all times for, inter alia, the purpose of retrieving information or data recorded by the CCTV.

[10] 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.

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

[12] Article 4 GDPR.

6.2 This Decision concerns CCTV systems and ANPR. 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. Analysis and findings

7.1 The Authorised Officers identified a total of 13 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 the 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) Housing Department CCTV Cameras at [redacted]: Legal Basis

Regime: LED

Inquiry Report Issue: 6

7.3 The Council's Housing Department operates CCTV systems at the [redacted] which are both estates comprising [redacted] accommodation. Six CCTV cameras have been deployed at the [redacted] and two CCTV cameras at [redacted]. I must assess whether the Council has a legal basis to process personal data and, if applicable, special categories of personal data, collected via these CCTV cameras in these circumstances and also whether it complied with its obligations in connection with carrying out a DPIA in relation to this processing.

7.4 The Council indicated that it relies on Article 6(1)(c) and Article 6(1)(e) of the GDPR when processing personal data via these CCTV cameras. The Council's stated purpose for this processing is the prevention of crime and anti-social behaviour. In the 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.

7.5 The Council sought to rely on its estate management functions set out in the following legislation as its basis for relying on Article 6(1)(c) and Article 6(1)(e) of the GDPR:

1) The general estate management function conferred on local authorities, pursuant to Section 1 of the Housing (Miscellaneous Provisions) Act 1997 (as amended by

Section 19 of the Housing (Miscellaneous Provisions) Act 2014) (the '**1997 Housing Act**'), which refers broadly to the securing and promotion of the interests of tenants, lessees, owners or occupiers of local authority houses as well as the avoidance, prevention or abatement of anti-social behaviour in a local authority housing estate;

2) The obligation conferred on local authorities, pursuant to Section 35 of the Housing (Miscellaneous Provisions) Act 2009 (the '**2009 Housing Act**') to develop and approve an anti-social behaviour strategy;

3) The various powers conferred on local authorities, derived from the anti-social behaviour provisions such as:

   a. the power to apply to the District Court for an excluding order against a respondent who the local authority believes to be engaging in anti-social behaviour (pursuant to Section 3 of the 1997 Housing Act);

   b. the power to refuse to allocate or defer the allocation of a dwelling to a household where the local authority considers that any member of the household is or has been engaged in anti-social behaviour, pursuant to Section 9 of the Housing (Miscellaneous Provisions) Act 2014 (the '**2014 Housing Act**');

   c. the power to refuse to sell a property where the person is or was engaged in anti-social behaviour (pursuant to Section 48(3) of the 2009 Housing Act);

   d. the power to refuse or defer an authorisation to a person to occupy a caravan on a site where the local authority considers that the person or a member of his or her household is or has engaged in anti-social behaviour (pursuant to Section 19(10) of the 2014 Housing Act).

7.6 While the Council referred to provisions in the GDPR in its submissions, the processing activities of the Council in these circumstances must be considered under the LED regime. To be entitled to process personal data in circumstances where Part 5 of the 2018 Act applies, among other things:

- pursuant to Section 71(1)(a) of the 2018 Act, the data must be processed lawfully and fairly;
- pursuant to Section 71(2) of the 2018 Act, processing may be lawful only where the data subject has given his or her consent, or where 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 EU or Ireland;
- pursuant to Section 73 of the 2018 Act, where special categories of personal data are processed, the processing shall be lawful only where Section 71 is complied with and one of the 9 conditions in Section 73(1)(b) is met.

7.7 I have examined the above legislation in light of these requirements under Part 5 of the 2018 Act. While it confers functions on the Council in relation to housing estates to which this legislation applies, which include the prevention of anti-social behaviour

(as defined) in those estates, I have found no requirement to support the deployment of CCTV cameras by local authorities in housing estates or Traveller caravan parks, as described above. The cited Irish legislation does not impose a legal obligation on the Council that would require the Council to monitor housing estates by way of CCTV systems, nor does it refer to the use of CCTV for the performance of the Council's estate management functions in a way that would meet the requirements of clarity, precision and foreseeability set out in respect of Issue 1 above.

7.8 In these circumstances, it is my view that Council's processing of personal data in these circumstances is not necessary for the performance of a function of a controller for a purpose specified in Section 70(1)(a) which has a legal basis in the law of the EU or Ireland. As a result, it is my view that this processing does not have a valid legal basis for the purpose of Section 71(2) and therefore infringes Section 71(1)(a).

7.9 Section 69 of the 2018 Act defines special categories of personal data as including "*personal data revealing the racial or ethnic origin of the data subject*". In Case C-184/20 the CJEU took a broad approach to defining special category personal data. It held that where the processing of personal data is liable indirectly to reveal sensitive information concerning a person, such personal data can constitute special category personal data.[13] In this case specifically it was held that publication on the website of the public authority personal data which was liable to disclose indirectly the sexual orientation of the natural person subject to the processing constituted the processing of special categories of personal data.

7.10 Irish Travellers are an ethnic group. Traveller specific accommodation may be easily identified as such by reference to its unique design and layout. Monitoring a housing estate or caravan park primarily used to accommodate members of the Traveller community, over a period of time, would tend to distinguish the residents of that estate or caravan park from visitors. By identifying the residents of such an estate or caravan park, it is possible to identify their ethnic origin. Therefore, this Decision finds that the CCTV cameras at [redacted] process special category personal data, as defined in Section 69 of the 2018 Act.

7.11 It is my view that the processing of personal data collected via these CCTV cameras is not currently supported by a valid legal basis for the purpose of Section 71 of the 2018 Act. That being the case, there can be no question of there being a legal basis to support the processing of special category personal data in accordance with Section 73 given that such processing must, in the first instance, be supported by a legal basis under Section 71 of the 2018 Act.

7.12 I welcome the submission made by the Council in response to the Draft Decision, which indicated that the CCTV cameras at [redacted] have now been disabled. 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) and 73 of the 2018 Act.

---

[13] Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* (1 August 2022) ECLI:EU:C:2022:601 paragraph 127.

Findings

7.13 ***I find that the Council infringed Sections 71(1)(a) and 73 of the 2018 Act by unlawfully processing personal data, including special categories of personal data, collected via the CCTV cameras at [redacted] for the purposes of the prevention of criminal offences without a lawful basis for such processing in European Union law or the law of the State.***

ii) Environment Section: Legal Basis for CCTV Cameras to detect illegal dumping

Regime: LED

Inquiry Report Issue: 13

7.14 CCTV cameras have been installed by the Environment Section of the Council at two recycle bring centres 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. There is one camera installed at each of the following two locations: Newbridge Tesco Bring Centre and Kildare Town Tesco Bring Centre. In both locations, there is prominent signage notifying users of the recycle centres that CCTV Cameras are in operation. I must assess whether the Council has a legal basis to process personal data collected via these cameras (to the extent that they are operational) in these circumstances.

7.15 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.

7.16 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.*

7.17 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[14], the Supreme Court interpreted the Irish legislation[15] that implemented Directive 2003/4/EC.[16] 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.*[17]

7.18 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.*[18]

7.19 In *Minister for Justice and Equality, Commissioner of An Garda Síochána v Workplace Relations Commission*[19], 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*'[20]. 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.

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

> *1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.*
>
> *2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.*

7.21 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

---

[14] *National Asset Management Agency -v- Commissioner for Environmental Information* [2015] IESC 51.
[15] Statutory Instrument No. 133 of 2007.
[16] 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.
[17] Ibid At paragraph 10.
[18] Ibid at paragraph 11.
[19] 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).
[20] At paragraph 39.

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.

7.22 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.

7.23 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.*

7.24 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*[21] 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.*

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

7.25 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.

7.26 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.

7.27 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 the three Acts that can be said to govern such a wide scope of processing. Even if the Acts did specify for this personal data to be processed, in the absence of significant other amendments, the Acts would be severely lacking in rules that govern the scope and application of such CCTV, including, among others, the criteria that must be fulfilled before installing such CCTV, the supervision of such CCTV once installed, and the termination of the CCTV. Furthermore, the Acts do not specify any procedures for preserving the integrity and confidentiality of personal data processed by such CCTV.

7.28 Therefore, I find that any such processing of personal data by the Council in these circumstances is not lawful and infringes Section 71(1)(a) of the 2018 Act.

7.29 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,[22] it stated that sections 5 – 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.

7.30 I have considered the Council's submission that "*the CCTV cameras located on the grounds of two supermarkets in Kildare and Newbridge were not operational before, during or after the DPC audit*". I have also considered the Council's comment that inaccurate information was inadvertently provided by the Data Protection Officer to the Inquiry Team during the inspection phase of the inquiry in connection with these cameras. The Council has submitted that the status of the CCTV cameras at the time of the audit, is evidenced in statements provided by staff involved and the fact that no fines were awarded based on any evidence gathered using CCTV footage for this period. The Council ought to have sought to clarify this point at an earlier stage in this

[22] See < https://www.irishstatutebook.ie/eli/isbc/2022_26.html>.

process rather than only raising it in submissions on the Draft Decision. I accept that these CCTV cameras were not operational and that, as a result, the Council was not processing personal data collected via this cameras the time the inquiry was conducted. However, if these cameras were used to collect personal data for these purposes, then this would infringe Section 71(a)(a) of the 2018 Act.

Findings

7.31 ***I find that the Council did not infringe Section 71(1)(a) of the 2018 Act by installing CCTV cameras at the 2 locations identified in circumstances where the Council did not operate these CCTV cameras.***

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

a) CCTV Cameras

i) Traffic Management CCTV cameras

Regime: GDPR

Inquiry Report Issue: 1

7.32 At the time of the inspection on 12 September, 2018, there were ninety-four CCTV cameras of the Council feeding into the Traffic Management Centre at Áras Chill Dara. The Council uses these CCTV cameras as an aid for the management of traffic in the county. This includes, for example, to alleviate congestion. The CCTV Traffic Centre Technician can remotely adjust traffic lights sequencing in the area. These CCTV cameras do not fall under the scope of Section 38 of the Garda Síochána Act 2005 and, therefore, they have not been authorised by the Garda Commissioner for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offenses. However, the images captured by the traffic management CCTV cameras may be of interest to An Garda Síochána from time to time for law enforcement functions carried out by An Garda Síochána – such as crime detection and investigation. It follows, therefore, that the images recorded on the CCTV footage are capable of being used to identify individuals, vehicles and their movements.

7.33 I accept that the Council has a function in relation to the management of traffic in the county of Kildare. However, I must assess whether the Council has a legal basis to process personal data collected via these CCTV cameras in carrying out its traffic management function. In order to lawfully process personal data using CCTV 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.

7.34 The lawful basis relied on by the Council for the operation of these cameras is Sections 2 and 13 of the Roads Act 1993 (as amended) and Article 6(1)(e) of the GDPR.

7.35 Sections 13(1) and 13(2) of the Roads Act 1993 provide that the maintenance and construction of public roads is a function of the local authorities. Sections 13(7) and 13(8) of the Roads Act 1993 provide:

> *(7) A road authority may do all such things as arise out of or are consequential on or are necessary or expedient for the performance of its functions under this Act or otherwise in relation to public roads or are ancillary thereto.*
>
> *(8) Without prejudice to the generality of subsection (7) and save as otherwise provided by law, a road authority may—*
> *(a) provide any amenity, structure or thing for the safety or convenience of road users,*
> *(b) undertake landscaping, planting or any similar activity in the interests of amenity and the environment,*
> *(c) provide artistic features.*

7.36 Section 2(d) of the Roads Act 1993 defines a 'road' as including:

> *(d) any other structure or thing forming part of the road and—*
>
> *(i) necessary for the safety, convenience or amenity of road users or for the construction, maintenance, operation or management of the road or for the protection of the environment, or*
>
> *(ii) prescribed by the Minister*

7.37 Article 6(1)(e) of the GDPR provides:

> *1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
> ...
> *(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*

7.38 To be entitled to rely on Article 6(1)(e), the processing must be necessary for the performance of a task carried out in the public interest by the Council, or necessary in the exercise of official authority vested in the Council. In addition, for the Council to have a valid legal basis for processing personal data by CCTV cameras for traffic management purposes, the relevant law relied upon must meet the criteria set out in Article 6(3) of the GDPR[23] in addition to falling within Article 6(1)(e) of the GDPR. The criteria set out in Article 6(3) can be summarised as follows:

- The legal basis should set out the purposes of the processing but this is not necessary if the processing falls within Article 6(1)(e);
- The legal basis may contain specific provisions to adapt the rules of the GDPR;

---

[23] Article 6(3) of the GDPR provides:
"The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a) Union law; or
(b) Member State law to which the controller is subject."

- The legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued.

7.39 In order for the Council to be entitled to rely on legislative measures as a basis for processing personal data, those measures also must be clear and precise and their application should be foreseeable to persons subject to them in accordance with the case law of the CJEU and the European Court of Human Rights. This requirement is reflected in Recital 41 of the GDPR, which provides as follows:

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

7.40 This is consistent with the requirement in Article 52(1) of the Charter of Fundamental Rights of the European Union that limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law. In *Schrems v Data Protection Commissioner*[24], the CJEU held that EU legislation which interferes with the fundamental rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union must lay down clear and precise rules governing the scope of the measure:

> *As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data.*[25]

7.41 Case law[26] 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 does not require the law to codify every possible instance of processing of personal data, however, it must set out principles that are capable of being predictably applied to any situation. This assessment will necessarily depend on the type of processing in question and the legal bases being relied upon.

7.42 The deployment of wide-spread video devices has significant potential to impact on the rights and freedoms of data subjects, while also, naturally, having the potential to bring significant benefits in the context of 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 CCTV and to provide adequate protection to data subjects. This

---

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

[25] Ibid, at paragraph 91.

[26] Including *Fernández Martínez v Spain* [2014] ECHR 615 and *Slivenko v Latvia* [2003] ECHR 498

is also necessary to restrict the scope of the discretion of the Council to install CCTV cameras and to reduce the likelihood of arbitrary interferences with personal data subjects' right to the protection of their personal data.

7.43 The Council relies on Section 13 of the Roads Act 1993 (as amended), interpreted in light of the definitions set out in Section 2 of that Act, as this gives local authorities the competence of carrying out traffic management functions in relation to public roads, which is a task carried out in the public interest. However, neither Section 13 nor Section 2 contains the level of detail required of a legislative basis for processing personal data via CCTV cameras for traffic management purposes in order for these legislative provisions to meet the applicable standards of clarity, precision and foreseeability that are required under applicable case law and as described in Recital 41 of the GDPR. By not providing that the persons employed by the local authority can make use of CCTV cameras for traffic management purposes, the Roads Act 1993 (as amended) is unclear as to what personal data the local authority is entitled to process and what means it is entitled to use to do this. A data subject would not be able to foresee from the wording of Sections 13 or 2, that the Council would be able to conduct CCTV surveillance for traffic management purposes, or the circumstances in which such CCTV is permitted. Therefore, the Act is an insufficiently clear, precise and foreseeable to constitute a valid legal basis for the processing of personal data via CCTV for the purpose of Article 6(1)(e) of the GDPR, interpreted in light of applicable case law and Recital 41 of the GDPR.

7.44 I note the Council's submissions made on receipt of the Draft Decision that the traffic management CCTV system is used on a "*necessary and proportionate basis*" to monitor traffic and to assist the Council in its "*legal duties to manage the safe operation of all transportation modes on the public road network*" and that if the Council is required to cease using the traffic management CCTV system that this will have an impact on road safety. I acknowledge that the Council has a role in managing traffic in the County of Kildare. However as I have outlined above, the Council must have a legislative basis to rely on in order to lawfully process personal data using CCTV cameras.

7.45 I have also given regard to the Council's submission that the "*the provision of traffic management CCTV to monitor traffic flows are specific planning conditions for approved planning applications in the County Kildare, both for permissions by the Council and An Bord Pleanála ...*" The Council did not however outline the legislative basis for processing personal data via CCTV cameras for the purpose of proper planning and development of the area. Therefore I remain of the view that the Council did not have a lawful basis to process personal data collected via these CCTV cameras for the purpose of traffic management and accordingly infringed Article 5(1)(a) of the GDPR.

Findings

7.46 ***I find that the Council infringed Article 5(1)(a) of the GDPR by not having a lawful basis to process personal data collected via these CCTV cameras for the purposes of traffic management.***

b) Sharing live feed of traffic management cameras with An Garda Síochána

Regime: GDPR

7.47 At the time of the inspection on 12 September 2018, seventy-three CCTV cameras of the Council that feed into the Traffic Management Centre at Áras Chill Dara were linked over a radio link network to An Garda Síochána at Naas Garda Station, which is a different controller. These feeds allow An Garda Síochána to monitor images from the camera feeds in real time, to view and rewind CCTV footage and to adjust the position of the cameras on the camera poles. The Council understands that An Garda Síochána uses the CCTV feeds for law enforcement functions such as crime detection and investigation.

7.48 As the primary purpose for installing cameras was the monitoring of traffic, whereas it appears the use of cameras by An Garda Síochána for crime detection purposes was a secondary or ancillary purpose, the applicable framework for assessing the legality of processing is the GDPR.

7.49 The Council does not have a valid legal basis for sharing the traffic management cameras with An Garda Síochána under Article 6 GDPR. An application for authorisation to the Garda Commissioner was not made under section 38 of the 2005 Act in respect of the traffic management cameras and the Council accordingly was not bound by section 38(7) of the 2005 Act to ensure that members of An Garda Síochána had access to the CCTV cameras.

7.50 I note the Council's submissions made on receipt of the Draft Decision, in which it stated that the live feed has been disabled. Although I welcome this submission, as this was not the case at the time the inquiry was conducted, I find the Council infringed Article 5(1)(a) GDPR.

Findings

7.51 ***I find that the Council has infringed Article 5(1)(a) GDPR by sharing the live feed of the traffic management CCTV cameras with An Garda Síochána despite not having a valid legal basis for same.***

c) [redacted] ANPR Cameras: Legal Basis

Regime: GDPR

Inquiry Report Issue: 5

7.52 Two ANPR cameras are in operation at [redacted]. One camera is positioned at the car park entrance while the second camera is positioned at the car park exit. Both cameras were provided as a vehicle counting mechanism for a future Vehicle Messaging System for Naas Town to display occupancy of the car parks in the town. While the Vehicle Messaging System is not yet in use, both ANPR cameras are operational and are viewable at the Traffic Management Centre.

7.53 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 by 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.

7.54 *Kopp v Switzerland* is an authority for the proposition that legal bases for surveillance technologies must be particularly precisely worded. The lawful basis relied on by the Council for the operation of these cameras is Sections 2 and 13 of the Roads Act 1993 (as amended) and Article 6(1)(e) of the GDPR.

7.55 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.

7.56 For example, it is important that the legal basis include 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, will be of assistance in ensuring 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 vehicle counting. 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.

7.57 As neither Section 2 nor 3 of the Roads Act 1993 explicitly permits the Council to conduct surveillance of data subjects with ANPR technology, I find the Council does not have a lawful basis to operate CCTV cameras with ANPR facilities.

7.58 I welcome the submission made by the Council in response to the Draft Decision which indicated that the CCTV cameras in operation at [redacted] were disabled on 18 July 2019 and that prior to this the Council removed the ANPR functionality on 1 July 2019. Nonetheless, as both the CCTV and ANPR were operational at the time of the inquiry I remain of the view that the Council has infringed its obligations under Article 5(1)(a) GDPR.

Findings

7.59 ***I find that the Council has 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. I find the legislative provisions considered above cumulatively do not provide a valid legal basis for such processing under Article 5(1)(a) GDPR.***

C. Appropriate signage and general transparency

i) CCTV Cameras used for traffic management purposes

Regime: GDPR

Inquiry Issue: 4

7.60 At the time of the inspection of the Traffic Management Centre on 12 September 2018, it was established that there was no signage in place in County Kildare to inform data subjects that CCTV cameras are in operation by the Council for traffic management purposes or to indicate that the camera feeds are disclosed by the Council to An Garda Síochána, which may monitor them for law enforcement purposes. 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.

7.61 Article 5(1) of the GDPR provides:

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

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

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

7.63 Article 13 of the GDPR imposes an onus on the controller to provide this information at the time the personal data was obtained.[27] However, due to the volume of information that is required to be provided to the data subject it is permissible for the Council to adopt a "layered approach".[28] EDPB Guidelines provide that the most

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

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

important information should be included in the first layer. For CCTV surveillance, the first layer normally will be a sign which is placed at a reasonable distance from where the monitoring occurs.[29] The rationale for this is to allow the data subject "*to estimate which area is captured by a camera so that he or she is able to avoid surveillance or adapt his or her behaviour if necessary.*"[30] The content of the sign should include the details of the purposes of the processing, the identity of the controller and the existence of the rights of the data subject.[31] The contact details of the Data Protection Officer and a reference to the more detailed second layer of information and where and how to find it should also be included. [32]

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

> *The second layer information must also be made available at a place easily accessible to the data subject, for example as a complete information sheet available at a central location (e.g. information desk, reception or cashier) or displayed on an easy accessible poster. As mentioned above, the first layer warning sign has to refer clearly to the second layer information. In addition, it is best if the first layer information refers to a digital source (e.g. QR-code or a website address) of the second layer... In addition to these options, and also to make them more effective, the EDPB promotes the use of technological means to provide information to data subjects. This may include for instance; geolocating cameras and including information in mapping apps or websites so that individuals can easily, on the one hand, identify and specify the video sources related to the exercise of their rights, and on the other hand, obtain more detailed information on the processing operation.*[33]

7.65 I find the Council infringed Article 13(1) of the GDPR by failing to provide data subjects whose personal data was being collected via these CCTV cameras with details of the identity of the controller, the contact details of the data protection officer, the purposes of the processing and details on where further information required to be given by Article 13 can be obtained[34] at the time the personal data was processed. The EDPB Guidelines make clear this information is required to be provided in the first layer of information. In other words, this information should be included on signs in the vicinity of the cameras, which the Council failed to do.

7.66 Article 13(3) of the GDPR also requires the Council to provide information to data subjects when the Council intends to use the personal data for a purpose other than that for which it was collected. As the Council provided the personal data to An Garda Síochána to be used by An Garda Síochána for law enforcement purposes, there was an obligation on the Council to notify the data subject of this intention at the time the

---

[29] Ibid page 22.

[30] Ibid page 26.

[31] Ibid.

[32] Ibid.

[33] Ibid page 27.

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

personal data was collected. In not including this secondary purpose in the signs, I find the Council infringed Article 13(3) of the GDPR.

7.67 In a submission in respect of the Draft Decision, the Council stated that it has "*ring-fenced a budget*" to erect CCTV signage and intends to incorporate technological solutions to meet its transparency requirements. I have also given regard to the correspondence the Council submitted to the DPC on 20 August 2019 regarding the wording for the proposed signage. Although I welcome these intended actions on behalf of the Council, I remain of the view that the Council has infringed its obligations under Articles 13(1) and 13(3) GDPR.

Findings

7.68 ***I find the Council infringed Articles 13(1) and 13(3) of the GDPR in failing to erect signage or by providing the necessary information to data subjects in respect of the processing of personal data collected via these CCTV cameras for traffic management purposes.***

D. Joint controller agreement

i) Traffic Management CCTV Cameras: Live Feed to Naas Garda Station and Joint Controller Status

Regime: GDPR and LED

Inquiry Report Issue: 2

7.69 Article 4(7) of the GDPR defines 'controller' as meaning:

> *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

7.70 Article 26(1) of the GDPR provides:

> *Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.*

7.71 Naas Garda Station was at the time of the inspection in a position to make adjustments to the positioning of the cameras. However, the CCTV cameras were installed for the purpose of traffic management and this suggests the Council is the sole controller. While An Garda Síochána also use the CCTV for crime detection purposes and have access to the CCTV by way of a live feed to Naas Garda Station, there is no evidence of An Garda Síochána and the Council '*jointly*' determining the '*purposes*' of processing. There is no connection between the Council's decision to use the cameras for traffic management purposes and An Garda Síochána's decision to use the cameras for the purpose of countering crime. The EDPB Guidelines note there will joint

participation in the determination of means and purposes of processing where a '*common*' or a '*converging*' decision takes place on such.[35]

7.72 The EDPB Guidelines define a '*common decision*' as

> *deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.*[36]

7.73 A '*converging decision*' is defined as:

> *if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing. As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.*[37]

7.74 Applying these definitions, it is my view there is no evidence a common decision was made with respect to the traffic management CCTV cameras by the Council and An Garda Síochána. The relationship also does not fall under the definition of a converging decision. For example, An Garda Síochána's role in the processing of data is not integral to the relationship and the processing of data by the Council for traffic management purposes could take place in the absence of An Garda Síochána using it for the purpose of countering crime.

Findings

7.75 ***I find there is no joint controller relationship in respect of the traffic management CCTV cameras and the Council has not infringed Article 26 of the GDPR.***

E. Security Measures for Traffic Management CCTV

Regime: GDPR

Inquiry Issue: 3

i) Access Logs

7.76 The CCTV system operated by the Traffic Management Centre at Áras Chill Dara has a functionality that electronically logs all accesses to the CCTV camera views and recorded footage. This includes accesses to the system which occurs at Naas Garda Station. In the case of Council staff who access the traffic management CCTV system, the accesses are logged by individual usernames which allows for the identification of specific Council staff members who access the system and the date and time of access. However, where there is access to the system from Naas Garda Station, the access is logged under one common username, "Garda 1". Therefore, it is impossible for the Council to identify from the logging records precisely which members of staff at Naas

[35] EDPB Guidelines, Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 (adopted on 02 September 2020).
[36] Ibid page 18.
[37] Ibid.

Garda Station have access or are accessing its CCTV camera views and recorded footage. I must assess whether this infringed the Council's security obligations under the GDPR.

7.77 Under Article 5(1)(f) of the GDPR, personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Article 32(1) of the GDPR requires a controller to implement appropriate technological and organisational measures to ensure a level of security appropriate to the risk in connection with the processing of personal data including among other things, the ability to ensure the ongoing confidentiality and integrity of processing systems. The requirement to have an access log or an equivalent security measure can be derived from Article 32(1) of the GDPR. An access log is necessary to demonstrate compliance as there is no other way of verifying whether the purpose the data was processed for was a lawful one and if the person who sought the data was legally entitled to access it.

7.78 I am of the view that this would be appropriate in relation to personal data collected via the CCTV system operated by the Council's Traffic Management Centre and that, accordingly, access to such personal data by members of An Garda Síochána from Naas Garda Station ought to have been logged in a way that ensured that the specific member of An Garda Síochána was capable of being identified, rather than all such members using a common username.

7.79 I acknowledge the corrective measures taken by the Council to address the security concerns raised at the inspection stage of the inquiry which were described in submissions made on receipt of the Draft Decision. These included ensuring that access to the live CCTV feed was locked down in Naas Garda Station and confirming An Garda Síochána had designated authorised users to access the live feed in the Garda Station. Although I welcome these measures I remain of the view, that during the time of the inquiry, the Council infringed Article 32(1) GDPR.

Findings

7.80 ***I find that the Council infringed Article 32(1) of the GDPR by failing to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station.***

F. Security Measures for Housing Department CCTV Cameras

Regime: LED

Inquiry Report Issue: 7, 8

(i) Accessibility of Monitoring Screens

7.81 The Housing Department operates CCTV systems at the [redacted] – both of which are estates [redacted] The camera feeds from both CCTV systems are accessible on a monitoring screen connected to a computer in the Housing Department at Áras Chill Dara.

7.82 On the day of inspection, there was no restriction on staff from other sections of the Council entering the area of the Housing Department where the monitoring screen and computer are situated. This is in contrast to the Traffic Management Centre, which is located in the same building, which is secured against unauthorised staff.

7.83 Access to the monitoring screen and computer is password controlled; however, this equipment is located in an unrestricted area which presents a security vulnerability as the CCTV live feeds or recorded footage can be viewed by passing staff. I must assess whether the Council has complied with its security obligations in these circumstances.

7.84 The Council's stated purpose for this processing is the prevention of crime and anti-social behaviour. In the 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.

7.85 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

7.86 I have considered the Council's submissions relating to the Draft Decision, in which the Council stated that, on foot of the provisional view of the Authorised Officers at the inspection stage of the inquiry, the Council moved the CCTV monitor to an enclosed space with a restrictive view and further ensured that the download functionality was disabled on the computer. The Council also stated that it had implemented a protocol whereby access to the monitor was limited to signed, authorised users. While I acknowledge that corrective measures have been taken by the Council and the CCTV cameras have now been disabled, I remain of the view that the Council infringed its obligations under Sections 71(1)(f), 72(1) and 28 of the 2018 Act.

Findings

7.87 ***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*** [redacted]

(ii) Access Logs for CCTV Systems

Regime: LED

Inquiry Report Issue: 8

7.88 The CCTV system operated by the Housing Department has a functionality which electronically logs all accesses to the CCTV camera views and recorded footage. Access to the cameras are restricted to two authorised Housing Department staff; however, access by both authorised Housing Department staff members are logged under one common username: "Admin". It is impossible for the Council to identify from the logging records precisely which members of the Housing Department staff have accessed or are accessing its CCTV system. I must assess whether the Council has complied with its security obligations under the 2018 Act in these circumstances.

7.89 In the 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.

7.90 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, in so far as is possible.

7.91 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.

7.92 I have considered the Council's submission relating to the Draft Decision, in which the Council stated that it has implemented stronger access limitations or controls and had assigned unique and identifiable usernames and passwords to designated authorised users of the CCTV monitor. The Council outlined that these actions were carried out prior to the CCTV cameras being disabled on 25 March 2022. Although I welcome this submission, this was not the case at the time of the inquiry and so I remain of the view that the Council has infringed Section 82(2) of the 2018 Act.

Findings

7.93 ***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*** [redacted]

(iii) Focus of one CCTV Camera at [redacted]

Regime: LED

Inquiry Report Issue: 9

7.94 The Housing Department of the Council has deployed six CCTV cameras at [redacted] since the summer of 2018. The Inquiry Team inspected these cameras on 7 November 2018 during the investigation. The Inquiry Team noted that one of the six cameras focused on the private space at the front of a dwelling house at which a black car was parked. This CCTV camera was focused on a private space rather than a public space and, accordingly, the camera had the potential to invade on

the privacy of residents of and visitors of the dwelling house. I must assess whether the Council has complied with its data minimisation obligations in these circumstances.

7.95 In the 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.

7.96 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.*"

7.97 The concept of what is "*not excessive*"[38] was considered in *Deutsche Post AG v Hauptzollamt Köln.*[39] 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 to that purpose. This judgment illustrates the breadth of purposes that must be considered for determining what is not excessive.

7.98 The alleged purpose of the processing of personal data via these CCTV systems is to reduce the incidences of anti-social behaviour at [redacted] 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.

7.99 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

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

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

position to demonstrate that the focus of the CCTV camera on the private dwelling is not excessive to preventing anti-social behaviour at [redacted]

7.100 The Council has infringed section 76(2) of the 2018 Act for 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.

7.101 I welcome the Council's submission made in response to the Draft Decision, which indicated that the Council had disabled the CCTV cameras and prior to this the Council had sought to remedy the positioning of one of the CCTV cameras on foot in order to capture the public area as provided for in the DPIA. However as this was not the case at the time of the inquiry was conducted I find the Council has infringed Section 71(1)(c) and Section 76(2) of the 2018 Act.

Findings:

7.102 ***I find that the Council infringed Section 71(1)(c) and Section 76(2) of the 2018 Act by recording CCTV of private properties, in the absence of any privacy masking technology, at*** [redacted]

7.103 ***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 via CCTV cameras at the*** [redacted] ***is not excessive to its purpose of preventing anti-social behaviour.***

G. Security Measures regarding Transmission of CCTV Footage to An Garda Síochána

Regime: LED

Inquiry Report Issue: 12

7.104 There is an authorised community-based CCTV scheme under Section 38(3)(c) of the Garda Síochána Act 2005 covering three estates in Athy, Co. Kildare. The management and control of this CCTV system comes under one staff member's remit at the [redacted] One of his roles is to process requests made to the Council by An Garda Síochána for copies of CCTV footage captured by the community-based CCTV scheme. The Inquiry Team established that three such requests for CCTV footage were made in 2018. It further established that on receipt of a Garda request, the Council's practice was for the designated Council staff member to download the CCTV footage to an unencrypted USB stick which he then delivered in person to the Garda station. I must assess whether the Council complied with its security obligations under the LED in these circumstances.

7.105 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.

7.106 I find that at the time of the inspection, the Council's obligations to ensure appropriate security measures were taken to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage were not complied with in respect of security measures surrounding the transfer of personal data from [redacted] to An Garda Síochána using unencrypted USB sticks.

7.107 I have considered the Council's submission on receipt of the Draft Decision in which the Council stated that this CCTV system was not operating in November 2018 when an on-site inspection was carried out by the Inquiry Team and that no CCTV footage was being transmitted to An Garda Síochána in connection with this system on that date. The Council also stated that since the on-site inspection was carried out, the Council has taken steps to ensure that all such requests are now centralised through the Council's data protection unit. I accept that this CCTV system was not operational on the date on which the site inspection was carried out by the Inquiry Team and welcome the steps that the Council informs me have been taken since that date. However, these do not alter the facts, as established by the Inquiry Team, that CCTV footage collected via these cameras was previously provided to An Garda Síochána on request, via unencrypted USB sticks. In these circumstances, the Council had infringed its obligations under Sections 71(1)(f), 72(1) and 78 of the 2018 Act, even if such infringements were not ongoing on the date of the on-site inspection.

Finding

7.108 ***I find that the Council infringed its obligations under Sections 71(1)(f), 72(1) and 78 of the 2018 Act in connection with arrangements surrounding the transfer of personal data from [redacted] to An Garda Síochána using unencrypted USB sticks.***

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	I have found the Council has infringed this section by: Unlawfully processing personal data via CCTV cameras at [redacted] without having a lawful basis to do so; and
Article 5(1)(a) of the GDPR	I have found the Council has infringed this section by: Unlawfully processing personal data via CCTV cameras for the purposes of traffic management at in respect of the 94 CCTV cameras which were feeding into the Traffic Management Centre at Áras Chill Dara;

	Unlawfully processing personal data by sharing the feed of 73 CCTV cameras feeding into the Traffic Management Centre at Áras Chill Dara with An Garda Síochána at Naas Garda Station; Unlawfully processing personal data via ANPR cameras for the purposes of traffic management at [redacted];
Article 13 of the GDPR	I have found the Council has infringed Article 13 of the GDPR in failing to erect signage or by providing the necessary information to data subjects in relation to its processing of personal data by traffic management CCTV cameras.
Section 73 of the 2018 Act	I have found the Council unlawfully processed special categories of personal data at [redacted]
Article 32 of the GDPR	I have found that the Council infringed Article 32(1) of the GDPR by failing to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station.
Section 71(1)(f) of the 2018 Act	I have found that the Council infringed Section 71(1)(f) of the 2018 Act by: Failing to implement technical or organisational 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 [redacted]; and Failing to implement measures to ensure appropriate security of personal data in connection with arrangements surrounding the transfer of personal data from [redacted] to An Garda Síochána using unencrypted USB sticks.
Section 72(1) of the 2018 Act	I have found that the Council infringed Section 72(1) of the 2018 Act by: Failing to implement technical or organisational 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 [redacted]; and Failing to implement measures to ensure appropriate security of personal data in connection with arrangements surrounding the transfer of personal data from [redacted] to An Garda Síochána using unencrypted USB sticks.
Section 78 of the 2018 Act	I have found that the Council infringed Section 72(1) of the 2018 Act by: Failing to implement technical or organisational 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 [redacted]: and Failing to implement measures to ensure appropriate security of personal data in connection with arrangements surrounding the transfer of personal data from Athy Customer Hub to An Garda Síochána using unencrypted USB sticks.
Section 82(2) of the 2018 Act	I have found that the Council infringed Section 82(2) of the 2018 Act by failing to maintain a data log that recorded the identify of any individual who consulted personal data contained in the CCTV camera views and recorded footage from [redacted]
Section 71(1)(c) of the 2018 Act	I have found that the Council infringed Section 71(1)(c) of the 2018 Act by recording CCTV of private properties in the absence of any privacy masking technology at [redacted]
Section 71(10) of the 2018 Act	I have found that the Council infringed Section 71(10) of the 2018 Act by failing to demonstrate that the its processing of personal data via CCTV cameras at the [redacted] is not excessive to its purpose of preventing anti-social behaviour.

8.2 Having considered the infringements that I found in this Decision, I have decided 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 in Part 9 of 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. <u>Lawful Bases for the Processing</u>

No.	Action	Time Scale
1.	CCTV cameras located at [redacted] used for law enforcement purposes CCTV cameras located at Newbridge Tesco Bring Centre and Kildare Town Tesco Bring Centre used for law enforcement purposes Section 71(1)(a) of the 2018 Act I find that there is no lawful basis for the Council's processing of personal data by means of CCTV cameras at [redacted]. I 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	The Council is required to confirm to the Data Protection Commission within 90 days of receiving this Decision that the cameras are switched off, unless another legal basis for the processing can be pinpointed in the meantime.

	such processing in accordance with Article 8(2) of the LED. I find that there is no lawful basis for the Council's processing of personal data by means of CCTV cameras at Newbridge Tesco Bring Centre and Kildare Town Tesco Bring Centre. I impose a temporary ban on the Council's use of CCTV at these locations. This processing must not commence or resume, as applicable, 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.	
2.	CCTV cameras feeding into the Traffic Management Centre at Áras Chill Dara used for traffic management purposes Sharing of live feed of 73 CCTV cameras feeding into the Traffic Management Centre at Áras Chill Dara with An Garda Síochána at Naas Garda Station ANPR cameras at [redacted] used for traffic management purposes Article 5(1)(a) of the GDPR I find that there is no lawful basis for the Council's processing of personal data by means of CCTV cameras for traffic management purposes. I impose a temporary ban on the Council's use of CCTV cameras feeding into the Traffic Management Centre at Áras Chill Dara. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing in accordance with Article 5(1)(a) and Article 6 of the GDPR. I find that there is no lawful basis for the Council providing An Garda Síochána with a live feed to the traffic management CCTV cameras. I impose a temporary ban on the Council providing this live feed from the Traffic Management Centre at Áras Chill Dara to An Garda Síochána at Naas Garda Station. The provision of the live feed should not resume, unless, and until there is a	The Council is required to confirm to the Data Protection Commission within 120 days of receiving this Decision that the cameras are switched off and the live feed has been discontinued unless another legal basis for the processing can be pinpointed in the meantime.

	basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing in accordance with Article 5(1)(a) and Article 6 of the GDPR. I find that there is no lawful basis for the Council's processing of personal data by means of ANPR cameras. I impose a temporary ban on the Council's use of ANPR cameras for traffic management purposes at [redacted] in Naas. This processing must not resume unless, and until, there is a basis for it in EU or Member State Law, for example an Act of the Oireachtas that regulates such processing in accordance with Article 5(1)(a) and Article 6 of the GDPR.	

ii. Transparency

No.	Action	Time Scale
3.	Traffic Management CCTV Cameras feeding into the Traffic Management Centre Articles 13(1) and Article 13(3) of the GDPR I order the Council to bring its processing by means of CCTV cameras into compliance with Article 13 of the GDPR by ensuring that all data subjects are provided with all the information required by Articles 13(1) and 13(3) of the GDPR. This must be achieved by installing signage in the vicinity of where the traffic management CCTV cameras are operating which gives data subjects advanced notice of the processing, the purposes of the processing, and the identity of the controller.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with traffic management CCTV cameras, prior to commencing processing Order 3 must be complied with.

iii. Technical and Organisational Measures

No.	Action	Time Scale
4.	Security Measures for CCTV system at the Traffic Management Centre at Áras Chill Dara Article 32(1) of the GDPR I order the Council to bring its processing into compliance with the GDPR by requiring the controller to ensure persons who access footage from the CCTV cameras connected to the Traffic Management Centre at Áras Chill Dara leave	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with traffic management CCTV cameras, prior to commencing processing Order 4 must be complied with.

	their identity and the purpose for which they accessed the data in the log book.	
5.	Security Measures for Housing Department CCTV Cameras Sections 71(1)(f), 72(1) and 78 of the 2018 Act I order the Council to bring its processing operations into compliance with the 2018 Act by implementing security measures so as to restrict access to the room where the CCTV cameras are to authorised persons only.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at [redacted] prior to commencing processing Order 5 must be complied with.
6.	Security Measures for Housing Department CCTV Cameras Section 82(2) of the 2018 Act I order the Council to bring its processing into compliance with the 2018 Act by requiring the controller to ensure persons who access footage from the Housing Department CCTV cameras leave their identity and the purpose for which they accessed the data in the log book.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at [redacted] prior to commencing processing Order 6 must be complied with.
7.	Security Measures for CCTV camera at [redacted] Sections 71(1)(c), 76(2) and 71(10) of the 2018 Act I order the Council to integrate appropriate technical organisational measures required by section 76(2) of the 2018 Act in respect of the CCTV cameras at [redacted] These technical and organisational measures could include privacy masking.	If the Council identifies an appropriate legal basis and intends to recommence processing personal data with CCTV cameras at [redacted] prior to commencing processing Order 7 must be complied with.
8.	[redacted]: Transmission of CCTV Footage to An Garda Síochána Sections 71(1)(f), 72(1) and 78 of the 2018 Act I order the Council to bring its processing into compliance with Section 71(1)(f), 72(1) and 78 of the 2018 Act by implementing appropriate organisational and technical measures to ensure that transfers of CCTV footage are protected by encryption.	Complete task and submit a short report detailing the action that the Council intends to take to implement appropriate technical and organisational measures within 90 days from the date of this Decision.

9. Decision to Impose 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) provides the 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 Article 83(1) of the GDPR requires, the Decision-Maker to ensure that any administrative fines imposed on a controller as a result of an infringement of the GDPR be '*effective, proportionate and dissuasive.*' In deciding whether to impose an administrative fine, I am required to have regard to the criteria in Article 83(2) of the GDPR.[40] I will now consider each of the criteria set out in Article 83(2), in deciding whether to impose an administrative fine (or fines) following my findings that the Council has infringed Articles 13(1), 13(3) and 32(1) GDPR.

9.3 I will not consider the Article 83(2) criteria in relation to the Council's infringements of Article 5(1)(a) GDPR as I consider the orders above will suffice to bring the Council's processing into compliance with the GDPR.

A. Article 82(2) Criteria

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

i) Articles 13(1) and 13(3): Failure to erect signage and provide required information to data subjects in relation to the Council's use of CCTV cameras for traffic management purposes

9.4 The principle of transparency is of totemic importance under the GDPR. It not only relates to informing the data subject that his or her personal data has been processed, but it also imposes requirements on controllers to provide data subjects with information which will permit them to exercise their rights under the GDPR.

9.5 The infringement of Article 13 in this case is grave in nature. The Council has not provided information to data subjects which would notify them that their personal data would be processed by traffic management cameras on entering particular parts of the city. No information has been provided in relation to the traffic management cameras via signage.

9.6 Furthermore, the Council has failed to provide any of the information required to be provided to data subjects at the time the personal data has been processed as required by Article 13(1) of the GDPR. The Council has failed, at the time the personal data was processed to provide:

[40] These criteria are also relevant to determining the amount of the administrative fine, in the event a fine is imposed.

- the identity and contact details of the controller;[41]

- the contact details of the data protection officer;[42]

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;[43]

9.7 The Council has also failed to notify data subjects that the personal data captured could be used for a secondary purpose of law enforcement in violation of Article 13(3) of the GDPR. The infringement is of a significant duration continuing from the date the GDPR came into effect on 25 May 2018 at least until the inquiry report was completed on 10 December 2019.

9.8 The nature and scope of the processing are broad with 94 CCTV cameras feeding into the Traffic Management Centre and with 73 of those being shared with An Garda Síochána. In the context of processing personal data with these CCTV cameras for traffic management purposes, the Council would have processed a voluminous quantity of personal data.

9.9 The Council had licit purposes for the processing. The management of traffic can be seen as a necessary function of local authorities. Furthermore, the sharing of personal data with members of An Garda Síochána was motivated by the desire to assist this entity in carrying out its law enforcement functions.

ii) Article 32(1) GDPR: Failure to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station

9.10 I find the failure by the Council to implement an access log which would have allowed identification of individual members of An Garda Síochána who accessed the footage to be an infringement of a moderate nature and gravity. The infringement prevented the investigator from verifying whether the data had been accessed by authorised personnel only for valid purposes. The infringement is of a significant duration continuing from the date the GDPR came into effect on 25 May 2018 at least until the inquiry report was completed on 10 December 2019.

9.11 The nature and scope of the processing are broad, the Council shared 73 CCTV cameras with An Garda Síochána. In the context of processing personal data with these CCTV cameras for traffic management purposes, the Council would have processed a voluminous quantity of personal data.

9.12 The Council had licit purposes for the processing. The management of traffic can be seen as a necessary function of local authorities. Furthermore, the sharing of personal data with members of An Garda Síochána was motivated by the desire to assist this entity in carrying out its law enforcement functions

(b) the intentional or negligent character of the infringement

[41] GDPR, Article 13(1)(a).
[42] GDPR, Article 13(1)(b).
[43] GDPR, Article 13(1)(c).

i) Articles 13(1) and 13(3): Failure to erect signage and provide required information to data subjects in relation to the Council's use of CCTV cameras for traffic management purposes

9.13 I find the Council's infringement of Article 13 of the GDPR was of a negligent character. The Council did not provide an explanation for its failure to erect signage in respect of the CCTV cameras at the time of inspection on 12 September 2018 of when the Final Inquiry Report was published on 10 December 2019.

ii) Article 32(1) GDPR: Failure to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station

9.14 I find the Council's infringement of Article 32(1) of the GDPR was of a negligent character. The Council was culpable in failing to ensure that Garda members accessing the footage would be able to be identified at a subsequent date to ensure the processing was undertaken for valid reasons.

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

i) Articles 13(1) and 13(3): Failure to erect signage and provide required information to data subjects in relation to the Council's use of CCTV cameras for traffic management purposes

9.15 In a submission in respect of the Draft Decision, the Council stated that it has "*ring-fenced a budget*" to erect CCTV signage and intend to incorporate technological solutions to meet its transparency requirements. I have also given regard to the correspondence the Council submitted to the DPC on 20 August 2019 regarding the wording for the proposed signage. Although I welcome this action on behalf of the Council, this proposed action relates to the duration of the infringement, rather than action taken to mitigate damage already suffered by data subjects.

9.16 I remain of the view that the Council has not taken any actions which amount to a mitigating factor in respect of damage already suffered by data subjects as a result of this infringement.

ii) Article 32(1) GDPR: Failure to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station

9.17 I consider the following actions to be a mitigating factor in respect of the infringement:

> *An Garda Síochána have approved in writing and communicated to the Council a limited number of named users who are set up in the Data Log with unique and identifiable user names and passwords.*
>
> *The Data Log is available for audit by the Council's Data Protection Officer but also by an approved local Garda Inspector and a Superintendant so Gardai can supervise their access. This will make the identity of Garda Users available to the relevant supervisors who can oversee compliance in appropriate*

confidentiality measures in the operational environment of Naas Garda Station"[44]

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

9.18 This limb of Article 83(2) is not relevant in the circumstances for considering whether an administrative fine should be imposed in respect of the infringements of the GDPR. Insofar as the controller was negligent in respect of failing to implement appropriate technical and organisational measures required by Article 32 (for example a valid access log) this has already been considered under Article 83(2)(b).

(e) any relevant previous infringements by the controller or processor;

9.19 The Council has no previous infringements since the GDPR came into effect on 25 May 2018. However, in the circumstances, this is of no mitigating value considering the brief period of time that passed prior to the inquiry commencing in June 2018.

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

9.20 I find the Council has cooperated with the DPC during the course of the inquiry. I do not regard this as a mitigating factor, however, as the Council has a statutory duty to cooperate under Article 31 of the GDPR.

(g) the categories of personal data affected by the infringement;

9.21 It should be noted many data protection implications arise from video surveillance. The EDPB Guidelines note:

> *Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed.*[45]

9.22 I have given regard to the particular risks posed to data subjects' rights and freedoms by video surveillance in arriving at my conclusion on whether it is appropriate to impose an administrative fine or not (and, if so, the quantum of such) in this Decision.

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

9.23 The information grounding this Decision was obtained by way of an own volition inquiry conducted by the Data Protection Commission. The Council co-operated with the Data Protection Commission in furnishing the necessary information as requested. I have identified a number of infringements of the GDPR committed by the Council

[44] Final Inquiry Report page 22.

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

on foot of this information. However, as the Council is under a legal obligation to supply this information, the Council's co-operation with the Data Protection Commission during the inquiry cannot be seen as a mitigating factor.

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

9.24 This limb of Article 83(2) is not relevant for considering whether an administrative fine should be imposed in respect of the infringements of the GDPR as there has been no previous measures ordered against the Council under Article 58(2).

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

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

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

9.26 I can identify no other aggravating or mitigating factors in respect of any infringements found in this Decision.

a. ***Decision to impose an administrative fine for each infringement***

i) Articles 13(1) and 13(3): Failure to erect signage and provide required information to data subjects in relation to the Council's use of CCTV cameras for traffic management purposes

9.27 Having considered the criteria set out in Article 83(2) of the GDPR, I have decided to impose an administrative fine for the Council's infringement of Article 13 of the GDPR.

9.28 In arriving at the conclusion to impose a fine, I have been particularly influenced by the blanket nature of the infringements which gives the infringements an added level of gravity and severity. In relation to the infringements of sub-sections (1) and (3) of Article 13, the Council has failed to provide any of the required information, which is relevant to the processing under these sub-sections.

9.29 I have had regard to the fining cap provided for in section 141(4) of the 2018 Act and to the nature, gravity and duration of the infringement as assessed in accordance with Article 83(2)(a) above. I have also had regard to the aggravating factors, specifically the negligent character of the infringement as assessed in accordance with Article 83(2)(b) above. I therefore consider that a fine of **€50,000** is appropriate. I consider that this fine is an effective, proportionate and dissuasive figure as required by Article 83(1).

ii) Article 32(1) GDPR: Failure to maintain a data log that recorded user specific accesses of the CCTV camera views and recorded footage from Naas Garda Station

9.30 Having considered the criteria set out in Article 83(2) of the GDPR, I have decided not to impose an administrative fine for the Council's infringement of Article 32(1). In deciding not to impose a fine, I have given particular regard to the corrective measures the Council has taken to rectify the infringement.

b) Total value of the administrative fine

9.31 In summary, I have decided to impose one administrative fine in this case of **€50,000**.

9.32 It is my view that the administrative fine imposed meets the requirements of effectiveness, proportionality and dissuasiveness. In order for any fine to be effective it must reflect the circumstances of the individual case. I consider that the circumstances of the relevant infringement requires a significant fine in order for it to be effective. In order for a fine to be dissuasive, it must dissuade the controller from repeating the conduct concerned. I am satisfied that the administrative fine would be dissuasive to the Council. As regards the requirement for any fine to be proportionate, this requires me to adjust the quantum of any administrative fine to the minimum amount necessary to achieve the objectives pursued by the GDPR. I am satisfied that the administrative fine does not exceed what is necessary to enforce compliance with the GDPR, taking into account the impact of the infringements on the data subject rights enshrined in the GDPR. Accordingly, I am satisfied that the administrative fine would be effective, proportionate and dissuasive, taking into account all of the circumstances of the case.

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. Furthermore, as this Decision includes a decision to impose an administrative fine, pursuant to Section 142 of the 2018 Act, the Council also has the right to appeal against the decision to impose an administrative fine within 28 days from the date on which notice of the decision is given to it.

Helen Dixon

Commissioner for Data Protection

11. Appendices

Materials considered

11.1 The Authorised Officers delivered the Inquiry Report to me on 10 December 2019. I was also provided with all of the submissions received in compiling the report and the submissions made by the Council in respect of the Inquiry Report, including:

List of Appendices to the Inquiry Report

(i) Appendix 1 – Copy of Questionnaire No 1;
(ii) Appendix 2 – Copy of Completed Questionnaire No 1 (submitted on 16 July 2018);
(iii) Appendix 3 – Copy of Revised Completed Questionnaire No. 1 (submitted on 23 August 2018);
(iv) Appendix 4 – Index of documents submitted by Kildare County Council;
(v) Appendix 5 – Revised CCTV Inventory submitted on 25 September 2018;
(vi) Appendix 6 – Copy of letter accompanying the Draft Inquiry Report;
(vii) Appendix 7(i) – Covering letter from Kildare County Council regarding submissions;
(viii) Appendix 7(ii) – Copy of submissions received from Kildare County Council;
(ix) Appendix 8 – Confirmation of disabling of cameras in [redacted] submitted on January 2019;
(x) Appendix 9 – DPIA CCTV [redacted] submitted on 16 July 2018;
(xi) Appendix 10 – Revised DPIA CCTV [redacted] submitted on 11 October 2018
(xii) Submissions on the Draft Decision dated 20 December 2022 and appended correspondence.

Inquiry Team References in relation to documents submitted by Kildare County Council:

(i) Attachment A – CCTV Justification for Traffic Management;
(ii) Attachment B - Traffic Management DPIA;
(iii) Attachment C – Traffic Management Lawful Basis – Email of 11 October 2018;
(iv) Attachment D – Letter of 13 June 2019 regarding Garda Síochána access to Traffic Management CCTV and related lawful basis;
(v) Attachment E – Email of 21 August 2019;
(vi) Attachment F – Letter of 20 August 2019 from Chief Executive to An Garda Síochána;
(vii) Attachment G(a) – Draft Incomplete Joint Controller Agreement Heads – An Garda Síochána and Kildare County Council;
(viii) Attachment G(b) – Daft Incomplete Joint Controller Agreement Tabular – An Garda Síochána and Kildare County Council;
(ix) Attachment H – Item 19 Signage – Email of 11 October 2018;
(x) Attachment I – Sample of CCTV Sign
(xi) Attachment J – CCTV Signage Plan;

(xii) Attachment K(a) – Lawful Basis – Estate Management;
(xiii) Attachment K(b) – Estate Management CCTV DPIA;
(xiv) Attachment L – CCV Policy – Appendix 3 CCTV Authorised Users Protocol;
(xv) Attachment M – Litter Enforcement CCTV – necessity and lawful basis assessment;
(xvi) Attachment N – Litter Enforcement CCTV DPIA.